

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ  
АЕРОКОСМІЧНИЙ ФАКУЛЬТЕТ  
КАФЕДРА АЕРОДИНАМІКИ ТА БЕЗПЕКИ ПОЛЬОТІВ  
ЛІТАЛЬНИХ АПАРАТІВ

ДОПУСТИТИ ДО ЗАХИСТУ  
Завідувач кафедри канд. військ. наук,  
доц.

О.С. Бондік

“ “ \_\_\_\_\_ 2024 р.

**КВАЛІФІКАЦІЙНА РОБОТА  
(ПОЯСНЮВАЛЬНА ЗАПИСКА)**

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА ЗА НАПРЯМОМ 27  
«АВІАЦІЙНИЙ ТРАНСПОРТ»

Тема: “Методика ідентифікації загроз та оцінки ризиків діяльності транспортної системи (комплексу) в ході некомерційної експлуатації”

Виконавець: \_\_\_\_\_ (студент,  
група, прізвище, ім'я, по батькові)

Керівник: \_\_\_\_\_  
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

Нормоконтролер: \_\_\_\_\_  
(підпис) (П.І.Б.)

КИЇВ 2024

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ  
Аерокосмічний факультет  
Кафедра аеродинаміки та безпеки польотів ЛА  
Освітній ступень «Магістр»  
Спеціальність 272 «Авіаційний транспорт»  
Освітньо-професійна програма «Управління авіаційними транспортними  
системами та комплексами»

**ЗАТВЕРДЖУЮ**

Завідувач кафедри канд. військ. наук, доц.  
О.С. Бондік  
«   » \_\_\_\_\_ 2024 р.

**ЗАВДАННЯ**

на виконання магістерської роботи ГМИРЯНСЬКОМУ Олександровичу

Тема роботи: “Методика ідентифікації загроз та оцінки ризиків діяльності транспортної системи (комплексу) в ході некомерційної експлуатації”, затверджено наказом ректора від “ \_\_\_\_ ” жовтня 2024 року № \_\_\_\_.

Термін виконання роботи:

з “ \_\_\_\_ ” \_\_\_\_\_ 2024 р.

по “ \_\_\_\_ ” \_\_\_\_\_ 2024 р.

Вихідні дані до роботи: нормативно-правова база документації зі спеціалізованої експлуатації повітряних суден, вимоги та умови виконання робіт з технічного обслуговування виробів авіаційної техніки, порядок освоєння ремонту виробів авіаційної техніки державної авіації, методи досліджень АТС.

Зміст пояснювальної записки: безпека на авіаційному транспорті; категоріально-правовий аналіз; загальна характеристика загроз та ризиків у системі управління авіаційною безпекою; аналіз методів загального оцінювання ризиків та загроз безпеці авіаційних транспортних систем; обґрунтування вимог до методичного забезпечення діяльності АТС щодо ідентифікації загроз та оцінки ризиків в ході некомерційної експлуатації; методичний підхід до забезпечення авіаційної безпеки; обґрунтування системи показників загроз та ризиків; узагальнена модель динаміки рівня безпеки авіаційної транспортної системи; методика визначення пріоритетів показників, що характеризують рівень безпеки авіатранспортної системи; комплексна методика оцінювання загроз і ризиків; рекомендації щодо удосконалення методичної бази оцінювання загроз та ризиків в авіапідприємствах України; методичні рекомендації щодо оцінювання факторів ризику для безпеки польотів; оцінка ризику за методологією European Risk Classification Scheme (ERCS); рекомендації, що пов’язані з ризиками та загрозами

безпеці цивільної авіації України, які спричинені збройною агресією Російської Федерації.

Перелік обов'язкового графічного (ілюстративного) матеріалу: онтологічна схема забезпечення авіаційної безпеки; внесок загального оцінювання ризику до процесу керування ризиком; функціональна модель системи авіаційної безпеки; послідовність визначення пріоритетів окремих показників, що характеризують рівень безпеки АТС; узагальнена схема ієрархії знаходження пріоритетів окремих показників, що визначають рівень безпеки; блок-схема алгоритму визначення пріоритетів окремих показників, що характеризують рівень АТС; визначення заходів протидії загрозам АТС; граф оцінювання загроз та ризиків; блок-схема алгоритму методики оцінювання загроз та ризиків; структура процесу управління факторами ризику; алгоритм управління факторами ризику при забезпеченні безпеки польотів; матриця оцінки факторів (індекси); матриця припустимості факторів ризику; варіант матриці припустимості факторів ризику для безпеки польотів; загальна оцінка рівня ризику події з безпеки польотів за шкалою матриці ERCS.

Графічний (ілюстративний) матеріал виконано із застосуванням Google Docs, Google Slides та надано у вигляді листів.

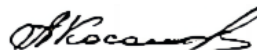
### Календарний план-графік

Завдання	Термін виконання	Відмітка про виконання
Безпека на авіаційному транспорті: категоріально-правовий аналіз		
Загальна характеристика загроз та ризиків у системі управління авіаційною безпекою		
Аналіз методів загального оцінювання ризиків та загроз безпеці авіаційних транспортних систем		
Обґрунтування вимог до методичного забезпечення діяльності АТС щодо ідентифікації загроз та оцінки ризиків в ході некомерційної експлуатації.		
Методичний підхід до забезпечення авіаційної безпеки. Обґрунтування системи показників загроз та ризиків		
Узагальнена модель динаміки рівня безпеки авіаційної транспортної системи.		
Методика визначення пріоритетів показників, що характеризують рівень безпеки авіатранспортної системи		
Комплексна методика оцінювання загроз і ризиків		

Рекомендації щодо удосконалення методичної бази оцінювання загроз та ризиків в авіапідприємствах України		
Методичні рекомендації щодо оцінювання факторів ризику для безпеки польотів		
Оцінка ризику за методологією European Risk Classification Scheme (ERCS)		
Рекомендації, що пов'язані з ризиками та загрозами безпеці цивільної авіації України, які спричинені збройною агресією Російської Федерації		
Оформлення пояснювальної записки та ілюстративного матеріалу		
Попередній захист роботи		
Консультанти по окремим розділам		
Розділ	Консультант	Дата, підпис

Дата видачі завдання: « \_\_\_\_\_ » жовтня 2024 року.

Керівник дипломної роботи



Косо́гов О.М.

Завдання прийняв до виконання \_\_\_\_\_

## ЗМІСТ

### РОЗДІЛ 1. СУТНІСТЬ ЗАВДАННЯ ІДЕНТИФІКАЦІЇ ЗАГРОЗ ТА ОЦІНКИ РИЗИКІВ В СИСТЕМІ АВІАЦІЙНОЇ БЕЗПЕКИ.....

- 1.1. Безпека на авіаційному транспорті: категоріально-правовий аналіз.....
  - 1.2. Загальна характеристика загроз та ризиків у системі управління авіаційною безпекою.....
  - 1.3. Аналіз методів загального оцінювання ризиків та загроз безпеці авіаційних транспортних систем.....
  - 1.4. Обґрунтування вимог до методичного забезпечення діяльності АТС щодо ідентифікації загроз та оцінки ризиків в ході некомерційної експлуатації.....
- Висновки до розділу.....

### РОЗДІЛ 2. РОЗРОБКА МЕТОДИЧНОГО АПАРАТУ ІДЕНТИФІКАЦІЇ ЗАГРОЗ ТА ОЦІНКИ РИЗИКІВ ДІЯЛЬНОСТІ ТРАНСПОРТНОЇ СИСТЕМИ (КОМПЛЕКСУ) В ХОДІ НЕКОМЕРЦІЙНОЇ ЕКСПЛУАТАЦІЇ.....

- 2.1. Методичний підхід до забезпечення авіаційної безпеки. Обґрунтування системи показників загроз та ризиків.....
  - 2.2. Узагальнена модель динаміки рівня безпеки авіаційної транспортної системи.....
  - 2.3. Методика визначення пріоритетів показників, що характеризують рівень безпеки авіатранспортної системи.....
  - 2.4. Комплексна методика оцінювання загроз і ризиків.....
- Висновки до розділу.....

### РОЗДІЛ 3 РЕКОМЕНДАЦІЇ ЩОДО ЗАСТОСУВАННЯ РОЗРОБЛЕНОГО МЕТОДИЧНОГО АПАРАТУ ДЛЯ ІДЕНТИФІКАЦІЇ ЗАГРОЗ ТА ОЦІНКИ РИЗИКІВ ДІЯЛЬНОСТІ ТРАНСПОРТНОЇ СИСТЕМИ (КОМПЛЕКСУ)

- 3.1. Рекомендації щодо удосконалення методичної бази оцінювання загроз та ризиків в авіапідприємствах України
- 3.2. Методичні рекомендації щодо оцінювання факторів ризику для безпеки польотів
- 3.3. Оцінка ризику за методологією European Risk Classification Scheme (ERCS)
- 3.4. Рекомендації, що пов'язані з ризиками та загрозами безпеці цивільної авіації України, які спричинені збройною агресією Російської Федерації

Висновки до розділу

ЗАГАЛЬНІ ВИСНОВКИ

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

## **ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ**

BIA – аналіз впливу на діяльність

ICAO - International Civil Aviation Organization (Міжнародна організація цивільної авіації)

EASA - Європейська організація з безпеки авіації

ECAC - Європейська конференція цивільної авіації

ERCS – European Risk Classification Scheme (Європейська схема класифікації ризиків)

MCA – Міжнародна рада аеропортів

RCA – аналіз першопричин

АНВ – акт незаконного втручання

АТС(К) - авіаційна транспортна система (комплекс)

МБ – матриця безпеки

НАССР – аналіз небезпечних чинників і критичні точки контролю

ОПР – особа, що приймає рішення

ПС - повітряне судно

РБС – рівень безпеки системи

ЦА - цивільна авіація

МО – Міністерство оборони

ТО - технічне обслуговування

ТОіР - технічне обслуговування і ремонт

ЛА - літальний апарат

АТ - авіаційна техніка

БП – безпека польотів

## РЕФЕРАТ

Пояснювальна записка до дипломної роботи: ”“Методика ідентифікації загроз та оцінки ризиків діяльності транспортної системи (комплексу) в ході некомерційної експлуатації””:

\_\_\_\_\_ с., \_\_\_\_\_ рис., \_\_\_\_\_ табл., 57 джерел

Об’єкт дослідження – загрози безпеці та ризики авіаційної транспортної системи.

Предмет дослідження – оцінка загроз та ризиків діяльності авіаційної транспортної системи (комплексу).

Методи досліджень – метод системного аналізу, елементи теорії матриць, елементи теорії множин, методи аналізу ієрархій, нечітких множин, статистичного прогнозування, експертного оцінювання, логіко-евристичний метод.

Мета дипломної роботи - розробка методичного апарату ідентифікації загроз та оцінки ризиків діяльності авіаційної транспортної системи (комплексу) в ході некомерційної експлуатації

Методи досліджень – метод системного аналізу, елементи теорії матриць, елементи теорії множин, методи аналізу ієрархій, нечітких множин, статистичного прогнозування, експертного оцінювання та логіко-евристичний метод.

Практичне значення результатів дипломної роботи: висновки й пропозиції можуть бути використані для розробки нормативних документів, що регламентують роботу суб’єктів авіатранспортної системи в умовах спеціалізованої експлуатації, а також програм технічної експлуатації повітряних суден.

Розроблено комплекс взаємопов’язаних методик, побудованих на узагальненій моделі та показниках багатокритеріального оцінювання безпеки авіаційної транспортної системи (комплексу), а також рекомендації щодо удосконалення методичної бази оцінювання загроз та ризиків в авіапідприємствах України.

**НЕКОМЕРЦІЙНА ЕКСПЛУАТАЦІЯ, АВІАЦІЙНА БЕЗПЕКА, ЗАГРОЗИ БЕЗПЕЦІ, ОЦІНЮВАННЯ ЗАГРОЗ ТА РИЗИКІВ, УПРАВЛІННЯ РИЗИКАМИ, ІДЕНТИФІКАЦІЯ ЗАГРОЗ**



## ВСТУП

**Актуальність теми.** Основним завданням України як члена Міжнародної організації цивільної авіації (ІСАО) є забезпечення безпеки цивільної авіації, приведення національної нормативно-правової бази у відповідність до стандартів та рекомендованої практики Додатка 17 "Безпека. Захист міжнародної цивільної авіації від актів незаконного втручання" до Конвенції про міжнародну цивільну авіацію, Керівництва з авіаційної безпеки [1], Політики Європейської конференції цивільної авіації (ЄКЦА) у сфері авіаційної безпеки цивільної авіації [2], а також змін в нормах українського законодавства, які відбулися з прийняттям 21 березня 2017 року № 1965-VIII Закону України "Про Державну програму авіаційної безпеки цивільної авіації" [3].

Зазначеними документами передбачено здійснення уповноваженим органом з питань цивільної авіації (Державіаслужба) та суб'єктами авіаційної діяльності оцінки загроз та ризиків авіаційної безпеки, а також запровадження і здійснення заходів авіаційної безпеки, що відповідають рівню та характеру загроз безпеці цивільної авіації.

Наявність внутрішніх та зовнішніх для України загроз потребує особливої уваги до забезпечення заходів авіаційної безпеки на об'єктах інфраструктури, зокрема, об'єктах цивільної авіації. Ці заходи мають бути адекватними рівню загрози авіаційній безпеці. З метою запровадження адекватних рівню загрози заходів авіаційної безпеки необхідно проводити постійну оцінку рівня загрози та ризику авіаційній безпеці.

Наказом Міністерства інфраструктури України "Про затвердження Інструкції з оцінки рівня загрози безпеці цивільної авіації України" [4] частково приведено процес оцінки загроз та ризиків авіаційній безпеці цивільної авіації Державіаслужбою та суб'єктами авіаційної діяльності, що задіяні у виконанні Державної програми авіаційної безпеки цивільної авіації, у відповідність до національних та міжнародних вимог шляхом впровадження єдиної методики щодо здійснення оцінки загроз та ризиків авіаційній безпеці.

Останнім часом збільшилися випадки виявлення заборонених до перевезення на борту повітряного судна предметів у пасажирів, їхній ручній поклажі та багажу, що є одним із типів загрози безпеці цивільної авіації. Так, у 2017 році заборонені до перевезення на борту повітряного судна предмети були виявлені у 1993 осіб. У 2018 році – у 2602 осіб, що на 30% більше, ніж у 2017 році. У 2019 році значення цього показника досягло 4199 осіб, що на 61 % більше, ніж у 2018 році. Тобто за три роки значення цього показника збільшилося вдвічі. Таке зростання свідчить про збільшення ймовірності вчинення акту незаконного втручання та необхідності здійснення оцінки загрози та ризику авіаційній безпеці у відповідності до міжнародних вимог [5].

Крім цього, з дати прийняття Інструкції з оцінки рівня загрози безпеці цивільної авіації України, затвердженої наказом Міністерства транспорту та зв'язку України від 11 травня 2007 року № 390/ДСК, зареєстрованим в Міністерстві юстиції України 25 травня 2007 року за № 542/13809, суттєво змінилися вимоги керівних документів ІКАО, ЄКЦА у сфері авіаційної безпеки та Державної програми авіаційної безпеки цивільної авіації. Так з 2007 року вже вийшло 3 нових видання Додатку 17 до Конвенції про міжнародну цивільну авіацію, 6 нових видань Керівництва з авіаційної безпеки (ІКАО, DOC 8973), 6 нових видань DOC 30, частина II Політика Європейської конференції цивільної авіації.

Також згідно з оцінкою ІКАО фінансові та економічні збитки від декількох нещодавно проведених терористичних атак склали 4,47 млрд доларів США, що призвело до двотижневої перерви у діяльності експлуатантів аеродромів та експлуатантів повітряних суден, відновлення інфраструктури та інших збитків. Акти незаконного втручання 11.09.2001 за оцінками ІКАО призвели до сукупних втрат у розмірі 2 трлн доларів США.

Трагічним прикладом неврахування поточного стану рівня загрози та ризиків для цивільної авіації в результаті зміни політичної ситуації на Близькому Сході, загостренням конфлікту між Сполученими Штатами Америки та Ісламською Республікою Іран, є збиття 08.01.2020 ракетою Сил протиповітряної оборони Ірану цивільного українського повітряного судна авіакомпанії "Міжнародні авіалінії

України", внаслідок якого сталася загибель 167 пасажирів та 9 членів екіпажу, які знаходилися на борту. Економічні збитки від цієї трагедії ще будуть оцінені і включатимуть прямі, непрямі, моральні, іміджеві та інші втрати.

Аналогічна авіакатастрофа, яка сталася 21.12.1988 з цивільним повітряним судном США авіакомпанії "Пан Америкен" і була вчинена спецслужбами Лівійської арабської Джамахірії, призвела до загибелі 259 пасажирів та 11 членів екіпажу, які знаходилися на борту цього повітряного судна, а також до виплат усіх компенсацій у розмірі 2,8 млрд доларів США. Ця трагедія сталася в результаті нехтування елементарних заходів авіаційної безпеки з боку авіакомпанії, що, врешті-решт, призвело до банкрутства найпотужнішого на той час авіаперевізника США та всього світу.

Також, прикладом економічних та інших збитків було збиття 17.07.2014 повітряного судна авіакомпанії "Малайзійські авіалінії", що виконував регулярний рейс МН17 над Донецькою областю, унаслідок якого загинули всі пасажирів та екіпаж (загалом 298 осіб).

Результатом нехтування та низької якості здійснення заходів авіаційної безпеки, в тому числі оцінки рівня загрози та ризиків авіаційній безпеці є створення загрози безпеці цивільної авіації та скоєння або спроби скоєння актів незаконного втручання у діяльність цивільної авіації, що, зокрема, включають:

незаконне захоплення повітряних суден;

руйнування повітряного судна, що перебуває в експлуатації;

захоплення заручників на борту повітряних суден або на аеродромах;

насильницьке проникнення на борт повітряного судна, в аеропорт або в розташування аеронавігаційного засобу чи служби;

розміщення на борту повітряного судна або в аеропорту зброї, небезпечного пристрою або матеріалу, призначених для досягнення злочинних цілей;

використання повітряного судна, що перебуває в експлуатації, з метою заподіяння каліцтва, інших ушкоджень здоров'ю, смерті фізичній особі або значної шкоди майну чи навколишньому природному середовищу.

Перераховані вище приклади свідчать про те, що наслідки неналежного виконання заходів авіаційної безпеки, зокрема, здійснення оцінки загрози та ризиків призводять до масової загибелі людей та фінансових збитків в особливо великих розмірах.

Враховуючи викладене, завдання ідентифікації загроз та оцінки ризиків діяльності транспортної системи (комплексу) є актуальним для цивільної авіації України.

**Метою дослідження** є розробка методичного апарату ідентифікації загроз та оцінки ризиків діяльності авіаційної транспортної системи (комплексу) в ході некомерційної експлуатації

**Досягнення поставленої мети передбачає розв'язання таких завдань:**

1. За результатами аналізу сучасних умов некомерційної експлуатації авіаційних транспортних систем визначити основні напрямки дослідження методів оцінювання ризиків та загроз.

2. Розробити узагальнену модель динаміки рівня безпеки авіаційної транспортної системи та визначити систему показників оцінки загроз та ризиків

3. Розробити методику визначення пріоритетів показників, що характеризують рівень безпеки авіатранспортної системи та комплексну методику оцінювання загроз і ризиків.

4. Розробити методичні рекомендації щодо оцінювання факторів ризику для безпеки польотів.

**Об'єкт дослідження** – загрози та ризики безпеки авіаційної транспортної системи.

**Предмет дослідження** – оцінка загроз та ризиків діяльності авіаційної транспортної системи (комплекса).

**Методи досліджень** – метод системного аналізу, елементи теорії матриць, елементи теорії множин, методи аналізу ієрархій, нечітких множин, статистичного прогнозування, експертного оцінювання та логіко-евристичний метод.

**Наукова новизна.** Полягає у напрацюванні взаємопов'язаних методик оцінювання загроз та ризиків, побудованих на узагальненій моделі та показниках

багатокритеріального оцінювання безпеки авіаційної транспортної системи (комплексу)

1. Розроблено онтологічну схему забезпечення авіаційної безпеки, яка дає змогу що всі ідентифікувати можливі загрози та їх джерела, визначити всі можливі уразливості та зіставити їх з відповідними джерелами загроз, всім визначеним джерелам загроз і вразливостям (факторам) поставити у відповідність певні методи їх реалізації (атаки). Це дає змогу, не змінюючи методичного інструментарію, вводити нові види джерел загроз, методи їх реалізації, уразливості, які стануть відомі в результаті подальшого отримання знань у відповідній сфері.

2. Розроблено функціональну модель забезпечення безпеки, яка надає змогу сформулювати вимоги до методичного апарату ідентифікації загроз та оцінки ризиків та на її основі удосконалено систему критеріїв і показників стану безпеки з метою їх прийнятності для розв'язання багатокритеріальних задач.

3. Удосконалено методику знаходження пріоритетів окремих показників, що визначають рівень небезпеки (загрози) та дають змогу отримувати кількісні значення пріоритетів окремих показників, що визначають рівень небезпеки (загрози) авіаційної діяльності; отримувати оціночні значення тенденції зростання (спадання) окремих показників для певного проміжку часу.

4. Розроблено методику та алгоритм оцінки загроз та ризиків АТС, які дають змогу визначати заходи протидії загрозам на підставі комплексного оцінювання результатів аналізу можливих і виявлення актуальних загроз, оцінювання можливих ризиків, що виникають внаслідок реалізації певної загрози, можливих негативних наслідків загроз, ідентифікації можливих джерел загроз, факторів, що сприяють їх прояву (уразливостей).

**До практичних значень роботи слід віднести такі результати.**

1. Запропоновані рекомендації щодо удосконалення методичної бази оцінювання загроз та ризиків в авіапідприємствах України. Визначено, що доцільно удосконалити існуючий методичний апарат у напрямках розроблення та впровадження відповідних превентивних заходів авіаційної безпеки для зниження ризику незаконного втручання до прийнятного рівня; координації та співпраці

органів державної влади щодо оцінки рівня ризиків та загроз відповідно до визначених критеріїв, а також розробки стандартизованої методики оцінки ризиків і загроз.

2. Розроблено методичні рекомендації щодо управління факторами ризику для безпеки польотів, у яких визначено заходи оцінювання ризику. Зазначено, що виявлення чинників небезпеки є першим кроком в офіційному процесі збору, обліку, використання і генерування зворотної інформації про чинники небезпеки і чинники ризику у виробничій діяльності, а також те, що джерела виявлення чинників небезпеки повинні включати три методи: реагуючий, проактивний і прогностичний.

3. Запропоновано рекомендації щодо оцінки ризику за методологією European Risk Classification Scheme (ERCS). Констатовано, що моніторинг і вимірювання показників ефективності забезпечення безпеки польотів є щонайпершою задачею забезпечення безпеки польотів. Моніторингом і вимірюванням результатів діяльності рекомендовано займатися експлуатаційному персоналу організації.

4. Розроблено рекомендації, що пов'язані з ризиками та загрозами безпеці цивільної авіації України, які спричинені збройною агресією Російської Федерації.

**Апробація.** Результати роботи опубліковані у збірнику тез виступів на XII Міжнародної науково-практичної конференції «INNOVATIONS AND PROSPECTS IN MODERN SCIENCE» 20-22 листопада 2023 року Стокгольм, Швеція [Косошов О. М., Власенко Г. М., Гладкий К. С. Багатокритеріальний алгоритм прийняття рішення в системі забезпечення інформаційної безпеки об'єктів цивільної авіації. // Innovations and prospects in modern science. Proceedings of the 12th International scientific and practical conference. SSPG Publish. Stockholm, Sweden. 2023. Pp. 250-257. URL: <https://sciconf.com.ua/xii-mizhnarodna-naukovo-praktichna-konferentsiya-innovations-andprospects-in-modern-science-20-22-11-2023-stokgolm-shvetsiya-arhiv/>].

Висновки й пропозиції можуть бути використані для розробки нормативних документів, що регламентують функціонування системи управління безпекою польотів авіатранспортної системи в умовах некомерційної експлуатації, а також програм безпеки польотів повітряних суден.

## **РОЗДІЛ 1. СУТНІСТЬ ЗАВДАННЯ ІДЕНТИФІКАЦІЇ ЗАГРОЗ ТА ОЦІНКИ РИЗИКІВ В СИСТЕМІ АВІАЦІЙНОЇ БЕЗПЕКИ**

### **1.1. Безпека на авіаційному транспорті: категоріально-правовий аналіз**

Серед важливих завдань, які вирішує цивільна авіація, забезпечення безпеки польотів займає особливе місце. З соціальної точки зору безпека польотів зачіпає перш за все право на безпеку людини. Запровадження в експлуатацію якісно нових дорогих повітряних суден великої пасажиромісткістю значно загостило її як в економічному, так і в соціальному аспектах.

У відповідь на збиття рейсу MH17 авіакомпанії Malaysia Airlines 17 липня 2014 року Міжнародна організація цивільної авіації (ІКАО) здійснила низку ініціатив, першою з яких стало проведення 29 липня 2014 року спеціальної наради високого рівня за участю Міжнародної ради аеропортів (МСА), Організації з аеронавігаційного обслуговування цивільної авіації і Міжнародної асоціації повітряного транспорту (ІАТА). На нараді було ухвалено спільну заяву, в якій висловлюється рішуче засудження застосування зброї проти цивільних літаків. У зв'язку з цим ІКАО почала приділяти значну увагу питанням, пов'язаним з безпекою цивільної авіації та безпекою польотів цивільних повітряних суден у повітряному просторі над зонами конфліктів або поблизу них [8].

Під час розгляду ризиків, пов'язаних із польотами над зонами збройних конфліктів або поблизу них, а також у контексті воєнного стану, оголошеного в Україні, найбільш важливим фактором вважається пряма загроза галузі цивільної авіації. Імовірність загрози, що виникає внаслідок наміру та можливості нападу на цивільне повітряне судно над зоною конфлікту або поблизу неї, є ключовим фактором оцінки ризику та попередньою умовою для визначення заходів з пом'якшення наслідків, які необхідно застосувати. Будь-які заходи щодо зниження вразливості мають бути вжиті до того, як повітряне судно досягне зони конфлікту, тому одним із ключових чинників

є розуміння конкретної загрози на початковому етапі польоту. Таким чином, необхідно в пріоритетному порядку зосередитися на початковій оцінці загрози, яка передбачає збір відповідної інформації з усіх доступних джерел, включно з інформацією правоохоронних органів та інших державних органів, що відповідають за безпеку. Такого роду інформація, що відображає конкретні військові можливості, є основним джерелом для виявлення небезпек, що становлять ризик для цивільної авіації. Отримана таким чином інформація, що стосується наявних загроз і небезпек, є цінним внеском у процес оцінки ризиків, який стає надійною підставою для прийняття рішень щодо ймовірності подальшого продовження польотів цивільних повітряних суден над зонами збройних конфліктів або поблизу них, а також в умовах воєнного стану [9].

Участь держави в процесі оцінки ризиків і прийняття рішень для визначення прийняттого рівня ризику може здійснюватися з певними варіаціями. Наприклад, одна держава може взагалі не брати участі в такому процесі. Інша держава, навпаки, може встановлювати правила, що обмежують або забороняють певні операції. Крім того, існують відмінності в тому, як держави розкривають відповідну інформацію про оцінку ризиків.

Обсяг інформації та методи її поширення значною мірою залежать від здатності держави збирати, обробляти й аналізувати відповідну інформацію, а також від її юридичних повноважень і обов'язків щодо видання заборонних і обмежувальних нормативних актів.

За даними Міжнародної організації цивільної авіації, відносні показники рівня безпеки польотів у вітчизняній галузі цивільної авіації значно гірші від середніх загальносвітових показників. Проблема безпеки перевезень авіаційним транспортом дуже важлива, тому що вона пов'язана із значними збитками соціального та економічного характеру. Моральні збитки у зв'язку з травматизмом чи загибеллю людей, втрата іміджу авіатранспортних підприємств, втрата підготовлених фахівців і необхідність їх заміни в суспільстві, економічні збитки, пов'язані з необхідністю



відшкодувань наслідків авіаподій, розробка та реалізація заходів із запобігання причин транспортних подій та інше – являють собою складові цих втрат. При цьому безпека повітряного транспорту стосується не тільки безпеки пасажирів. Це поняття стосується і безпеки транспортників, населення в зоні можливих авіаподій, вантажів, транспортних засобів та споруд, довкілля, які можуть постраждати внаслідок авіаційних подій.

Питання забезпечення безпеки польотів залишалися і залишатимуться актуальними, поки експлуатуються літальні апарати самого різного призначення, зокрема, і повітряні судна цивільної авіації. Відбувається постійне вдосконалення конструкції повітряних суден, методів і способів їх експлуатації, підготовки екіпажів, проблеми льотної придатності, живучості повітряних суден, безпеки повітряного руху, що постійно залишається у полі зору представників експлуатуючих підприємств і наукових установ. Дані процеси найгостріше позначають проблему браку нових способів управління процесами забезпечення безпеки польотів, визначення загроз та відповідних джерел небезпеки авіаперевезень, а відтак продовжуватимуть ставати все більш актуальними [10, с.85]. За таких умов нагальною є потреба у розробці нового переліку критеріїв (показників) безпеки польотів на авіаційному транспорті та його законодавчого закріплення. Неабиякої важливості вивченню цієї проблеми додає й той факт, що сьогодні в діючому законодавстві України та в юридичній науковій літературі відсутнє єдине загальновизнане визначення безпеки польотів.

Розв'язання цього завдання дозволить визначити безпеку польотів на авіаційному транспорті та конкретизувати її місце серед інших складових транспортної безпеки країни.

Загострення ситуації пов'язане з відсутністю налагодженої системи забезпечення безпеки польотів, з низькою результативністю здійснення покладених на неї задач і функцій, зі зниженням рівня наукового і технічного супроводу зазначеної діяльності. Цьому сприяє складність і невивченість характеру й особливостей соціальних взаємозв'язків, що складаються між різними категоріями

учасників суспільних відносин у процесі створення й збереження стійкого техногенно-безпечного стану на об'єктах забезпечення безпеки авіації. Сукупність такого роду факторів дозволяє розглядати безпеку польотів на авіаційному транспорті в сучасних умовах як одну з найголовніших цілей і невід'ємну умову ефективного функціонування як всієї транспортної системи країни взагалі, так і авіаційного комплексу зокрема. Безпеку польотів слід розглядати як одну з найважливіших характеристик, що показує ступінь стійкості соціальних взаємозв'язків, що визначає загальнолюдську цінність і значимість суспільних відносин.

Розглядаючи безпеку польотів, необхідно передусім зупинитися на етимологічному визначенні поняття «безпека». Так, під безпекою розуміють «стан, коли кому-, чомунебудь ніщо не загрожує» [11, с.115], або «відсутність небезпеки, схоронність, надійність» [12, с.167], а також «становище якому загрожує небезпека комусь, чомусь» [13, с.38], «стан захищеності» [14, с.207]. Нормативні джерела визначають термін «безпека» як «відсутність неприпустимого ризику, пов'язаного з можливістю завдання будь-якої шкоди» [15, с.3]. На думку вчених безпека являє собою сукупність опосередкованих джерелами підвищеної небезпеки відносин, які регулюються юридичними, технічними та організаційними нормами з метою запобігання та усунення загрози життю і здоров'ю людей, матеріальним цінностям та зовнішньому середовищу [16, с.21].

Поняття «безпека» відповідно до етимології цього слова, означає «відсутність небезпеки», тобто відсутність яких-небудь загроз. Небезпечний та безпечний – стани, протилежні один одному. З іншого боку під безпекою розуміють стан загрози, можливість заподіяння шкоди, нещастя, кому-небудь, чомунебудь [13, с.338]. Під загрозою розуміють «можливість, або неминучість виникнення чогось небезпечного, прикрого. Те, що може заподіяти якесь зло, неприємність» [4, с.115]. Безпека і загроза заподіяння шкоди – поняття, близькі за значенням.

Законодавець не дає визначення загрозам стану безпеки польотів, не називає джерел небезпеки, які загрожують цьому стану, але вказує на фактори – як суттєві

обставини, які впливають на виникнення небезпечної ситуації (ризик). При цьому ним виділяються фактори безпосередні (обставини, котрі безпосередньо призвели до авіаційної події і пов'язані з помилками екіпажу або відмовами техніки), супутні (обставини, котрі сприяли негативному розвитку особливої ситуації в польоті) та головні (обставини, пов'язані з недоліками в організації та управлінні діяльністю авіації, ергономічними і конструктивно-виробничими недоліками повітряних суден) [10].

Розглядаючи безпеку повітряного транспорту, зауважимо, що вона є складовою явища більш загального характеру. Зокрема, в науковій літературі з цього приводу є декілька термінів, що характеризують безпеку: транспортна безпека, безпека на транспорті, безпека транспорту та ін. Серед них найбільшу популярність отримало саме поняття «транспортна безпека». На думку деяких вчених, «транспортна безпека – властивість людиномашинною системи зберігати при функціонуванні такі стани, при яких з високою вірогідністю виключаються техногенні події, а збиток від неминучих енергетичних і шкідливих матеріальних викидів не перевищує допустимого рівня» [11]. Під системою забезпечення транспортної безпеки П.Г. Белов пропонує розуміти «сукупність взаємопов'язаних нормативно-розпорядчих документів, організаційно-технічних та інших заходів, а також відповідаючих ним сил і засобів, призначених для попередження і зниження тих побічних витрат, які обумовлені реально існуючими на транспорті небезпеками» [11].

З точки зору принципу причинності, який передбачає встановлення взаємозв'язку між причинами і наслідками подій та явищ, поняття транспортної безпеки (безпеки транспортування) має три складові: безпечне транспортування пасажирів та вантажів завдяки забезпеченню надійності транспортних засобів і споруд, виконанню всіх передбачених технологічних процесів, пов'язаних з роботою транспорту; захист процесу транспортування та транспортних підприємств від проявів протидії, провокацій та тероризму; захист довкілля у зв'язку із функціонуванням транспортних підприємств.

Тобто транспортна безпека (безпека на транспорті) – поняття широке, воно стосується не тільки безпеки перевезень, але й безпеки всіх технологічних процесів транспортних галузей, в тому числі й економічної, та авіаційної безпеки. Вона спрямована на захист: пасажирів, власників, отримувачів і перевізників вантажів як осіб, що безпосередньо споживають або створюють транспортний продукт; власників транспортних засобів і осіб, що його фрахтують; транспортного комплексу, включаючи інфраструктуру та працівників; економічний стан країни, включаючи бюджети всіх рівнів; екологічний стан оточуючого середовища [12].

Таким чином, транспортна безпека фактично складається з підсистем, що характеризують стан безпеки на різних видах транспорту. В досліджуваній сфері не можна ототожнювати безпеку польотів, наприклад, з більш широким поняттям як безпека на авіаційному транспорті. Останнє включає разом з безпекою польотів також авіаційну, економічну та ін. безпеки.

Найбільш поширеним у законодавстві є визначення авіаційної безпеки, під якою розуміється комплекс заходів, а також людські та матеріальні ресурси, призначені для захисту цивільної авіації від актів незаконного втручання в її діяльність [13]. З іншого боку у Тимчасових правилах контролю з метою забезпечення безпеки цивільної авіації, затверджених Постановою Кабінету Міністрів України від 02.08.1995 р. № 592, безпека (авіаційна безпека) – комплекс заходів щодо захисту цивільної авіації від актів незаконного втручання, інших протиправних посягань, а також людські та матеріальні ресурси, призначені для виконання цих заходів [14]. Як бачимо у цьому визначенні авіаційну безпеку законодавець трактує більш широко, маючи на увазі захист цивільної авіації не тільки від актів незаконного втручання, але й інших протиправних посягань.

Чинне законодавство також містить визначення «безпека авіації» як комплексної властивості авіаційної транспортної системи виконувати свої функції без завдання збитків (чи з мінімальними збитками) самій системі або населенню, в інтересах якого вона розвивається [15]. Зазначене визначення є ще більш об'ємним,

оскільки включає, на нашу думку, і авіаційну безпеку, і безпеку польотів. Підтвердженням тому є Концепція розвитку цивільної авіації України, згідно якої забезпечення безпеки цивільної авіації – комплексний процес, який передбачає забезпечення безпеки польотів, захист цивільної авіації від актів незаконного втручання (авіаційну безпеку) та захист навколишнього середовища від шкідливого впливу з боку авіації (екологічну безпеку) [16]. Серед інших складових безпеки цивільної авіації категорію «безпека польотів» можна вважати визначальною, оскільки вона є пріоритетом діяльності авіаційного транспорту і невід’ємною складовою національної безпеки [17].

## **1.2. Загальна характеристика загроз та ризиків у системі управління авіаційною безпекою**

Система управління безпекою – це сукупність заходів із застосування єдиного підходу до управління безпекою польотів, що передбачає оптимізацію організаційної структури, розподіл відповідальності між органами державної влади та суб’єктами авіаційної діяльності, визначення політики та експлуатаційних процедур щодо забезпечення безпеки польотів. В основі управління безпекою польотів лежить системний підхід до виявлення і усунення джерел небезпеки та здійснення контролю за ризиками для забезпечення безпеки польотів з метою мінімізації людських втрат, матеріальних, фінансових, екологічних та соціальних збитків [17].

Аналіз основ забезпечення авіаційної безпеки дає змогу зробити висновок про те, що поняття “забезпечення авіаційної безпеки” включає об’єкти авіаційної безпеки, загрози об’єктам авіаційної безпеки та діяльність щодо захисту цих об’єктів, засновану на сукупності сил, засобів, способів і методів забезпечення авіаційної безпеки.

Головними цілями діяльності із забезпечення авіаційної безпеки є попередження, уникнення та ліквідація загроз об'єктам авіаційної безпеки та мінімізація можливого збитку, завданого внаслідок реалізації цих загроз.

Загроза – одне із ключових понять у сфері забезпечення авіаційної безпеки.

Загроза об'єкту авіаційної безпеки – сукупність факторів і умов, що виникають у процесі взаємодії різних об'єктів (їх елементів), здатних впливати на конкретний об'єкт авіаційної безпеки. Негативні впливи розрізняються за характером завданої шкоди, а саме: за ступенем зміни властивостей об'єкта безпеки та можливістю ліквідації наслідків прояву загрози.

До найбільш важливих властивостей загрози відносяться: вибірковість, передбачуваність і шкідливість. Вибірковість характеризує націленість загрози на завдання шкоди тим чи іншим конкретним властивостям об'єкта безпеки. Передбачуваність характеризує наявність ознак виникнення загрози, що дають змогу заздалегідь прогнозувати можливість появи загрози та визначати конкретні об'єкти безпеки, на які вона буде спрямована. Шкідливість характеризує можливість завдання шкоди різного виміру об'єкту безпеки. Шкода, як правило, може бути оцінена вартістю витрат на ліквідацію наслідків прояву загрози або на запобігання її появи.

Необхідно виділити два найбільш важливі типи загроз:

1. Намір завдати шкоди, що з'являється у вигляді наявного мотиву діяльності суб'єкта (акт незаконного втручання (АНВ), несанкціоноване перевезення небезпечних речовин тощо);

2. Можливість завдання шкоди – існування достатніх для цього умов і факторів.

Особливість першого типу загроз полягає в невизначеності можливих наслідків, неясності питання про наявність у загрозового суб'єкта сил і засобів, достатніх для здійснення наміру.

Можливість завдання шкоди полягає в існуванні достатніх для цього умов і факторів. Особливість загроз цього типу полягає в тому, що оцінити потенціал

сукупності факторів, які можуть слугувати перетворенню цих можливостей і умов на шкоду, можуть тільки суб'єкти загроз.

Між загрозою та небезпекою завдання шкоди завжди існує стійкий причинно-наслідковий зв'язок. Загроза завжди породжує небезпеку. Небезпеку також можна подати як стан, в якому перебуває об'єкт безпеки внаслідок виникнення йому загрози. Головна відмінність між ними полягає в тому, що небезпека є властивістю об'єкта авіаційної безпеки та характеризує його здатність протистояти прояву загроз, а загроза – властивістю об'єкта взаємодії або елементів, що перебувають у взаємодії, об'єкта безпеки, які виступають як джерело загроз. Поняття загрози має причинно-наслідковий зв'язок не тільки з поняттям небезпеки, але й з можливою шкодою, як наслідком негативної зміни умов існування об'єкта. Можлива шкода визначає величину небезпеки.

Опираючись на уведені вище поняття (п.1.2), можна побудувати таку онтологічну схему забезпечення авіаційної безпеки (рис.1.1).

Суб'єкти авіаційної діяльності (джерело, власник або користувач інформації) визначають множину авіаційних ресурсів, які повинні бути захищені від різного роду атак. До активів АТС зазвичай відносять: матеріальні ресурси; авіаційні ресурси (аналітична, службова, керівна інформація на всіх етапах свого життєвого циклу: створення, обробка, зберігання, передача, знищення); авіаційні технологічні процеси життєвого циклу автоматизованих систем; надані авіаційні послуги тощо [22].

Атаки є результатом реалізації загроз, здійснюються через різні уразливості в захисті і мають імовірність реалізації (ризик атаки).

У результаті аналізу вразливостей, властивостей джерел загроз (природи виникнення, характеру, відношення до об'єктів АТС) і ймовірностей їх можливої реалізації в конкретному оточенні, визначаються ризики для цього набору об'єктів. Це, у свою чергу, дає змогу визначити стратегію протидії, що є політикою безпеки.

Вироблена суб'єктом авіаційної діяльності стратегія протидії може передбачати для кожної із загроз одну з можливих ліній поведіння: спробу ліквідації джерела

загрози, ухилення від загрози, прийняття загрози, мінімізація збитку від атаки, викликаного цією загрозою, за допомогою сервісів і механізмів безпеки. При цьому слід враховувати, що окремі уразливості можуть зберегтися й після застосування заходів безпеки.

Процес забезпечення безпеки інформації має бути комплексним і ґрунтуватися на глибокому аналізі можливих негативних наслідків (логіко-евристичний аналіз). Такий аналіз припускає обов'язкову ідентифікацію можливих джерел загроз, факторів, що сприяють їхньому прояву (уразливостей) і, як наслідок, визначення актуальних загроз безпеці інформації.

Виходячи з такого принципу, моделювати й класифікувати джерела загроз, самі загрози та їх прояви, а також розробляти ефективні заходи протидії доцільно на основі аналізу взаємодії логічного ланцюжка: Джерело загрози → Загроза → Уразливість → Реалізація загрози (атака) → Наслідки (збиток) → Заходи протидії.



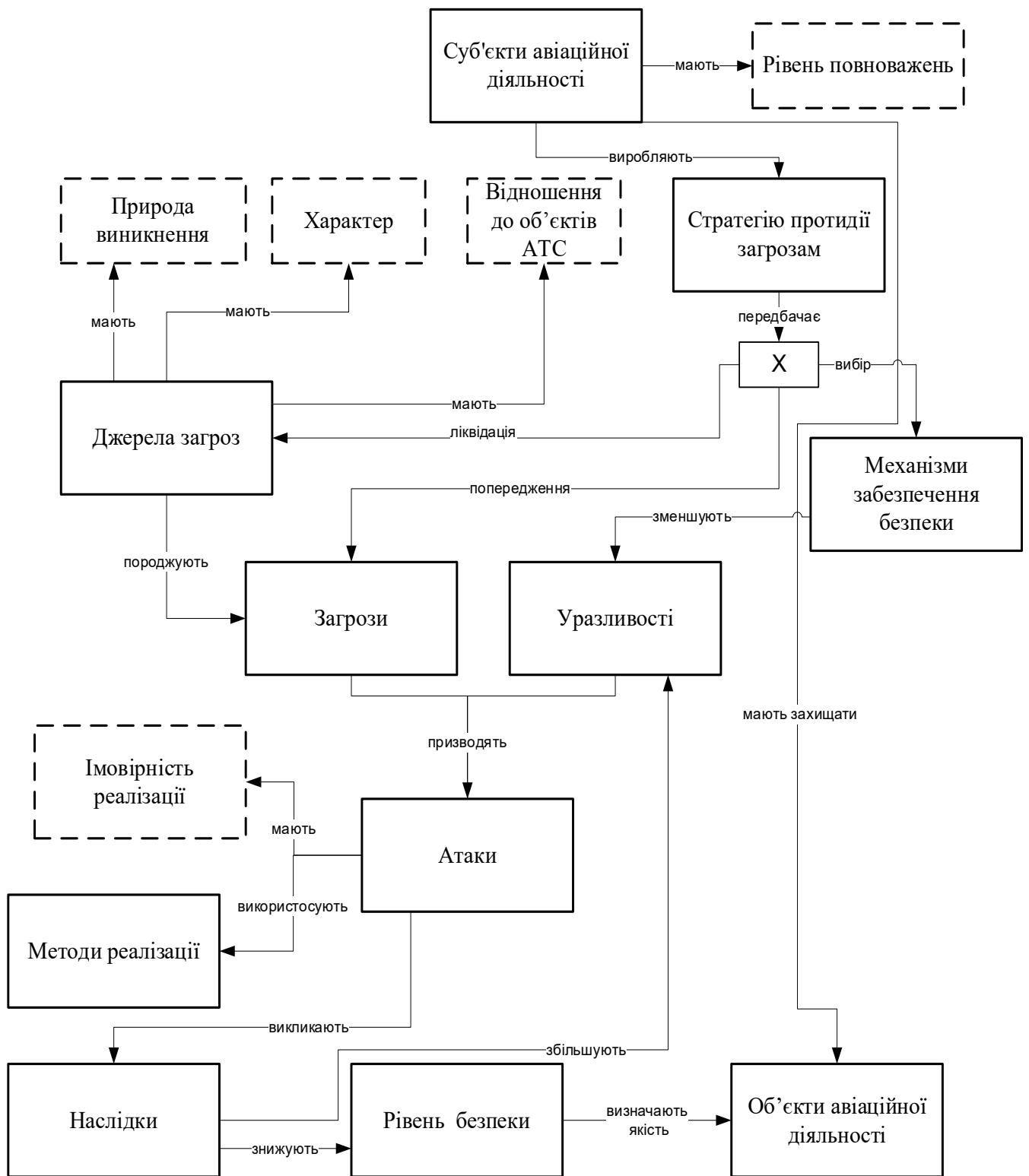


Рис. 1.1 – Онтологічна схема забезпечення авіаційної безпеки

У ході аналізу необхідно переконатися, що всі можливі загрози та їх джерела ідентифіковані, всі можливі уразливості ідентифіковані та зіставлені з відповідними

джерелами загроз, всім визначеним джерелам загроз і уразливостям (факторам) відповідають певні методи реалізації.

При цьому важливо мати змогу, в разі потреби, не змінюючи методичного інструментарію, вводити нові види джерел загроз, методи їх реалізації, уразливості, які стануть відомі в результаті подальшого отримання знань у цій сфері.

Отже, аналіз негативних наслідків реалізації загроз припускає обов'язкову ідентифікацію (наприклад, присвоєння унікального коду) загроз, можливих джерел загроз, уразливостей, що сприяють їх прояву, та методів реалізації.

У науковій літературі запропоновано ряд класифікацій загроз безпеці, що відображає ті чи інші аспекти розглянутої проблеми [23 – 27].

Морфологічний аналіз показує, що можна виділити такі основні складові загрози авіаційній безпеці: джерело впливу на авіаційну систему, спосіб впливу, об'єкти впливу, а також результат впливу (завданий збиток).

Ці елементи для класифікації можуть бути обрані як базові класифікаційні ознаки з метою подальшої їхньої декомпозиції.

Фактори, що впливають на інформаційну безпеку, можна розподілити за ознакою відношення до природи їхнього виникнення – на об'єктивні та суб'єктивні, стосовно об'єктів інформаційної системи – на внутрішні та зовнішні.

Розподіл джерел на суб'єктивні та об'єктивні обґрунтований необхідністю виходити з міркувань щодо визначення провини за завданий збиток інформації, а розподіл на внутрішні й зовнішні джерела обґрунтований тим, що для однієї й тієї ж загрози методи протидії зовнішнім і внутрішнім джерелам можуть бути різними.

Крім того, і зовнішні, і внутрішні джерела можуть носити як навмисний, так і ненавмисний характер.

Ненавмисні загрози виникають незалежно від волі та бажання людей. Цей тип загроз пов'язаний найчастіше із прямим природним або техногенним фізичним впливом на елементи інформаційної системи та веде до порушення роботи цієї

системи або її фізичного знищення, пошкодження носіїв інформації, засобів обробки й передачі даних, телекомунікаційних каналів.

Причиною виникнення загроз ненавмисного характеру можуть бути як відмови внаслідок конкретних помилок персоналу та прямих дій інших осіб (наприклад, пошкодження кабельної лінії зв'язку під час проведення будівельних робіт), так і випадкові порушення в роботі системи (наприклад, внаслідок поломки устаткування, збою в роботі програмного забезпечення тощо).

Навмисні загрози, на відміну від ненавмисних, можуть бути створені тільки людьми, що діють цілеспрямовано з метою дезорганізувати роботу інформаційної системи. Навмисні загрози, у свою чергу, розподіляються на пасивні й активні.

**Загальне оцінювання ризику** – це спільний процес ідентифікування ризику, аналізування ризику та оцінювання ризику.

Загальне оцінювання ризику можна провадити на рівні організації, на рівні підрозділів, стосовно проектів, окремих видів діяльності або конкретних ризиків. Різним оточенням можуть відповідати різні засоби та методики.

Загальне оцінювання ризику забезпечує розуміння ризиків, їхніх причин, наслідків і їхніх імовірностей. Воно зазначає вхідні дані для прийняття рішень щодо:

- необхідності розпочинати певну діяльність;
- способів максимізування можливостей;
- потреби обробляти ризики;
- вибирання серед варіантів з різними ризиками;
- устанавлення пріоритетності варіантів обробляння ризику;
- вибору найбільш відповідних стратегій обробляння ризиків, які зменшуватимуть несприятливі ризики до допустимого рівня.

**Оброблення ризику.** Після завершення загального оцінювання ризику провадять обробляння ризику, яке передбачає вибір та погоджування одного чи кількох прийнятних варіантів, що дають змогу змінити ймовірність виникнення ризиків, впливи ризиків або й те і друге, а також запровадження цих варіантів.

Після цього етапу виконують циклічне повторне загальне оцінювання нового рівня ризику задля визначення його допущеності за попередньо встановленими критеріями з тим, щоб прийняти рішення щодо потреби подальшого додаткового оброблення.

**Моніторинг і критичне аналізування.** Як частину процесу керування ризиком треба регулярно здійснювати моніторинг і критичне аналізування ризиків і засобів контролю для перевірки того, що

- припущення щодо ризиків й надалі чинні;
- припущення, на яких базується загальне оцінювання ризику (зокрема, зовнішнє та внутрішнє оточення) й надалі чинні;
- очікуваних результатів досягають;
- результати загального оцінювання ризику узгоджуються з наявним досвідом;
- методики загального оцінювання ризику належно застосовують;
- заходи щодо оброблення ризиків є результативні.

Загальне оцінювання ризику дає змогу тим, хто приймає рішення, а також відповідальним сторонам краще розуміти ризики, які можуть впливати на досягнення цілей, адекватність та результативність запроваджених засобів контролювання. Це забезпечує основу для прийняття рішень щодо найбільш відповідного підходу до оброблення ризиків. Вихідні дані загального оцінювання ризику – це вхідні дані для процесів прийняття рішень в організації.

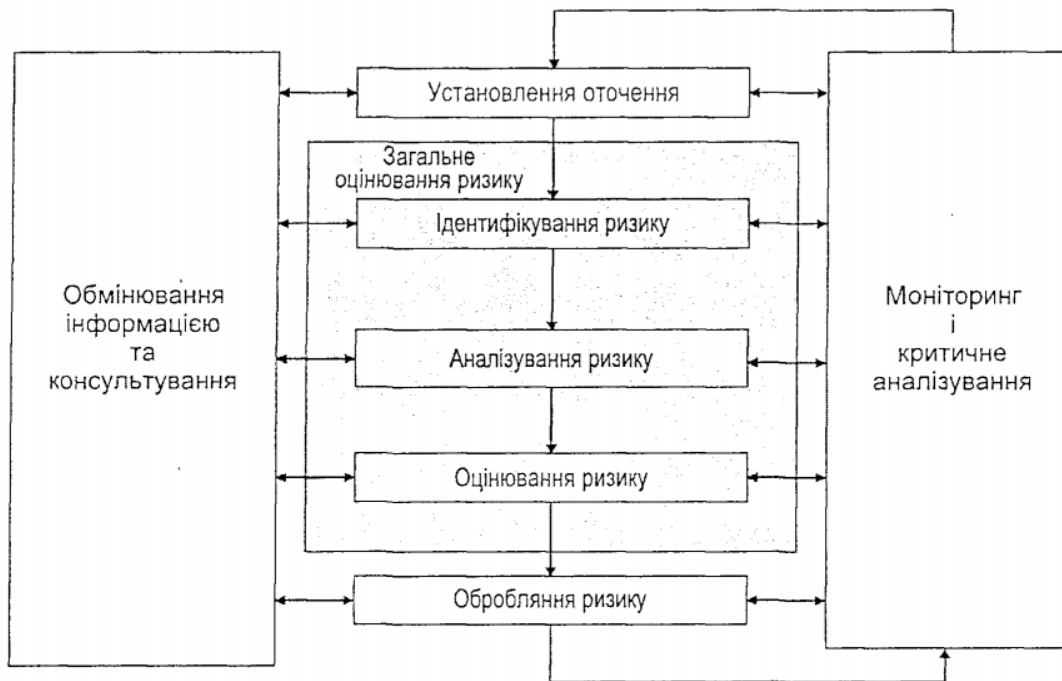


Рисунок 1 – Внесок загального оцінювання ризику до процесу керування ризиком

**Загальне оцінювання ризику** – це спільний процес ідентифікування ризику, аналізування ризику та оцінювання ризику (див. рисунок 1). Спосіб застосування цього процесу залежить не лише від оточення процесу керування ризиком, але також від методів і методик, використовуваних для загального оцінювання ризику.

Для загального оцінювання ризику може бути потрібно застосувати багатодисциплінарний підхід, оскільки ризики можуть охоплювати широкий діапазон причин і наслідків.

### **Ідентифікація ризику**

Ідентифікація ризику – це процес виявлення, усвідомлення та реєстрування ризиків.

Мета ідентифікації ризику – визначити, що може статися, або які можуть виникнути ситуації, що можуть впливати на досягнення цілей системи чи організації. Після того, як ризик ідентифіковано, організація має визначити будь-які наявні засоби контролювання, зокрема стосовно конструктивних особливостей, персоналу, процесів і систем.

Процес ідентифікації ризику охоплює визначення причин і джерела ризику (небезпеки в контексті фізичної шкоди), подій, ситуацій або обставин, які можуть чинити матеріальний вплив на досягнення цілей, а також визначення характеру цього впливу.

Методами ідентифікації ризику можуть бути:

- доказові методи, наприклад, застосування переліків контрольних запитань і критичне аналізування хронологічних даних;
- системні методи групової роботи, коли група експертів систематично ідентифікує ризики за допомогою структурованого набору навідних фраз або запитань;
- методи індуктивного мислення, наприклад, НА70Р.

Щоб поліпшити точність і повноту ідентифікування ризику, можна використовувати різноманітні допоміжні методи, зокрема «мозкову атаку» та метод Дельфі.

Незалежно від фактично застосованих методів під час ідентифікації ризику особливу увагу важливо приділяти людським та організаційним чинникам. Тому під час процесу ідентифікації ризику треба враховувати відхилення людських і організаційних чинників від очікуваних станів, а також події, пов'язані з технічними та програмними засобами.

**Аналіз ризику**

Ризик аналізують для того, щоб поглибити розуміння ризику. Воно дає змогу отримувати вхідні дані для загального оцінювання ризику і прийняття рішень щодо потреби оброблення ризику та щодо найбільш відповідних стратегій і методів оброблення.

Аналізу ризику полягає у визначанні наслідків і їхніх імовірностей стосовно ідентифікованих ризикових подій, урахування наявності (чи відсутності) і результативності будь-яких наявних засобів контролювання. Потім наслідки та їхні ймовірності поєднують, щоб визначити рівень ризику.

Аналіз ризику передбачає розглядання причин і джерел ризику, їхніх наслідків та ймовірностей виникнення цих наслідків. Треба визначити чинники, що впливають на наслідки і ймовірність.

Подія може мати багато наслідків і може впливати на багато цілей. Треба враховувати наявні засоби контролювання та їхню результативність. Різноманітні методи цього аналізування описано в наступному підрозділі. У складних випадках може бути потрібно застосувати кілька методів.

Аналіз ризику, зазвичай, передбачає кількісне оцінювання низки потенційних наслідків, які можуть виникати за настання події, ситуації чи обставини, а також пов'язаних з ними ймовірностей з тим, щоб виміряти рівень ризику. Однак, у деяких випадках, наприклад, коли наслідки незначні чи коли очікувана ймовірність надзвичайно низька, для прийняття рішення може бути достатньо оцінки лише одного параметра.

За деяких обставин наслідок може бути результатом низки різних подій чи умов або того, що конкретну подію не ідентифіковано. У такому разі загальне оцінювання ризику зосереджують на аналізі важливості та вразливості елементів системи з тим, щоб визначити види оброблення ризику, пов'язані з рівнями захисту чи стратегіями відновлювання.

Методи, використовувані під час аналізування ризику, можуть бути якісними, напівкількісними чи кількісними. Необхідний ступінь докладності залежить від конкретного випадку застосування, наявності вірогідних даних і потреб організації щодо прийняття рішень. Деякі методи та ступінь докладності аналізу може бути прописано в законодавстві.

Якісне загальне оцінювання дає змогу позначити наслідок, імовірність і рівень ризику такими термінами щодо рівня значущості, як «високий», «середній» та «низький», поєднати наслідок та ймовірність і оцінити рівень ризику, який впливає з цього, відповідно до якісних критеріїв.

Напівкількісні методи передбачають застосування числових шкал оцінювання наслідків і ймовірностей та їх поєднання, щоб отримати рівень ризику за деякою формулою. Шкали можуть бути лінійними чи логарифмічними, або можуть мати якийсь інший взаємозв'язок; використовувані формули також можуть різнитися.

Під час кількісного аналізування оцінюють практичне значення наслідків і їхніх імовірностей, а також обчислюють значення рівня ризику в конкретних одиницях, визначених під час установлювання оточення. Повне кількісне аналізування не завжди може бути можливе чи слушне через недостатність інформації про аналізуванні системи чи діяльність, нестачу даних, вплив людських чинників тощо або тому, що витрати на кількісне аналізування неокупні чи потрібні. За таких обставин ефективним може бути порівняльне напівкількісне чи якісне ранжування ризиків із залученням спеціалістів, визнаних у відповідних галузях.

У разі кількісного аналізу треба чітко пояснити всі використовувані терміни та протоколювати основу для всіх критеріїв.

Навіть якщо проведено повне кількісне аналізування, потрібно визнавати, що обчислені рівні ризику є лише його оцінками. Треба бути уважним для забезпечення впевненості в тому, що їм не визначено рівень точності, несумісний з точністю використовуваних даних і методів аналізу.

Рівні ризику треба подавати в термінах, найпридатніших для цього типу ризику, та у формі, що сприяє оцінюванню ризику. У деяких випадках величину ризику може бути подано як розподілення ймовірності за діапазоном наслідків.

Рівень ризику залежить від адекватності та результативності наявних засобів контролю. Щоб з'ясувати це, треба відповісти на такі запитання:

- які засоби контролювання, пов'язані з конкретним ризиком, наявні?
- чи уможливають ці засоби контролювання адекватне оброблення ризику так, щоб підтримувати його на допустимому рівні?
- чи функціують на практиці засоби контролювання так, як передбачено, і чи можна, за потреби, продемонструвати їхню результативність?



Упевнено відповісти на ці запитання можна тільки за наявності належної документації та запровадження відповідних процесів забезпечення.

Рівень результативності конкретного засобу контролювання чи низки відповідних засобів контролю може бути подано якісно, напівкількісно чи кількісно. У багатьох випадках високий рівень точності не є виправданим. Однак може бути корисно подавати та протоколювати міру результативності контролю ризику так, щоб можна було скласти думку про те, на що доцільніше спрямовувати зусилля: на поліпшення засобу контролювання чи на забезпечення іншого оброблення ризику.

### **Аналіз наслідків.**

Аналізування наслідків дає змогу визначати характер і тип впливу, який може виникати, за припущення, що відбуваються конкретні події чи настають конкретні обставини. Подія може чинити низку впливів різної величини та позначатися на низці різних цілей і різних зацікавлених сторін. Типи наслідків, які треба аналізувати, і зацікавлені сторони, на яких вони позначаються, визначають під час установа оточення.

Аналіз наслідків може змінюватися від простого описування результатів до докладного кількісного моделювання чи аналізування вразливості.

Наслідок впливів може бути незначний, але з великою ймовірністю, або він може бути значний, але з малою ймовірністю, або може бути якийсь проміжний випадок. У деяких випадках доцільно робити наголос на ризиках з потенційно дуже змінюваними рівнями, оскільки часто саме вони є предметом особливої уваги з боку керівництва. В інших випадках може бути важливим аналізувати ризики зі значними та незначними наслідками окремо. Наприклад, часта (або постійна), але з незначним впливом проблема може мати значні сумарні чи довготривалі ефекти. Крім того, дії з оброблення, застосовувані до цих двох різних видів ризиків, часто суттєво різняться, отже, їх доцільно аналізувати окремо.

Аналіз наслідків може охоплювати

- розгляд наявних засобів контролювання для інтерпретації наслідків разом зі всіма відповідними спричинювальними чинниками, що позначаються на наслідках;
- зіставлення наслідків ризику і початкових цілей;
- розгляд як безпосередніх наслідків, так і тих, що можуть виникати в подальшому, якщо це узгоджується зі сферою загального оцінювання;
- розгляд вторинних наслідків, наприклад тих, що впливають на відповідно пов'язані системи, види діяльності, устаткування чи організації.

### **Аналіз правдоподібності та кількісне оцінювання ймовірності.**

Для кількісного оцінювання ймовірності зазвичай застосовують три загальні підходи, які можна застосовувати окремо або спільно:

а) використання відповідних хронологічних даних, щоб ідентифікувати події чи ситуації, які виникали у минулому, і завдяки цьому мати змогу екстраполювати ймовірність їх виникнення в майбутньому. Треба, щоб використовувані дані відповідали розглядуваному типу системи, устаткування, організації чи діяльності, а також стандартам функціонування цієї організації. Якщо так склалося, що частота виникнення дуже низька, тоді будь-яка оцінка ймовірності буде дуже невизначеною. Це особливо стосується випадків, коли подія, ситуація чи обставина ніколи не виникали та ніхто не може припустити, що вони не виникнуть у майбутньому;

б) прогнозування ймовірності з використанням прогнозних методів, наприклад, аналізування дерева відмов і аналізування дерева подій (див. додаток В). Якщо хронологічних даних немає чи вони неадекватні, то ймовірність необхідно визначити, аналізуючи систему, діяльність, устаткування чи організацію, а також пов'язані з ними відмови чи справні стани. Числові дані стосовно устаткування, персоналу, організацій і систем, отримані з практичного досвіду чи опублікованих джерел даних, потім об'єднують, щоб отримати оцінку ймовірності кінцевої події. Використовуючи прогнозні методи, важливо забезпечити, щоб під час аналізування було належним чином ураховано можливість виникнення загальної відмови за одночасної відмови кількох різних частин або складників системи, зумовлених

однією причиною. Для визначання ймовірності відмов устаткування чи конструкції внаслідок старіння чи інших процесів погіршення можуть бути потрібні методи імітаційного моделювання, базовані на обчислюванні впливів невизначеностей;

в) для кількісного оцінювання ймовірності під час регулярного та структурованого процесу можна використовувати експертні висновки. Експертні судження мають ґрунтуватись на всій наявній відповідній інформації, охоплюючи хронологічні дані, специфічну для системи та організації інформацію, експериментальні дані та проектно-конструкторську документацію тощо. Є низка формальних методів отримання експертних суджень, які допомагають формулювати доречні запитання, наприклад такі: метод Дельфі, методи парних порівнянь, ранжування за категоріями та експертного оцінювання абсолютної ймовірності.

### **Попередній аналіз**

Ризики можна ранжувати з тим, щоб визначити найзначніші ризики або вилучити з подальшого аналізування менш значні чи мінімальні ризики. Ціль полягає в тому, щоб забезпечити зосередження ресурсів на найважливіших ризиках. Однак треба дбати про те, щоб не відкинути низькі ризики, які виникають часто і мають значний сумарний ефект.

Ранжування треба базувати на критеріях, визначених для оточення. Попереднє аналізування дає змогу вибрати одну чи кілька з таких дій:

- прийняти рішення обробляти ризики без подальшого загального оцінювання;
- відхилити незначні ризики, оброблення яких недоцільне;
- вдатися до докладнішого загального оцінювання.

Початкові припущення та результати має бути задокументовано.

### **Невизначеності та чутливості**

З аналізуванням ризику часто пов'язано значні невизначеності. Розуміння невизначеностей не обхідне для того, щоб належним чином інтерпретувати результати аналізування ризиків і обмінювати ся інформацією про них. Аналізування

невизначеностей, пов'язаних з даними, методами та моделями, використовуваними для ідентифікації й аналізування ризиків, відіграє важливу роль в їх застосуванні. Аналізування невизначеності передбачає визначення відхилу або неточності результатів унаслідок сукупного змінення параметрів і припущень, використовуваних для визначення результатів.

З аналізом невизначеності значною мірою пов'язаний **аналіз чутливості**.

Аналіз чутливості передбачає визначення розміру та значення величини ризику, пов'язаних зі змінами в окремих вхідних параметрах. Його використовують, щоб ідентифікувати дані, які мають бути точними, і дані, які є менш чутливі, і, тому, менше впливають на загальну точність.

Всеохопність і точність аналізування ризику треба встановити якомога повніше. В усіх можливих випадках треба ідентифікувати джерела невизначеності та звернути увагу на невизначеності, пов'язані як з даними, так і з моделлю чи методом. Треба встановити характеристики, щодо яких аналізування вкрай важливе, а також ступінь важливості.

### **Оцінювання ризику**

Оцінювання ризику передбачає порівнювання кількісно оцінених рівнів ризику з критеріями ризику, визначеними під час установлювання оточення, для того, щоб установити значення рівня й типу ризику.

Оцінювання ризику ґрунтується на розумінні ризику, набутому під час аналізування ризику, і слугує для прийняття рішень щодо подальших дій. Етичні, правові, фінансові та інші міркування, зокрема, сприйняття ризику, також є вхідними даними для прийняття рішень.

#### Рішення можуть бути щодо:

- потреби в обробці ризику;
- пріоритетів обробки;
- доцільності виконання певної роботи;
- вибору з низки напрямків тих, яких треба дотримуватись.

На цій стадії, коли є більше інформації про конкретні ідентифіковані ризики, потрібно знову докладніше розглянути вибрані ще під час устанавлювання оточення характер рішень, що їх потрібно прийняти, і критерії, що їх використовуватимуть для прийняття цих рішень.

Найпростішою структурою критеріїв ризику є один рівень, що відокремлює ризики, які потребують оброблення, від ризиків, які не потребують оброблення. Ця структура дає цікаві прості результати, але не відображає невизначеності, притаманні кількісному оцінюванню ризиків і розмежуванню ризиків на ті, які потребують оброблення, і ті, які не потребують обробки.

Рішення щодо необхідності та способу обробки ризику може залежати від витрат і переваг, пов'язаних із взяттям на себе ризику, і від витрат і переваг, пов'язаних із запровадженням поліпшених засобів контролю.

Загальноприйнятий підхід полягає в розділенні ризиків на три діапазони:

а) верхній діапазон, у якому рівень ризику розглядають як недопустимий незалежно від будь-якої вигоди внаслідок діяльності, і в якому оброблення ризику конче потрібне незалежно від витрат на нього;

б) середній діапазон (або «сіра» зона), у якому враховано витрати та переваги, а можливості збалансовано відповідно до потенційних наслідків;

в) нижній діапазон, у якому рівень ризику розглядають як незначний або настільки малий, що жодних заходів з оброблення ризику не потрібно.

Система критеріїв AI-AIP («настільки низький, наскільки це практично доцільно»), використовувана у практиці убезпечення, реалізує цей підхід, за якого середній діапазон має рухому шкалу для низьких ризиків, що дає змогу безпосередньо порівнювати витрати та переваги, тоді як для високих ризиків потенційну можливість шкоди треба знижувати доти, доки витрати на подальше знижування не стануть цілком диспропорційними отриманій перевазі щодо безпеки (див. рисунок В.12).

### **1.3. Аналіз методів загального оцінювання ризиків та загроз безпеці авіаційних транспортних систем**

#### **1. Мозкова атака**

Мозкову атаку застосовують, щоб стимулюванням та заохочуванням до вільного обговорення в групі компетентних осіб ідентифікувати потенційні види відмов і асоційовані з ними небезпечні чинники, ризики, критерії прийняття рішень і/або варіанти оброблення. Термін «мозкова атака» часто досить довільно вживають на означення будь-якого типу групового обговорення. Однак, справжня мозкова атака передбачає застосування спеціальних прийомів, спрямованих на те, щоб активізувати творче мислення одних учасників за допомогою ідей та висловлювання інших членів групи.

Мозкова атака може бути формалізованою чи неформалізованою. Формалізована мозкова атака більш структурована, коли заздалегідь підготовлено учасників, визначено ціль і завдання засідання, передбачено способи оцінювання ідей, що їх висуватимуть. Неформалізована мозкова атака менш структурована і часто ситуативніша.

Вихідні дані залежать від стадії процесу керування ризиком, на якій цей метод застосовують, наприклад, на стадії ідентифікування вихідними даними може бути перелік ризиків і поточних засобів контролю.

#### ***Переваги мозкової атаки:***

- вона стимулює творче мислення, даючи змогу ідентифікувати нові ризики та оригінальні рішення;
- вона уможлиблює залучення ключових зацікавлених сторін і, тому, сприяє загальному обміну інформацією;
- її можна відносно швидко та легко запровадити.

### **Обмеженості:**

- учасникам може бракувати компетентності та знань, щоб робити результативний внесок;

- через її відносну неструктурованість важко продемонструвати, що процес був всеохопним, тобто що було враховано всі потенційні ризики;

- у конкретній групі може бути певна динаміка обговорення, коли деякі особи з цінними ідеями не

висловлюються, а інші домінують в обговоренні. Цю ситуацію можна долати за допомогою комп'ютеризованої мозкової атаки з використанням чат-форумів або методу номінальної групи. Комп'ютеризовану мозкову атаку можна налаштувати так, щоб вона була анонімною, даючи змогу уникати персональних або політичних питань, які можуть перешкоджати вільному обговоренню ідей. За методом номінальної групи ідеї надходять до координатора анонімно і потім їх обговорюють усі учасники групи.

### **2. Структуроване чи напівструктуроване опитування**

У структурованому опитуванні опитуваним особам ставлять низку підготовлених запитань з аркуша навідних запитань, які спонукають опитувану особу розглядати ситуації з різних кутів зору і, таким чином, ідентифікувати ризики з цих поглядів. Напівструктуроване опитування провадять подібним чином, але воно надає більшу свободу для обговорення, щоб дослідити питання, які виникають.

Структуроване та напівструктуроване опитування корисне в тих випадках, коли важко зібрати людей на засідання для мозкової атаки чи коли вільна дискусія в групі недоречна до ситуації чи залучених осіб. Це опитування найчастіше застосовують, щоб ідентифікувати ризики чи оцінити результативність наявних засобів контролювання в межах аналізування ризику. Їх можна застосовувати на будь-якій стадії проекту чи процесу. Вони є засобом отримання від зацікавлених сторін вхідних даних для загального оцінювання ризику.

Вхідні дані охоплюють:

- чітко визначені цілі опитувань;
- перелік опитуваних осіб, вибраних серед представників відповідних сторін-учасниць;
- підготовлену низку запитань.

***Переваги структурованих опитувань:***

- структуровані опитування надають можливість опитуваним особам мати час для розмірковування над проблемою;
- обмін інформацією «один на один» може сприяти більш поглибленому розгляданню проблем;
- структуровані опитування дають змогу залучати більшу кількість зацікавлених сторін, ніж мозкова атака, яку провадить відносно невелика група.

***Обмеженості:***

- координатор витрачає багато часу на збирання численних думок у цей спосіб;
- упередженість допускають і не усувають під час групового обговорювання;
- може виявитися неможливим стимулювати творче мислення присутніх осіб, що є значною перевагою мозкової атаки.

**3. Метод Дельфі**

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

***Переваги:***

- зважаючи на анонімність суджень, більш імовірним є висловлювання непопулярних думок;
- усі думки є рівноважними, що дає змогу уникати проблеми переважання думок окремих особистостей;



- дає право власності на результати;
- немає потреби збирати учасників одночасно в одному місці.

***Обмеженості:***

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

**4. Попереднє аналізування небезпечних чинників (РНА)**

Попереднє аналізування небезпечного чинника – простий індуктивний метод аналізування, який полягає в тому, щоб ідентифікувати небезпечні чинники, а також небезпечні ситуації та події, які можуть зашкодити діяльності, устаткованню чи системі.

- використовувані чи вироблювані матеріали та їхня хімічна активність;
- застосовуване устаткування;
- середовище функціонування;
- розташування;
- взаємодії між складниками системи тощо.

Може бути проведено якісне аналізування наслідків небажаної події та їхньої ймовірності для того, щоб ідентифікувати ризики для подальшого загального оцінювання.

***Переваги:***

- можливість використання за наявності обмеженої інформації;
- дає змогу розглядати ризики на ранній стадії життєвого циклу системи.

***Обмеженості:***

– РНА дає змогу отримувати лише попередню інформацію; він не є всеохопним і не забезпечує докладною інформацією стосовно ризиків і способу, у який можна якнайкраще їм запобігати.

**5. Метод HAZOP**

HAZOP – це акронім словосполучення «дослідження небезпечних чинників і працездатності» (**HAZ**ard and **OP**erability study). Це метод структурованого та

систематизованого дослідження планованих або наявних продукції, процесу, процедури чи системи. Він дає змогу ідентифікувати ризики для персоналу, устаткування, довкілля та/або цілей організації. Від дослідницької групи очікують також вироблення, в усіх можливих випадках, рішення щодо оброблення конкретного ризику.

HAZOP – якісний метод, базований на використанні керуючих слів, за допомогою яких формулюють питання, щоб визначити, якою мірою завдання проектування чи умови функціонування може бути не досягнуто на кожному етапі проекту, процесу, процедури чи системи. Зазвичай дослідження здійснює багатодисциплінарна група під час кількох засідань.

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

### ***Переваги та обмеженості***

Аналізування методом HAZOP має такі **переваги**:

- є засобом систематичного та ретельного досліджування системи, процесу чи процедури;
- передбачає формування багатодисциплінарної групи із залученням осіб, які мають досвід практичної роботи, і тих, які здатні виконувати дії з оброблення ризиків;
- уможливорює генерування рішень і дій щодо оброблення ризиків;
- застосовне до широкого спектра систем, процесів і процедур;
- дає змогу явно розглядати причини та наслідки людських помилок;
- забезпечує письмове протоколювання процесу, який можна використовувати для демонстрування належної старанності.

Аналізування методом HAZOP має такі **обмеженості**:

- докладне аналізування може потребувати багато часу і, тому, дорого коштувати;
- докладне аналізування вимагає високого рівня документування чи специфікування системи чи процесу, або процедури;
- може бути зосереджено здебільшого на пошуку докладних рішень, а не на критичному розгляді основоположних припущень (однак ці прояви може бути зменшено за поетапного підходу);
- обговорення може бути зосереджено на подробицях проекту, а не на ширших чи зовнішніх питаннях;
- обмежено (ескізним) проектом і призначеністю проекту, а також сферою застосування та цілями, запропонованими групі;
- процес значною мірою спирається на фаховий досвід проектувальників, яким може бути важко залишатися достатньо об'єктивними у виявленні проблем у їхніх проектах. [IEC 61882 Hazard and operability studies (HAZOP studies) – Application guide (Дослідження небезпечних чинників і працездатності (дослідження HAZOP). Настанови щодо застосування)]

## **6. Аналіз небезпечних чинників і критичні точки контролю (НАССР)**

Аналіз небезпечних чинників і критичні точки контролю (НАССР) надає структуру для ідентифікації небезпечних чинників і запровадження засобів контролю на рівні всіх важливих частин процесу, щоб запобігати небезпечним чинникам і підтримувати якість, надійність і безпечність продукції. Ціль НАССР – забезпечити зведення до мінімуму ризиків за допомогою саме засобів контролю протягом усього процесу, а не інспекційного контролювання кінцевої продукції.

### ***Переваги:***

- структурований процес, який уможливорює задокументовану засвідченість контролювання якості, а також ідентифікації та зменшування ризиків;

– зосередженість на практичних аспектах того, як і на яких етапах процесу можна запобігати небезпечним чинникам і контролювати ризики;

– заохочує до контролювання ризиків протягом усього процесу, а не тільки інспекційного контролювання кінцевої продукції;

•– уможлиблює ідентифікації небезпечних чинників, спричинюваних діями персоналу, і того, як ці чинники можна контролювати в точці утворення чи надалі.

### ***Обмеженості:***

– HACCP вимагає ідентифікувати небезпечні чинники, визначати ризики, притаманні цим чинникам, і розглядати їхню важливість як вхідні дані до процесу аналізування. Також потрібно визначити відповідні засоби контролювання. Усе це необхідне для того, щоб під час аналізування HACCP установити критичні точки контролю та контрольні параметри. Для цього може бути потрібно поєднати ці елементи з іншими аналітичними методами;

– застосування заходів у разі, коли контрольні параметри виходять за визначені межі, може призвести до того, що не буде помічено поступових змін контрольних параметрів, які є статистично значимими і, відповідно, щодо них треба застосувати належні дії [47].

## **7. Загальне оцінювання екологічного ризику**

Загальним оцінюванням екологічного ризику вважають процес загального оцінювання ризиків, які можуть бути для рослин, тварин і людей, підданих впливу низки екологічних небезпечних чинників. Керування ризиком стосується етапів прийняття рішень, зокрема оцінювання ризику та оброблення ризику.

Метод передбачає аналізування небезпечного чинника чи джерела шкоди і того, як вони впливають на цільову популяцію, а також шляхів, якими небезпечний чинник може досягати уразливої цільової популяції. Потім цю інформацію поєднують, щоб провести кількісне оцінювання ступеня ймовірності та характеру шкоди.

### ***Переваги та обмеженості***

Перевага цього аналізування полягає в тому, що воно забезпечує дуже докладне вивчення характеру проблеми та чинників, що підвищують ризик.

Аналізування напрямів впливу є зазвичай корисним аналітичним інструментом для всіх сфер ризику і дає змогу ідентифікувати, як і де можна поліпшити наявні або ввести нові засоби контролю.

Однак, для його застосування потрібно мати вірогідні дані, яких часто немає або які мають високий рівень пов'язаної з ними невизначеності. Наприклад, криві залежності «доза-відгук», одержані за результатами дослідження впливу на тварин високих рівнів небезпечного чинника, треба екстраполювати, щоб кількісно оцінити впливи дуже низьких рівнів забрудників на людей, і є численні моделі, за допомогою яких це провадять. Коли цільовим об'єктом є переважно довкілля, а не люди, і небезпечний чинник не має хімічного характеру, то даних, які безпосередньо стосуються конкретних умов до слідження, може бути обмежена кількість.

### **8. Структурований метод «Що – якщо» (SWIFT)**

Методика SWIFT – системне дослідження, яке провадить група спеціалістів із застосуванням набору «навідних» слів або фраз, що їх використовує координатор під час робочого засідання, щоб стимулювати ідентифікування ризиків з боку учасників. Координатор і група використовують стандартні фрази типу «що трапиться, якщо» у поєднанні з навідними фразами, щоб дослідити, як на систему, технічний об'єкт, організацію чи процедуру впливатимуть відхилення від нормального функціонування та поведіння. Методику SWIFT, на відміну від методики HAZOP, застосовують зазвичай на рівні систем за нижчого рівня докладності.

#### ***Переваги SWIFT:***

- широка застосовність до всіх видів технічних об'єктів або систем, ситуацій чи обставин, організацій або діяльності;
- потребує мінімального підготування членами групи;
- є відносно швидким, а основні небезпечні чинники та ризики швидко стають очевидними під час робочого засідання;

– дослідження «системно зорієнтовано» і дає змогу учасникам побачити, як система реагує на відхилення, а не просто дослідити наслідки відмови окремих складників;

– можна використовувати для визначення можливостей щодо поліпшення процесів і систем і, загалом, для визначення дій, які ведуть до успіху та збільшують його ймовірність;

– передбачає участь у засіданнях осіб, відповідальних за наявні засоби контролювання та за подальші дії щодо оброблення ризиків, збільшує їхню відповідальність;

– дає змогу скласти реєстр ризиків і, за незначного дороблення, – план оброблення ризиків;

– дає змогу ідентифікувати ризики та небезпечні чинники так, щоб результати можна було застосовувати для кількісного дослідження, тоді як, зазвичай, для оцінювання ризику та визначання пріоритетності відповідних дій використовують якісну чи напівкількісну форму ранжування ризику.

#### ***Обмеженості SWIFT:***

– результативність залежить від досвіду та кваліфікації координатора;

– потреба в ретельному підготовленні, щоб не втрачати часу на робочих засіданнях групи;

– якщо досвід групи недостатній або якщо система навідних фраз не всебічна, деякі ризики чи небезпечні чинники може бути не ідентифіковано;

– застосування методу на загальному рівні може не давати змоги виявити складні, докладні чи взаємопов'язані причини.

#### **9. Аналізування сценарію**

Аналізуванням сценарію називають розробку описових моделей того, що може трапитися в майбутньому. Його можна використовувати для ідентифікування ризиків, розглядаючи можливі варіанти розвитку подій у майбутньому та досліджуючи їхні наслідки. Набори сценаріїв, що відбивають, наприклад, «найкращий випадок», «найгірший випадок» і «прогнозований випадок», можна

використовувати, аналізуючи потенційні наслідки та їхні ймовірності для кожного сценарію як форму аналізу чутливості під час аналізу ризику.

### ***Переваги та обмеженості***

Аналізування сценаріїв передбачає врахування низки можливих подій у майбутньому. Воно може виявлятися кращим за традиційний підхід, згідно з яким спираються на довго-, середньо- та коротко тривалі прогнози, у яких припускають, використовуючи хронологічні дані, що майбутні події, ймовірно, і далі відповідатимуть минулим тенденціями. Це важливо для ситуацій, коли поточні знання, на яких базують прогнози, обмежені чи коли ризики розглядають у віддаленішому майбутньому.

Однак ця перевага має певну переконливість, яка полягає в тому, що за високої невизначеності деякі сценарії можуть бути нереалістичними.

Основні труднощі в аналізуванні сценарію пов'язані з наявністю даних і здатністю аналітиків і тих, хто приймає рішення, розробляти реалістичні сценарії, які придатні для дослідження можливих рішень.

Небезпеки аналізування сценарію як засобу прийняття рішень полягають у тому, що такі сценарії можуть не мати адекватного підґрунтя, що дані можуть бути гіпотетичними і що нереалістичні результати не можна інтерпретувати як нереалістичні.

### **10. Аналіз впливу на діяльність (BIA)**

Аналіз впливу на діяльність, яке також називають оцінюванням впливу на діяльність, дає змогу аналізувати те, як основні ризики дестабілізування могли б позначатися на роботах організації, а також ідентифікувати та кількісно подавати можливості, необхідні для керування цими ризиками. Зокрема, BIA уможливорює узгоджене розуміння:

- ідентифікації та критичності ключових бізнес-процесів, функцій і пов'язаних з ними ресурсів, а також основних взаємозалежностей, які є в організації;
- того, як дестабілізувальні події позначатимуться на здатності та можливості досягати критично важливих бізнесових цілей;

– здатностей і можливостей, необхідних, щоб керувати впливом дестабілізуючої події й допомагати організації відновлювати прийнятні рівні функціонування.

***Переваги ВІА:***

– належне розуміння критичних процесів, що дає змогу організації й надалі досягати своїх уста

новлених цілей;

– належне розуміння необхідних ресурсів;

– можливість по-новому визначати операційні процеси організації, щоб сприяти спроможності

поновлювати нормальне функціонування організації.

***Обмеженості:***

– брак знань у осіб, які беруть участь у заповнюванні анкет, проведенні опитувань або робочих засіданнях;

– групова динаміка може впливати на повноту аналізування критичного процесу;

– спрощене чи надмірно оптимістичне очікування вимог до відновлення;

– утрудненість досягання адекватного рівня розуміння робіт і діяльності організації.

**11. Аналіз першопричин (RCA)**

RCA застосовують щодо різноманітного оточення у широких сферах використання:

– RCA, зорієнтоване на безпеку, використовують для розслідування нещасних випадків, а також у сфері гігієни та охорони праці;

– аналізування відмов використовують стосовно технологічних систем, пов'язаних із забезпеченням надійності та технічним обслуговуванням;

– RCA, зорієнтоване на виробництво, застосовують у сфері контролю якості промислового виробництва;

– RCA, зорієнтоване на процеси, застосовують до бізнес-процесів;



– RCA, зорієнтоване на системи, розроблено як поєднання згадуваних вище сфер для дослідження складних систем, застосовуваних у керуванні змінами, керуванні ризиком і аналізуванні систем.

***Переваги RCA:***

- залучення належних експертів до роботи в групі;
- структуроване аналізування;
- розгляд усіх імовірних гіпотез;
- документування результатів;
- потреба виробляти остаточні рекомендації.

***Обмеженості:***

- необхідних експертів може не бути;
- істотні докази може бути знищено під час відмови чи видалено під час прибирання;
- групі може бракувати часу чи ресурсів, щоб оцінити ситуацію в повному обсязі;
- може не бути можливості належно виконати рекомендації.

Наведені методи не є вичерпними. Разом з тим, відомі методи не дають змоги комплексного оцінювання загроз і ризиків. Методи загального оцінювання ризику наведено у табл. 1.1.

Таблиця 1.1

## Методи та засоби аналізу ризиків

Методи та засоби аналізування	Процес загального оцінювання ризику				
	Ідентифікування ризику	Аналізування ризику			Оцінювання ризику
		Наслідок	Імовірність	Рівень ризику	
«Мозкова атака»	33 <sup>1)</sup>	НЗ <sup>2)</sup>	НЗ	НЗ	НЗ
Структуроване чи напівструктуроване опитування	33	НЗ	НЗ	НЗ	НЗ
Метод Дельфі	33	НЗ	НЗ	НЗ	НЗ
Переліки контрольних запитань	33	НЗ	НЗ	НЗ	НЗ
Попереднє аналізування небезпечних чинників (РНА)	33	НЗ	НЗ	НЗ	НЗ
Дослідження небезпечних чинників і працездатності (HAZOP)	33	33	3 <sup>3)</sup>	3	3
Аналізування небезпечних чинників і критичні точки контролю (HACCP)	33	33	НЗ	НЗ	33
Загальне оцінювання екологічного ризику	33	33	33	33	33
Структурований метод «Що — якщо» (SWIFT)	33	33	33	33	33
<b>Аналізування сценаріїв</b>	<b>33</b>	<b>33</b>	<b>3</b>	<b>3</b>	<b>3</b>
<b>Аналізування впливу на діяльність</b>	<b>3</b>	<b>33</b>	<b>3</b>	<b>3</b>	<b>3</b>
<b>Аналізування першопричини</b>	<b>НЗ</b>	<b>33</b>	<b>33</b>	<b>33</b>	<b>33</b>
<b>Аналізування видів і наслідків відмов</b>	<b>33</b>	<b>33</b>	<b>33</b>	<b>33</b>	<b>33</b>
<b>Аналізування дерева відмов</b>	<b>3</b>	<b>НЗ</b>	<b>33</b>	<b>3</b>	<b>3</b>
<b>Аналізування дерева подій</b>	<b>3</b>	<b>33</b>	<b>3</b>	<b>3</b>	<b>НЗ</b>
<b>Аналізування причин і наслідків</b>	<b>3</b>	<b>33</b>	<b>33</b>	<b>3</b>	<b>3</b>
<b>Аналізування причинно-наслідкових зв'язків</b>	<b>33</b>	<b>33</b>	<b>НЗ</b>	<b>НЗ</b>	<b>НЗ</b>
<b>Аналізування рівнів захисту (LOPA)</b>	<b>3</b>	<b>33</b>	<b>3</b>	<b>3</b>	<b>НЗ</b>
<b>Дерево рішень</b>	<b>НЗ</b>	<b>33</b>	<b>33</b>	<b>3</b>	<b>3</b>
<b>Загальне оцінювання надійності людини</b>	<b>33</b>	<b>33</b>	<b>33</b>	<b>33</b>	<b>3</b>
<b>Аналізування за схемою «краватка-метелик»</b>	<b>НЗ</b>	<b>3</b>	<b>33</b>	<b>33</b>	<b>3</b>
<b>Технічне обслуговування, зорієнтоване на забезпечення безвідмовності</b>	<b>33</b>	<b>33</b>	<b>33</b>	<b>33</b>	<b>33</b>
<b>Аналізування паразитних схем</b>	<b>3</b>	<b>НЗ</b>	<b>НЗ</b>	<b>НЗ</b>	<b>НЗ</b>

## Продовження таблиці 1.1

Методи та засоби аналізування	Процес загального оцінювання ризику				
	Ідентифікування ризику	Аналізування ризику			Оцінювання ризику
		Наслідок	Імовірність	Рівень ризику	
Марковське аналізування	3	33	НЗ	НЗ	НЗ
Імітаційне моделювання за методом Монте-Карло	НЗ	НЗ	НЗ	НЗ	33
Байєсова статистика і мережі Байєса	НЗ	33	НЗ	НЗ	33
Криві FN	3	33	33	3	33
Показники ризику	3	33	33	3	33
Матриця «наслідок-імовірність»	33	33	33	33	3
Аналізування витрат і вигод	3	33	3	3	3
Багатокритерійне аналізування рішень (MCDA)	3	33	3	33	3

- 1) Завжди застосовний.  
 2) Незастосовний.  
 3) Застосовний.

### 1.4. Обґрунтування вимог до методичного забезпечення діяльності АТС щодо ідентифікації загроз та оцінки ризиків в ході некомерційної експлуатації.

#### Постановка завдання дослідження

Відповідно до теоретичних розробок спеціалістів у галузі безпеки, основними напрямками забезпечення безпеки є правовий, організаційний, інженерно-технічний [51–52]. Застосування всіх цих напрямів є необхідним для формування вимог до методичного забезпечення діяльності АТС щодо ідентифікації загроз та оцінки ризиків в ході некомерційної експлуатації.

До правового напрямку належать чинні закони, нормативні акти, які регламентують правила використання авіаційного транспорту та відповідальність за їх порушення.

Інженерно-технічний напрям передбачає застосування фізичних, апаратних та програмних засобів. Основним принципом технічного забезпечення безпеки Державної авіації України є створення та використання комплексу програмно-



оперативність оцінювання загроз та ризиків;

всебічне і повне урахування дії всіх складових загроз на рівень авіаційної безпеки;

простота, доступність і наочність отриманих розрахункових даних;

можливість прогнозування ситуації, що склалася на майбутній перебіг подій і на ймовірність виникнення аварійних та катастрофічних ситуацій;

гнучкість у використанні і можливість оперативно вводити і оцінювати нові різноманітні дані, що стосуються складових авіаційної безпеки.

Таким чином, викладені вимоги до методичного апарату оцінки загроз та ризиків дають змогу охопити всі аспекти завдання оцінювання рівня безпеки авіації.

### **Висновки до розділу**

2. Визначено, що у контексті воєнного стану, оголошеного в Україні, найбільш важливим фактором вважається пряма загроза галузі цивільної авіації. Імовірність загрози, що виникає внаслідок наміру та можливості нападу на цивільне повітряне судно над зоною конфлікту або поблизу неї, є ключовим фактором оцінки ризику та попередньою умовою для визначення заходів з пом'якшення наслідків, які необхідно застосувати.

3. Сучасні негативні явища найгостріше позначають проблему браку нових способів управління процесами забезпечення безпеки польотів, визначення загроз та відповідних джерел небезпеки авіаперевезень, а відтак продовжуватимуть ставати все більш актуальними.

4. Аналіз понятійно-категорійного апарату надав змогу уточнити поняття безпека на транспорті як таке, що стосується не тільки безпеки перевезень, але й безпеки всіх технологічних процесів транспортних галузей, в тому числі й економічної, та інформаційної безпеки.

5. За результатами аналізу методів оцінювання загроз та ризиків визначено, що моделювати й класифікувати джерела загроз, самі загрози та їх прояви, а також розробляти ефективні заходи протидії доцільно на основі аналізу взаємодії логічного

ланцюжка: Джерело загрози → Загроза → Уразливість → Реалізація загрози (атака) → Наслідки (збиток) → Заходи протидії.

## **РОЗДІЛ 2. РОЗРОБКА МЕТОДИЧНОГО АПАРАТУ ІДЕНТИФІКАЦІЇ ЗАГРОЗ ТА ОЦІНКИ РИЗИКІВ ДІЯЛЬНОСТІ ТРАНСПОРТНОЇ СИСТЕМИ (КОМПЛЕКСУ) В ХОДІ НЕКОМЕРЦІЙНОЇ ЕКСПЛУАТАЦІЇ**

### **2.1. Методичний підхід до забезпечення авіаційної безпеки. Обґрунтування системи показників загроз та ризиків**

Вирішення проблеми захисту компонентів авіаційної діяльності від зовнішніх та внутрішніх загроз полягає не лише у виявленні і протидії цим загрозам, а й у наявності дієвих механізмів всебічного комплексного оцінювання стану безпеки, які дають змогу своєчасно організовувати боротьбу із зазначеними загрозами.

Дослідженню в цій галузі присвячено низку робіт, в яких пропонуються різні підходи до комплексного оцінювання рівня безпеки.

Так, наприклад, у [18] викладено системний підхід до побудови комплексного захисту системи підприємства та описано методику побудови такої системи із застосуванням технічних засобів захисту. У [19] розглянуті принципи й методи аудиту безпеки на основі процесорного підходу, наведено певні методи оцінювання.

Найбільш системно до вирішення завдання безпеки, на наш погляд, розглянуто у [20]. Запропонована тривимірна модель, що містить основні етапи, напрямки та методи забезпечення безпеки різних систем. Визначено, що специфічними особливостями завдання створення систем забезпечення безпеки є [20]:

неповнота й невизначеність вихідної інформації про склад і характер загроз;

багатокритеріальність завдання, що пов'язано з необхідністю врахування великої кількості часткових показників;

наявність кількісних і якісних показників, які необхідно враховувати, вирішуючи завдання розроблення та впровадження систем захисту і протидії;

неможливість застосування класичних методів оптимізації.

З огляду на викладене, пошук шляхів комплексного оцінювання стану безпеки є актуальним науковим і практичним завданням.

Діяльність щодо забезпечення безпеки розпочинається в ході вирішення суперечності між небезпекою і потребою управляти безпекою: передбачати, запобігати, локалізувати й усувати збиток від впливу небезпеки, тобто виявлення, ідентифікації та оцінювання загроз і ризиків [21].

Оцінка рівня безпеки завжди відносна. Спроби безпосередньо приписати цій оцінці числове значення в більшості випадків безперспективні в плані подальшої інтерпретації результатів.

Безпека – поняття комплексне, а тому не може розглядатися як проста сума її складових. Ці складові взаємопов'язані та взаємозалежні. Крім того, кожна частина з них є критично значущою та має різний ступінь впливу на величину узагальненого критерію.

Отже, методи, що передбачають усереднення часткових критеріїв безпеки (нехай і неявне) при комплексному оцінюванні стану безпеки, неприйнятні.

Часткові критерії та показники, що використовуються для оцінювання стану підсистем безпеки, зазвичай, носять суперечливий характер. Це призводить до того, що завдання комплексного оцінювання стану безпеки є багатокритеріальним.

Для розв'язання багатокритеріальних задач, зазвичай, використовуються різні методи згортки критеріїв в один узагальнений (інтегральний) критерій. Найбільш простий метод визначення інтегрального критерію полягає у виділенні одного з критеріїв як основного, а всі інші критерії додаються до обмежень, в яких задається область допустимих значень вектора незалежних змінних. Таким чином, завдання прийняття рішення з векторним критерієм зводяться до завдань зі скалярним аргументом.

Основний недолік такого підходу полягає в тому, що стан безпеки фактично оцінюється лише за одним критерієм. Значення інших критеріїв, якщо вони задовольняють обмеження, не впливають на результати оцінювання.

Отже, враховуючи багатовимірність безпеки, спроба оцінити її рівень за одним параметром (наприклад, який має стандартний кількісний вираз) є

некоректною. Тому такий спосіб отримання згортки розв'язання завдань, пов'язаних з оцінюванням стану безпеки, є неприйнятним.

Припустимо, що рівень безпеки оцінюється від нуля до одиниці. При цьому нулю відповідає абсолютно неприйнятний рівень безпеки (нижча оцінка), а одиниці – повністю задовільний рівень (найвища оцінка) [22].

При оцінюванні окремих сторін безпеки системи існує деякий граничний рівень, вище якого система вважається безпечною, а нижче – ні. Рівень залишкових ризиків при цьому лише змінює граничне значення в той чи інший бік, не змінюючи картину в цілому.

Під час комплексного оцінювання стану безпеки ситуація якісно змінюється. Певні ризики, неприйнятні за одних обставин, за інших оцінюються як допустимі. Причому, такими обставинами, які впливають на оцінювання стану безпеки, можна назвати і наявність або відсутність інших ризиків [22].

Будь-які неконтрольовані зовнішні або внутрішні процеси потенційно можуть призвести до виникнення загроз. Реалізація цих загроз спричинює різні деструктивні процеси, що, у свою чергу, впливає на стан безпеки всієї системи. Порушення нормального функціонування системи відображається в значеннях критеріїв і показників, які використовуються для оцінювання стану її безпеки [23]. Це, у свою чергу, свідчить про необхідність виваженого вибору узагальнених критеріїв і показників стану безпеки. У концептуальному плані підхід до вибору зазначених критеріїв і показників потрібно уніфікувати.

Іншими методами визначення комплексного критерію є адитивна та мультиплікативна згортка [23 – 26].

Адитивний критерій є найпростішим. Водночас, у зв'язку з можливістю необмеженої компенсації значень одних критеріїв за рахунок інших, він є нечутливим до граничних значень окремих критеріїв.

Отже, методи, в основі яких лежить припущення про лінійне поведіння системи (адитивна згортка припускає саме таку модель), при комплексному оцінюванні рівня безпеки, зазвичай, не можуть адекватно відображати реальну



ситуацію. Тому адитивна згортка для комплексного оцінювання рівня безпеки переважно також є неприйнятною.

Значення мультиплікативного критерію, на відміну від адитивного, різко зменшується при малих значеннях окремих критеріїв. Це дає змогу підвищити чутливість узагальненого критерію до незначних змін його складових.

Таким чином, для завдань, пов'язаних із забезпеченням безпеки у більшості випадків найбільш доцільним вважається застосування мультиплікативної згортки векторного критерію:

$$K = \sum_{i=1}^N K_i S_i, \quad (2.1)$$

де:  $K_i$  – часткові критерії,  $S_i$  – вага часткового критерію  $K_i$  (ступінь впливу на узагальнений критерій), яка визначається експертним шляхом,  $N$  – кількість часткових критеріїв  $K_i$ .

При виконанні згортки з метою уніфікації різнорідних критеріїв використовують перехід від абсолютних значень критеріїв до відносних величин. Для цього фіксується шкала можливих значень для критеріїв і можливі межі зміни для кожного з них. Наприклад, якщо за шкалу прийняти інтервал  $[0; 1]$ , а межі зміни критерію  $K_i$  знаходяться між  $K_{imin}$  та  $K_{imax}$ , то як відносне значення критерію буде виступати величина:

$$\bar{K} = \frac{K_i - K_i^{\min}}{K_i^{\max} - K_i^{\min}} \quad (2.2)$$

Однак, інколи отримати від особи, що приймає рішення (ОПР), надійну кількісну інформацію для побудови  $K$  буває дуже складно. У таких випадках прагнуть одержати від ОПР, в основному, тільки якісну інформацію. Наприклад, про те, який із критеріїв найбільш або найменш значущий, який з критеріїв може бути погіршений, а для яких погіршення є вкрай небажаним тощо.

Отримати таку інформацію можна за алгоритмом Беленсона–Капура [26-28].

Певні фактори, що стосуються авіаційної безпеки, можуть взагалі не підлягати кількісному виміру. В такому разі під час їхнього оцінювання застосовують штучні прийоми. Наприклад, кожному фактору відповідає кількісна бальна шкала [29]. Приклад такої шкали наведено в табл.2.1.

Зважаючи на вищевикладене, експертові бажано запропонувати методику, за якою він має призначити бали та в подальшому оцінити стан безпеки. Вона може складатися з таких етапів [29 – 31].

Експертне оцінювання факторів, що впливають на стан безпеки за шкалами, наведеними в табл.2.1.

Визначення часткових показників безпеки та їх ваги.

Визначення мінімального та максимального значень відповідного показника.

Обчислення відносного значення критерію за формулою (2.2).

Таблиця 2.1.

Оцінювальні шкали для визначення значущості факторів

Перелік питань, що дають змогу виділити значущість факторів	Пояснення значення шкал
Тривалість впливу фактора на безпеку АТС (шкала №1)	Недовго (0,3). Цей фактор буде нетривало впливати на безпеку АТС і за певних умов та припущень його можна звести до мінімуму
	Тривало (0,5). Цей фактор протягом значного відрізка часу буде впливати на безпеку АТС і може зі збігом обставин впливати і далі або припинити вплив
	Довго (0,7). Цей фактор буде впливати на безпеку АТС, незважаючи на зміни, які пов'язані зі значними організаційними, технічними та іншими перетвореннями
Наслідки, до яких може призвести нехтування фактором для оцінювання безпеки АТС (шкала №2)	Незначні (0,3). Нехтування цим фактором (його неврахування) не має відчутного впливу на оцінювання безпеки АТС.
	Відчутні (0,5). Нехтування цим фактором призводить до більш відчутного впливу на оцінювання безпеки АТС, але ці зміни можуть бути компенсовані урахуванням інших факторів або в інший спосіб за незначний проміжок часу
	Значні (0,7). Нехтування цим фактором призводить до значного впливу на безпеку АТС і матиме руйнівні наслідки. Наслідки змін, пов'язаних з нехтуванням цього фактору, можна мінімізувати (ліквідувати) тільки протягом значного відрізка часу із залученням значних ресурсів
	Катастрофічні (0,9). Нехтування цим фактором призводить до настільки значного впливу на безпеку АТС, що наслідки цих змін неможливо ліквідувати у найближчому майбутньому, і виникне проблема щодо цього майбутньому.
Зворотний вплив системи безпеки на цей фактор (шкала №3)	Не здійснює (0,1). Система безпеки не впливає на фактор, що розглядається

Перелік питань, що дають змогу виділити значущість факторів	Пояснення значення шкал
	Має слабкий вплив (0,3). Зі зміною системи безпеки АТС цей фактор змінюється незначно і за певних припущень може розглядатися як самостійний
	Значно впливає (0,5). Зі зміною системи безпеки цей фактор може змінитися настільки, що частково увійде до більш глобального або значно зросте його вплив
Ступінь зв'язку між цим фактором і рештою факторів (шкала №4)	Віддалено пов'язані (0,3). Цей фактор пов'язаний з іншим фактором так, що їх вплив один на одного не призводить до відчутних змін системи безпеки АТС
	Сильно пов'язані (0,7). Цей фактор пов'язаний із зіставленим настільки, що їхній взаємний вплив призводить до суттєвих змін у системі безпеки АТС і не може бути знехтуваний без наслідків для оцінювання
	Пов'язані визначально (0,9). Цей фактор пов'язаний із зіставленим настільки, що їхній взаємний вплив суттєво позначиться на системі безпеки АТС і не може змінитися навіть з плином часу

Забезпечення безпеки носить комплексний характер, ґрунтується на логіко-евристичному аналізі можливих негативних наслідків, а багато факторів, що впливають на її рівень можуть взагалі не підлягати кількісному виміру. Запропонований підхід до визначення критеріїв безпеки дає змогу уникнути труднощів, пов'язаних з оцінюванням її рівня.

Отже, запропонований підхід дає змогу комплексно оцінювати рівень безпеки, що підвищить обґрунтованість прийняття відповідних рішень при формуванні системи безпеки АТС.

## **2.2. Узагальнена модель динаміки рівня безпеки авіаційної транспортної системи**

Проблеми забезпечення безпеки АТС, з огляду на появу нових та зростання рівня існуючих ризиків і загроз, набувають великої значущості і потребують відповідного наукового підґрунтя для їх вирішення. Одним з напрямів розв'язання цих проблем є постійне удосконалення науково-методичного забезпечення безпеки авіації, а саме визначення спрямованості загроз та оцінювання їх рівня, виявлення об'єктів впливу та оцінювання ефективності заходів протидії.

Проблеми безпеки в авіатранспортних системах висвітлюються в низці публікацій. Завдання створення, організації й дослідження процесів функціонування,

удосконалювання й розвитку систем забезпечення безпеки авіації тою чи іншою мірою відображені в працях ряду вітчизняних і закордонних учених [47 – 52].

Однак дотепер повною мірою не вивчені й залишаються дискусійними методологічні, методичні й практичні аспекти дослідження проблем моделювання безпеки складних соціально-технічних систем.

Сучасні науково-практичні напрацювання в Україні, а також найпоширеніші міжнародні стандарти містять норми й вимоги, спрямовані переважно на захист від несанкціонованого доступу . При цьому вони часто не забезпечують базового рівня безпеки, тому що за ними моделюються лише частина загроз. Нині не розроблені загальноприйняті стандарти або підходи, що дають змогу забезпечити підвищений або високий рівень захисту. Так само шаблонність пропонованого захисту й відсутність варіативності є негативною стороною застосування сучасних стандартів [32–36].

Сформуємо загальну математичну модель, що описує динаміку зміни рівня безпеки системи [37].

Під рівнем безпеки системи (РБС) розуміється оцінка, яка отримана із сукупності показників і критеріїв, що характеризують стан системи стосовно захищеності критичних для неї елементів.

Рівень безпеки системи можна характеризувати за такою матрицею:

$$B = \begin{pmatrix} K_1 & F_1 & V_1 & T_1 & S_1 \\ K_2 & F_2 & V_2 & T_2 & S_2 \\ K_3 & F_3 & V_3 & T_3 & S_3 \\ \dots & \dots & \dots & \dots & \dots \\ K_n & F_n & V_n & T_n & S_n \end{pmatrix}, \quad (2.3)$$

де:

$K_i$  – показник рівня безпеки за  $i$ -м критерієм,  $i = \overline{1, n}$ ;

$F_i$  – тенденція зміни  $i$ -го критерію (зростає, зменшується, нейтральний),  $i = \overline{1, n}$ ;

$V_i$  – швидкість зміни  $i$ -го критерію (наприклад: низька, нижче середнього, середня, вище середнього, висока),  $i = \overline{1, n}$ ;

$T_i$  – час для  $i$ -го критерію, який дає змогу правильно інтерпретувати значення параметра  $V_i$ ,  $i = \overline{1, n}$ ;

$S_i$  – ступінь критичності негативних наслідків при реалізації ризиків, який погіршує значення  $i$ -го критерію,  $i = \overline{1, n}$ .

Матрицю вигляду  $B$  в подальшому будемо називати матрицею безпеки (МБ).

Загальна кількість стовпчиків МБ дорівнює 5, оскільки стаття 10 Повітряного кодексу України визначає що безпека авіації складається з 5 складових: безпеки польотів, авіаційної безпеки, екологічної безпеки, економічної та безпеки [40].

Перший і п'ятий стовпчики МБ являють собою вектор часткових критеріїв безпеки і їх значень, що характеризує стан безпеки, який дає змогу його оцінити на поточний момент часу. Інші стовпці матриці відображають динаміку розвитку процесів, що дають змогу прогнозувати їх розвиток в подальшому.

У цьому випадку мультиплікативну згортку інтегрального критерію безпеки можна подати у вигляді (2.1).

Оцінки  $S_i$  можуть бути отримані експертним шляхом. Однак, експерту не завжди буде легко оцінити ці коефіцієнти. Тому для цього необхідно використовувати різні рангові методи, реалізація яких вимагає правильного впорядкування цих критеріїв.

Як приклад, можна використати метод нестрогого ранжування. Відповідно до цього методу, експерт нумерує всі критерії в порядку зниження рівня негативних наслідків, які пов'язані з цим критерієм безпеки. Причому допускається, що експерту не вдається розрізнити між собою деякі критерії. Провівши ранжування, він розміщує їх поруч у довільному порядку. Потім критерії, які уже пройшли процес ранжування, послідовно нумеруються. Оцінка (ранг) критерію визначається за його номером.

Якщо на одному місці знаходяться декілька не розрізнених між собою критеріїв, то оцінка кожного з них приймається за середнє арифметичне їх нових номерів [37]. Однак, вважається за доцільне модифікувати такий метод оцінювання, прийнявши за ранг для кожного з нерозрізнених критеріїв – номер усієї групи, як цілого об'єкта за ступенем впорядкування [38].

У такий спосіб можуть бути оцінені як ступені впливу кожного параметра на часткові критерії безпеки  $K_i$ , так і ступені прийнятності наслідків реалізації загроз  $S_i$ .

Наприклад, будемо вважати, що експерт упорядкував критерії в такий спосіб:  $K_5, (K_3, K_7, K_2), K_1, (K_6, K_8), K_9, K_4$ .

Критерії, які не розрізнені між собою, об'єднані в круглих дужках. Тоді оцінки для кожного із критеріїв, які обчислені відповідно до описаної вище процедури, такі:

$$S_5 = 1; S_3 = S_7 = S_2 = 2; S_1 = 3; S_6 = S_8 = 4; S_9 = 5; S_4 = 6.$$

Застосуємо нормування за величиною, яка дорівнює сумі всіх оцінок:

$$R = \sum_i S_i. \quad (2.4)$$

У нашому випадку  $R = 29$ . Таким чином, після лінійного перетворення в шкалу  $[0;1]$  за нормою  $R$  отримаємо:

$$S_5 = \frac{1}{29}; S_3 = S_7 = S_2 = \frac{2}{29}; S_1 = \frac{3}{29}; S_6 = S_8 = \frac{4}{29}; S_9 = \frac{5}{29}; S_4 = \frac{6}{29}.$$

Визначені, запропонованим способом оцінки є узагальненням системи ваги Фішберна [39] у випадку змішаного розподілу переваг, коли поряд з перевагами в систему входять і відносини рівнозначності.

Критерії в матриці безпеки можна згрупувати за відповідними напрямками забезпечення безпеки.

Таким чином, кожний кортеж  $(K_i, F_i, V_i, T_i, S_i)$  характеризує стан безпеки за  $i$ -м критерієм.

Часткові матриці, що складаються з рядків і визначають певний напрям забезпечення безпеки, в свою чергу, описують стан у відповідній галузі.

Показники рівня безпеки  $K_i$  тісно пов'язані з наслідками від можливої реалізації наявних у системі загроз та заходами, які спрямовані на запобігання, локалізацію й усунення таких наслідків [39].

Слід особливо відзначити, що загрози можна розділити на первинні і вторинні. Первинні загрози існують незалежно від стану системи й апріорно мають певну безумовну ймовірність виникнення.

Імовірність виникнення вторинних загроз є умовною і залежить від стану системи та стану зовнішнього середовища.

Зокрема, деякі стани системи можуть спровокувати виникнення загроз, поява яких в інших умовах була б неможливою.

Введемо такі позначення:

$\overline{UG}_i$  і  $\widetilde{UG}_j$  ( $i, j = 1, 2, 3, \dots$ ) – сукупність первинних і вторинних загроз, що виникають з імовірностями  $\overline{PUG}_i$  і  $\widetilde{PUG}_j$ , відповідно, здійснюючи вплив  $\overline{n}_{km}$  і  $\check{n}_{km}$  на елемент  $(k, m)$  матриці безпеки  $B$  ( $k = 1, 2, 3, \dots$ ;  $m = 1, 2, 3, 4, 5$ ).

Вплив кожної з первинних або вторинних загроз можна описати матрицею впливу, що має вигляд [62]:

$$N_i = \begin{pmatrix} n_{11} & n_{12} & n_{13} & n_{14} & n_{15} \\ n_{21} & n_{22} & n_{23} & n_{24} & n_{25} \\ \dots & \dots & \dots & \dots & \dots \\ n_{n1} & n_{n2} & n_{n3} & n_{n4} & n_{n5} \end{pmatrix}. \quad (2.5)$$

Фактично матриця впливу являє собою матрицю ваги впливу і-го негативного фактору на елементи МБ.

Необхідно відмітити, що вплив  $\overline{n}_{km}$  і  $\check{n}_{km}$  на деякі елементи матриці безпеки  $B$  може бути як негативним, так і позитивним.

Елементи матриці, що негативно впливають, є негативними щодо елементів МБ, елементи, що позитивно впливають – є позитивними щодо елементів МБ, елементи, що ніяк не впливають, є нейтральними.

Кортеж  $\overline{R}_i = (\overline{N}_i; \overline{PUG}_i)$  назвемо ризиком реалізації і-ї первинної загрози.

Цей кортеж відображає появу наслідків з імовірністю  $\overline{PUG}_i$ , які змінюють стан системи через відповідні матриці впливу  $\overline{N}_i$ .

Імовірності виникнення первинних загроз  $\overline{PUG}_i$  від нас не залежать. Однак, сукупність превентивних заходів захисту дає змогу послабити вплив первинних загроз на ступінь комплексної безпеки системи.

Цей факт може бути описаний за допомогою матриці превентивних заходів:

$$Z_j = \begin{pmatrix} z_{11} & z_{12} & z_{13} & z_{14} & z_{15} \\ z_{21} & z_{22} & z_{23} & z_{24} & z_{25} \\ \dots & \dots & \dots & \dots & \dots \\ z_{n1} & z_{n2} & z_{n3} & z_{n4} & z_{n5} \end{pmatrix},$$

(2.6)

де  $j = \overline{1, M}$ ,  $M$  – загальна кількість превентивних заходів.

Елементи матриці  $Z_i$  назвемо демпферними коефіцієнтами.

Тоді під залишковим впливом будемо мати на увазі матрицю  $N$  (назвемо її матрицею залишкового впливу), елементи якої знаходяться з виразу:

$$\hat{n}_{mn} = n_{mn} \otimes \max_{k=1 \dots M} z_{mn}^k, \quad (2.7)$$

де  $z_{mn}^k$  – елемент  $(m, n)$  матриці превентивних заходів  $Z_k$ . Символом “ $\otimes$ ” позначена у такий спосіб певна для двох матриць операція.

У випадку числових значень елементів матриць, це може бути, наприклад, операція простого поелементного множення або додавання. У випадку лінгвістичних значень, ця операція (в нечіткій математиці – композиція) визначається за допомогою принципу розширення звичайних (чітких) математичних функцій на нечіткі числа, запропонованого Л.Заде [65].

Під залишковим ризиком будемо розуміти кортеж

$$\bar{R}_i = (\bar{N}_i; \overline{PUG}_i) \quad (2.8)$$

Якщо, незважаючи на превентивні заходи захисту, реалізація визначеної множини первинних загроз призвела до появи наслідків, то необхідно розпочати заходи для їх локалізації та усунення [37].

Насамперед, необхідно оцінити відхилення поточного стану системи  $B$  від безпечного стану  $B_s$ .

Уведемо поняття різниці між двома матрицями, визначивши результат застосування операції “ $\#$ ” до двох елементів матриць аналогічно тому, як це було зроблено для операції “ $\otimes$ ”: у випадку числових значень елементів матриць – це операція поелементного вирахування, у випадку лінгвістичних значень, операція визначається за допомогою принципу розширення Л. Заде.

Тоді матрицю  $Q = B_s \# \hat{B}$  назвемо матрицею втрат безпеки на цьому етапі.



Матриця втрат безпеки  $Q$  являє собою вхідні дані для блоку ліквідації наслідків (БЛН).

Реалізація заходів цього блоку може бути формалізована за допомогою матриці ліквідації наслідків:

$$L = \begin{pmatrix} l_{11} & l_{12} & l_{13} & l_{14} & l_{15} \\ l_{21} & l_{22} & l_{23} & l_{24} & l_{25} \\ \dots & \dots & \dots & \dots & \dots \\ l_{n1} & l_{n2} & l_{n3} & l_{n4} & l_{n5} \end{pmatrix} . \quad (2.9)$$

Результат застосування БЛН може бути записаний у такому вигляді:

$$\hat{Q} = Q \otimes L = \begin{pmatrix} \hat{q}_{11} & \hat{q}_{12} & \hat{q}_{13} & \hat{q}_{14} & \hat{q}_{15} \\ \hat{q}_{21} & \hat{q}_{22} & \hat{q}_{23} & \hat{q}_{24} & \hat{q}_{25} \\ \dots & \dots & \dots & \dots & \dots \\ \hat{q}_{n1} & \hat{q}_{n2} & \hat{q}_{n3} & \hat{q}_{n4} & \hat{q}_{n5} \end{pmatrix} . \quad (2.10)$$

Матрицю  $\hat{Q}$  назвемо матрицею залишкових втрат безпеки.

Якщо  $\hat{Q} \neq V_s$ , то такий стан системи може ініціювати появу вторинних загроз з імовірностями  $\overline{PUG}_i$ .

Таким чином, крім первинних загроз, залежно від поточного стану системи і її оточення, можуть виникнути вторинні загрози, ймовірність появи яких дорівнює  $\overline{PUG}_i$ .

Кортеж  $\bar{R}_i = (\bar{N}_i ; \overline{PUG}_i)$  назвемо ризиком реалізації  $i$ -ої вторинної загрози.

Зауважимо, що ймовірності виникнення вторинних загроз не є безумовними, як для первинних загроз. Вони залежать від поточного стану системи. З первинними загрозами починають боротися ще до їхнього настання, тобто фактично намагаються звести до мінімуму їхні наслідки, не маючи можливості вплинути на сам факт їх виникнення. У випадку з вторинними загрозами, намагаються взагалі не допустити їх, тобто нейтралізувати їх причини. Це принципова розбіжність у блоках заходів, вплив яких формалізовано множиною матриць  $Z_j$  і матрицею  $L$ .

Таким чином, на основі формалізації процесу динаміки безпеки соціально-технічних систем запропонована модель зміни рівня безпеки будь-якої системи, яка враховує ризики та наслідки реалізації загроз, а також вплив превентивних заходів

на безпеку системи. Модель слугує базовою основою методичного апарату щодо ідентифікації та оцінювання загроз і ризиків авіаціної транспортної системи.

### **2.3. Методика визначення пріоритетів показників, що характеризують рівень безпеки авіатранспортної системи**

Методика призначена для визначення ступеня важливості часткових показників під час оцінювання рівня інформаційних загроз з використанням кількісного критерію.

В основу методики покладені метод аналізу ієрархій (МАІ), методи експертного оцінювання. При цьому кількість елементів кожної ієрархії не повинна перевищувати 9 [43].

Загальна схема досліджень з визначення пріоритетів окремих показників являє собою процес планування, який починається у теперішній час  $t=0$  і закінчується в певний момент майбутнього  $t=T$ . У прямому процесі розглядаються поточні фактори і припущення, які є деяким логічним підсумком стану складної системи [38, 39].

Пріоритети окремих показників, що характеризують рівень загрози АТС, можна визначити, побудувавши відповідну ієрархію. Кількість і характер показників можна визначити, користуючись додатком 1 до Інструкції з оцінки рівня загрози безпеці цивільної авіації України [4].

Послідовність визначення пріоритетів окремих показників, що характеризують рівень безпеки, показана на рис. 2.1.

Користуючись наведеною послідовністю можна скласти узагальнюючу ієрархію визначення пріоритетів окремих показників ознак загроз (рис. 2.2). При цьому під авіаційною діяльністю розуміється діяльність фізичних та юридичних осіб у галузі авіації та/або організація повітряного руху України [40].

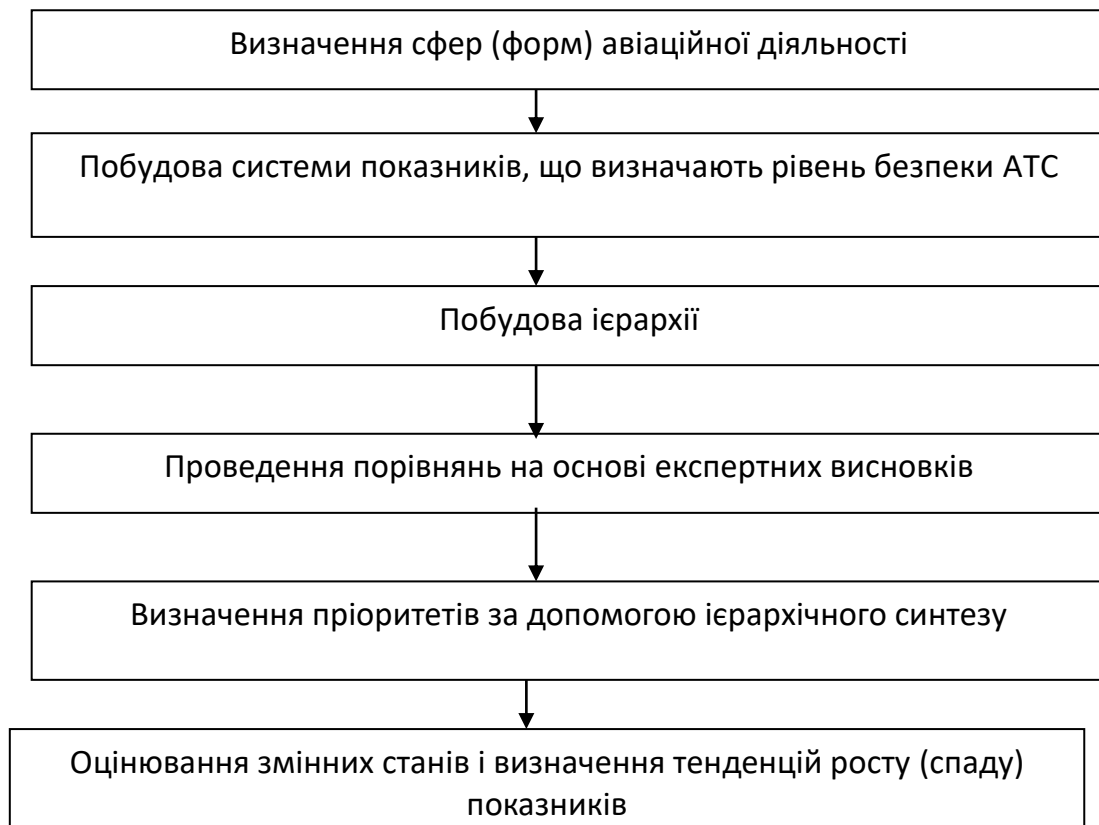


Рисунок 2.1 – Послідовність визначення пріоритетів окремих показників, що характеризують рівень безпеки АТС

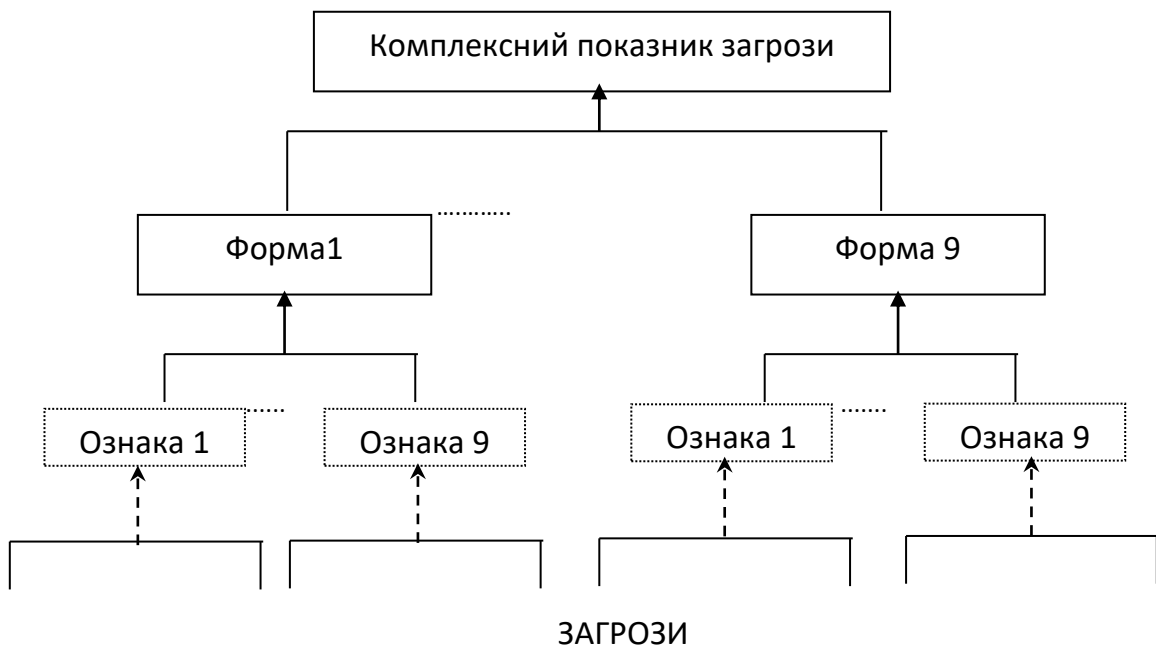


Рисунок 2.2 – Узагальнена схема ієрархії знаходження пріоритетів окремих показників, що визначають рівень безпеки

Відповідно до узагальненої схеми удосконалено методику визначення пріоритетів ознак, що характеризують рівень загрози розроблену в [42]. Суть удосконаленої методики полягає в такому:

1. Визначається множина джерел, що являють собою потенційну небезпеку для функціонування АТС, та обирається система окремих показників (ознак), що визначають рівень безпеки АТС.

2. Після окресленої загальної мети будується ієрархія знаходження пріоритетів окремих показників, що визначають рівень безпеки АТС.

3. Для кожного із нижніх рівнів ієрархії будуються матриці парних порівнянь – по одній для кожного елемента прилеглого верхнього рівня згідно з методом аналізу ієрархій (МАІ) [43]. Матриця парних порівнянь для визначення пріоритетів джерел загроз має вигляд:

$$\|A\| \rightarrow \begin{vmatrix} & B_1 & B_2 & \dots & B_n \\ B_1 & a_{11} & a_{12} & \dots & a_{1n} \\ B_2 & a_{21} & a_{22} & \dots & a_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ B_n & a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} \rightarrow \begin{vmatrix} L_{f1} \\ L_{f2} \\ \dots \\ L_{fn} \end{vmatrix}, \quad (2.11)$$

де:  $n$  – розмір матриці;

$B_1 \dots B_n$  – елементи (сфери діяльності) рівнів ієрархії;

$a_{11} \dots a_{nn}$  – значення парних порівнянь матриці;

$L_{f1} \dots L_{fn}$  – елементи власного вектора матриці, що визначають локальні пріоритети сфер діяльності.

4. Для заповнення матриць парних порівнянь використовуються міркування досвідчених експертів, які порівнюють елементи матриці згідно із шкалою відносної важливості, наведеною в табл. 2.2.

## Шкала відносної важливості елементів матриці парних порівнянь

Різниця у значеннях	Зміст
0	Значення не змінюється
2	Невелике збільшення(зменшення) значення
4	Велике збільшення(зменшення) значення
6	Значне збільшення(зменшення) значення
8	Максимальне збільшення(зменшення) значення
1, 3, 5, 7	Проміжні значення між двома суміжними міркуваннями

5. Після проведення експертами парних порівнянь і отримання власних векторів матриці, що визначають пріоритети сфер міждержавних відносин, визначається узгодженість локальних пріоритетів цієї матриці. Якщо ця узгодженість задовільна, то значення пріоритетів окремих показників, що визначають рівень загрози АТС, можна отримати, користуючись матрицями парних порівнянь нижніх рівнів:

$$\|M\| \rightarrow \begin{vmatrix} C_1 & C_2 & \dots & C_n \\ C_1 & d_{11} & d_{12} & \dots & d_{1n} \\ C_2 & d_{21} & d_{22} & \dots & d_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ C_n & d_{n1} & d_{n2} & \dots & d_{nn} \end{vmatrix} \rightarrow \begin{vmatrix} L_{f1} \times L_{p1} \\ L_{f1} \times L_{p2} \\ \dots \\ L_{f1} \times L_{pn} \end{vmatrix}, \quad (2.12)$$

де:  $n$  – розмір матриці;

$C_1 \dots C_n$  – елементи (показники ознак) рівнів ієрархії;

$d_{11} \dots d_{nn}$  – значення парних порівнянь матриці;

$L_{fi}$  – елемент власного вектора матриці, що визначає локальний пріоритет  $i$ -ї сфери діяльності;

$L_{p1} \dots L_{pn}$  – елементи власного вектора матриці, що визначають локальні пріоритети окремих показників ознак у відповідних сферах діяльності.

Блок-схема алгоритму визначення пріоритетів показників, що характеризують рівень безпеки АТС на рис. 2.3.



Рисунок 2.3 – Блок-схема алгоритму визначення пріоритетів окремих показників, що характеризують рівень АТС

За показником точності методика перевірялась із застосуванням критерію Колмогорова – Смірнова [42], що використовує емпіричну функцію розподілу

результатів спостережень. За даними розрахунків, що наведені в [42], можна зробити висновок про задовільну точність розробленої методики.

## 2.4. Комплексна методика оцінювання загроз і ризиків

Процес забезпечення безпеки авіації носить комплексний характер і ґрунтується на глибокому аналізі можливих негативних наслідків (логіко-евристичний аналіз). Такий аналіз припускає обов'язкову ідентифікацію можливих джерел загроз, факторів, що сприяють їх прояву (уразливостей), і, як наслідок, визначення актуальних загроз безпеці АТС.

Виявлення та аналіз загроз безпеці АТС є першим етапом у розробці стратегії протидії загрозам (політики безпеки). При цьому процес виявлення та аналізу загроз слід розглядати в органічному зв'язку з процесом аналізу ризиків та протидії загрозам.

Виходячи з цього принципу, моделювання й класифікацію джерел загроз, їх проявів, а також розробку ефективних заходів протидії доцільно проводити на основі аналізу взаємодії логічного ланцюжка (рис. 4.13.)

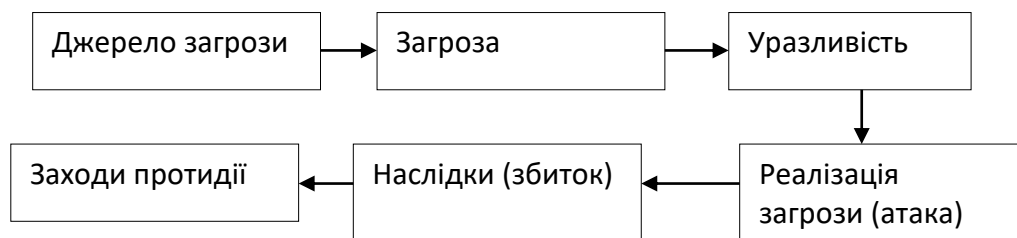


Рисунок 2.4 – Визначення заходів протидії загрозам АТС

Процес аналізу починається з визначення основних загроз та їх джерел (табл. 2.3 – 2.4) .

Таблиця 2.3

Перелік загроз безпеці АТС (зразок)

№ загрози	Зміст загрози
1	Загроза 1
2	Загроза 2
...	...
n	Загроза n

Таблиця 2.4

Перелік джерел загроз безпеці АТС (зразок)

№ джерела	Джерело
1	Джерело 1
2	Джерело 2
...	...
n	Джерело n

На основі ідентифікованих загроз та їх джерел складаються [таблиці](#) методів реалізації загроз (атак), можливих у зазначеній сфері авіаційної діяльності, й уразливостей об'єктів, якими ці атаки можуть скористатися (табл.2.5 – 2.6).

Таблиця 2.5

Перелік методів реалізації загроз (зразок)

№ атаки	Атака
1	Атака 1
2	Атака 2
...	...
n	Атака n

Таблиця 2.6

Перелік уразливостей об'єктів забезпечення безпеки АТС (зразок)

№ уразливості	Уразливість
1	Уразливість 1
2	Уразливість 2
...	...
n	Уразливість n

Уразливості, притаманні певним об'єктам забезпечення безпеки АТС. Об'єкти забезпечення зводяться у таблицю (табл. 2.7).

Таблиця 2.7

Перелік об'єктів забезпечення ї безпеки АТС (зразок)

№ об'єкта	Об'єкт
1	Об'єкт 1
2	Об'єкт 2
...	...
n	Об'єкт n



У такий же спосіб виділяються заходи забезпечення безпеки. Перелік заходів забезпечення безпеки наведений в табл. 2.8.

Таблиця 2.8

Перелік заходів забезпечення безпеки (зразок)

№ заходу	Зміст заходу
1	Захід 1
2	Захід 2
...	...
n	Захід n

Таким чином, на першому етапі аналізу загроз ідентифікуються всі елементи множин загроз, джерел, об'єктів і заходів забезпечення безпеки АТС .

Взаємодія різних факторів, що впливають на безпеку, має істотне значення для оцінювання їх кінцевої значущості та, відповідно, для визначення найбільш доцільних і ефективних заходів і засобів підвищення рівня безпеки.

Тому на цьому етапі роботи необхідно експертним методом встановити відносини між такими видами елементів.

“Джерела загроз – загрози”, тобто встановити джерело, які загрози воно породжує.

“Загрози – атаки”, тобто встановити загрозу, через яку атаку вона реалізується.

“Атаки – уразливості”, тобто встановити атаку, яку вона використовує уразливість.

“Уразливості – об'єкти захисту”, тобто встановити уразливість, до якого об'єкта захисту вона належить.

“Заходи протидії – загрози”, тобто встановити захід, якій загрозі протистоїть.

Результати такого аналізу подані в матричній формі на основі припущення, що між елементами множин можна встановити певне бінарне відношення “є причиною”. У табл. 2.9 наведено варіант матриці відносин “Джерела загроз – загрози” (“1” відповідає припущенню, що це джерело породжує цю загрозу; “0” – відсутність відносин між елементами множин.

На цьому етапі аналізується визначення відносин між елементами цих множин. [Джерело](#) загроз 1 (наприклад, терористичні організації іноземних держав) має пряму зацікавленість як в отриманні конфіденційної інформації про діяльність АТС, так і у впливі на неї, що призводить до ускладнення її діяльності.

Таблиця 2.9

Матриця відносин “Джерела загроз – загрози” (варіант)

		Загрози								
		1	2	3	4	5	6	7	8	9
Джерела загроз	1	1	1	0	0	0	1	0	0	0
	2	0	0	1	1	0	0	0	1	1
	3	0	1	0	0	0	0	0	0	0
	4	0	0	0	0	1	1	1	0	0

Аналогічно аналізуються відносини між усіма джерелами та загрозами.

У табл. 2.10 наведено варіант матриці відносин загроз і атак. Для зручності розміщення матриця переорієнтована. Номери елементів множин взяті з таблиць 2.3 – 2.8.

Таблиця 2.10

Матриця відносин “Загрози – атаки” (варіант)

		Загрози								
		1	2	3	4	5	6	7	8	9
Атаки	1	1	1	0	0	0	1	0	0	0
	2	0	0	1	1	0	0	0	1	1
	3	0	1	0	0	0	0	0	0	0
	4	0	0	0	0	1	1	1	0	0

У табл. 2.11 наведено варіант матриці відносин “Атаки – уразливості”, що ілюструє результати аналізу атаки, уразливості, які вона використовує. Номери елементів множини беруться з таблиць 2.3 – 2.8.

Таблиця 2.11 – Матриця відносин “Атаки – уразливості” (варіант)

		Уразливості				
		1	2	3	4	5
Атаки	1	1	0	0	0	1
	2	0	1	0	1	0
	3	0	1	0	0	0
	4	1	0	1	0	1

Аналіз відносин атак і уразливостей особливо важливий, тому що ілюструє відносини об’єкта забезпечення з навколишнім середовищем, показуючи, уразливості, які реалізації загроз можуть використовувати.

У таблиці 2.12 наведено варіант матриці відносин “Уразливості – об’єкти забезпечення безпеки”. Номери елементів множин [відповідають](#) номерам у табл.2.7 – 2.8.

Таблиця 2.12 – Матриця відносин “Уразливості – об’єкти забезпечення безпеки” (варіант)

Уразливість		Об’єкт забезпечення безпеки			
		1	2	3	4
	1	1	1	0	1
	2	1	0	0	0
	3	0	0	1	1
	4	0	0	1	0
	5	0	0	1	1

У цій матриці визначається, об’єкт, його уразливість. Таким чином, відстежується атака, на який об’єкт вона спрямована.

Табл. 2.13 містить варіант матриці відносин “Заходи протидії – загрози”.

Таблиця 2.13 – Матриця відносин “Заходи протидії – загрози” (варіант)

		Загрози								
		1	2	3	4	5	6	7	8	9
Заходи забезпечення безпеки	1	1	1	1	1	1	1	1	1	1
	2	0	0	0	0	0	0	1	0	0
	3	1	1	0	0	0	1	0	0	0
	4	0	0	0	0	0	1	1	0	0
	5	1	1	1	0	0	0	0	1	0
	6	0	0	0	0	0	0	0	0	1

Після аналізу відносин між елементами множин, виділених у процесі ідентифікації, оцінюються ризики. Цей процес дає змогу мінімізувати витрати ресурсів на заходи протидії. У процесі аналізу можливих і виявлення актуальних загроз оцінюється ризик, що виникає внаслідок потенційного впливу певної загрози.

Відомо декілька різних методик аналізу та оцінювання ризиків (переважно закордонних). Усі вони дають змогу отримати лише якісну їх оцінку на основі експертних методів.

З урахуванням міркувань, викладених у попередніх розділах, стосовно АТС оцінювання ризиків полягає в такому.

Ризик визначається як оцінювання можливості реалізації загроз безпеці, пов'язаних з уразливістю, властивими тим чи іншим об'єктам захисту. На основі аналізу впливу загроз їм приписується високий, середній або низький рівень ризику по кожній зоні локалізації уразливостей [45].

Під час оцінювання ризиків розглядаються три основні категорії втрат унаслідок реалізації загроз. Ці категорії втрат і їх опис наведено в табл. 2.14.

Матриця оцінки ризиків розділена на зони локалізації уразливостей. В рамках кожної уразливості перераховуються потенційні загрози. Справа від кожної загрози наводяться рівні в рамках категорій втрат.

Таблиця 2.14 – Категорії наслідків реалізації загроз (втрат)

Категорії наслідків	Опис наслідків
Фінансові збитки	Визначаються збільшенням витрат на відновлення та удосконалення технічних засобів, елементів інфраструктури, виробничої бази тощо
Зниження ефективності функціонування АТС	Визначається неспроможністю елементів АТС ефективно виконувати покладені на них завдання внаслідок: зниження рівня морально-психологічного стану персоналу, а також змін в стані психіки (психічного здоров'я); зниження мотивації персоналу до виконання польотів тощо. порушення функціонування системи управління повітряним рухом, повітряною навігацією; несправності (виведення з ладу) технічних засобів аеропортів, наземного обслуговування; порушення властивостей інформації, яка циркулює в кібернетичному просторі авіаційної галузі (конфіденційність, доступність, цілісність, спостережуваність)
Ускладнення діяльності АТС	Стосується ситуацій, що впливають на втрату суспільної довіри до авіаційного транспорту України та погіршення його іміджу

Матриця заповнюється доданням рівня ризику – високого (В), середнього (С) або низького (Н), щоб показувати залежність кожної загрози від кожної із зон локалізації уразливості з урахуванням заповненої раніше матриці “Загрози – об’єкт забезпечення безпеки”. Варіант матриці оцінювання ризиків наведений в табл. 2.15.

Таблиця 2.15 – Матриця оцінювання ризиків (варіант)

Об’єкти безпеки	Ризик грошової втрати			Ризик втрати продуктивності			Ризик ускладнення діяльності		
			Н		С		В		Н
Загроза 1			Н		С		В		
Загроза 2		С		В					Н
...			Н			Н		С	
Загроза n		С		В				С	

Опис рівнів ризику:

**високий:** значна грошова втрата, втрата продуктивності або ускладнення діяльності, є результатом загрози внаслідок відповідної уразливості;

**середній:** номінальна грошова втрата, втрата продуктивності або виникають певні ускладнення діяльності;

**низький:** або мінімальна можливість грошової втрати, або втрати продуктивності мінімальні чи не існують.

Після заповнення матриці оцінювання ризиків стає зрозумілим розподіл загроз і втрат від їх можливої реалізації за всіма об'єктами безпеки.

Подальшим етапом оцінювання ризиків є своєрідне підбиття підсумку – складання таблиці оцінювання ризиків.

Таблиця оцінювання ризиків заповнюється за допомогою додання об'єднаного рівня ризику кожної із зон уразливості. Об'єднаний рівень ризику необхідно отримати з усіх загроз, попередньо ідентифікованих, виходячи з матриці оцінювання ризиків.

Варіант оцінювання ризиків наведений в табл. 2.16.

За результатами аналізу складається граф протидії загрозам (рис. 2.5). На рис.2.5 позначено: Дж – джерело загрози; З – загроза; А – атака; О – об'єкт безпеки; Вр – уразливість об'єкта безпеки; Зх – захід протидії.

Таблиця 2.16 – Таблиця оцінювання ризиків (варіант)

Об'єкти безпеки	Категорія наслідків			
	Фінансові збитки	Зниження ефективності функціонування АТС	Ускладнення діяльності АТС	Загальний ризик
Повітряні судна	Середній	Високий	Високий	Високий
Технічні засоби ОПР	Середній	Високий	Середній	Середній
Засоби ІАО та АТО	Середній	Середній	Середній	Середній
Програмно-технічні засоби системи зв'язку	Середній	Середній	Середній	Середній
Співробітники	Високий	Високий	Високий	Високий

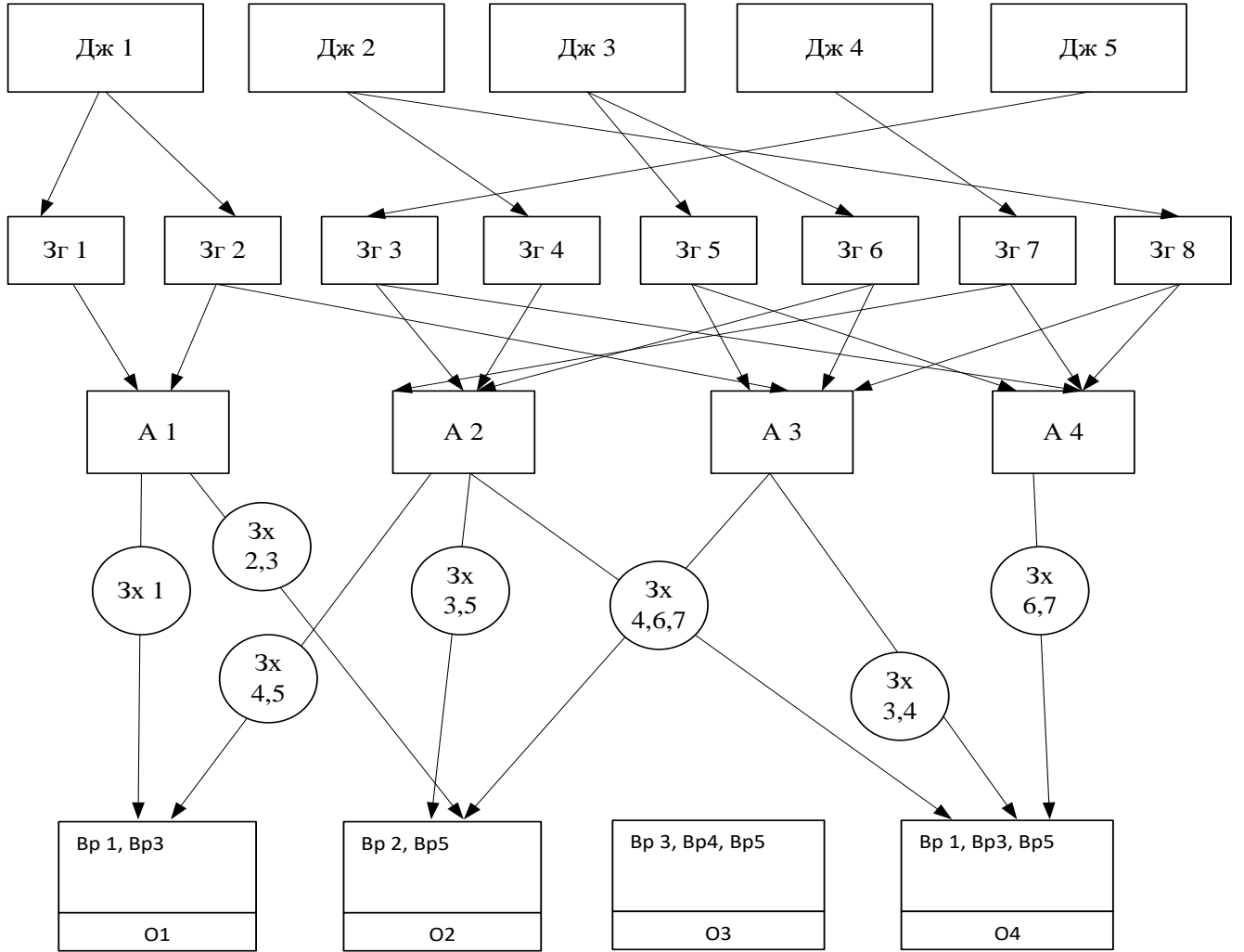


Рисунок 2.5 – Граф оцінювання загроз та ризиків (варіант)

Блок-схема алгоритму методики наведена на рис.2.6.

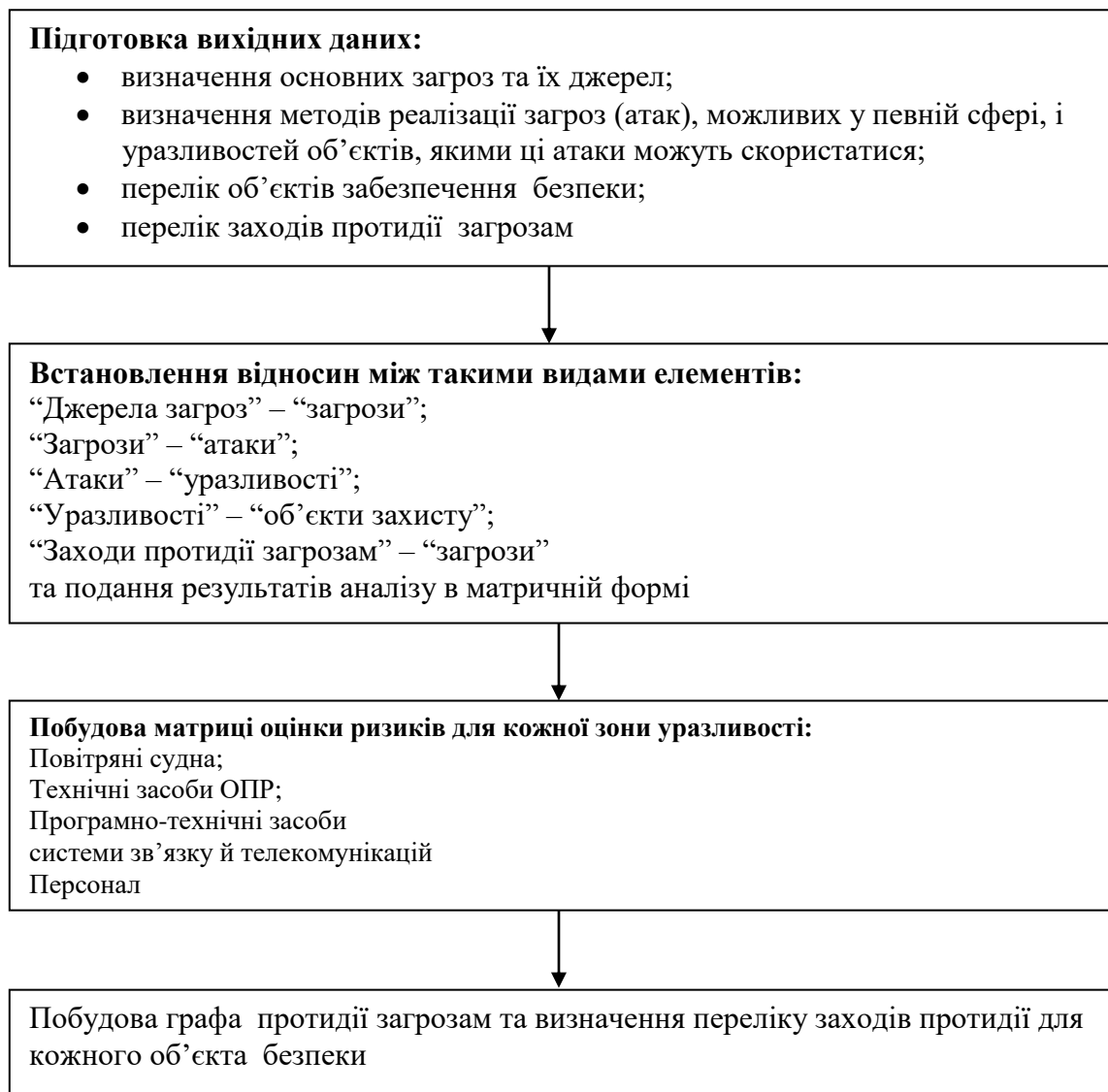


Рисунок 2.6. Блок-схема алгоритму методики оцінювання загроз та ризиків

### **Висновки до розділу**

1. Внаслідок проведеного концептуального аналізу поняття комплексної безпеки встановлено, що діяльність із забезпечення безпеки виникає в ході вирішення протиріччя між небезпекою й потребою управляти безпекою: передбачати, запобігати, локалізувати й усувати збиток від впливу небезпеки

2. Специфічними особливостями завдання створення систем забезпечення безпеки є:

неповнота й невизначеність вихідної інформації про склад і характер загроз;

багатокритеріальність завдання, що пов'язано з необхідністю урахування великої кількості часткових показників;



наявність як кількісних, так і якісних показників, які необхідно враховувати при вирішенні завдань розробки та впровадження систем забезпечення безпеки; неможливість застосування класичних методів оптимізації.

3. Визначено, що математична модель оцінки рівня комплексної безпеки системи може бути представлена у вигляді кортежу, який включає в себе орієнтований граф, накладену на цей граф систему переваг одних факторів іншим і набір якісних оцінок рівнів кожного фактора в ієрархії.

4. Розроблено методику знаходження пріоритетів окремих показників, що визначають рівень небезпеки (загрози) та дають змогу:

отримувати кількісні значення пріоритетів окремих показників, що визначають рівень небезпеки (загрози) авіаційної діяльності;

отримувати оціночні значення тенденції зростання (спадання) окремих показників для певного проміжку часу.

5. Розроблено методику та алгоритм оцінки загроз та ризиків АТС, які дають змогу визначати заходи протидії інформаційним загрозам на підставі результатів аналізу можливих і виявлення актуальних загроз, оцінювання можливих ризиків, що виникають внаслідок реалізації певної загрози, можливих негативних наслідків загроз, ідентифікації можливих джерел загроз, факторів, що сприяють їх прояву (уразливостей).

## **РОЗДІЛ 3 РЕКОМЕНДАЦІЇ ЩОДО ЗАСТОСУВАННЯ РОЗРОБЛЕНОГО МЕТОДИЧНОГО АПАРАТУ ДЛЯ ІДЕНТИФІКАЦІЇ ЗАГРОЗ ТА ОЦІНКИ РИЗИКІВ ДІЯЛЬНОСТІ ТРАНСПОРТНОЇ СИСТЕМИ (КОМПЛЕКСУ)**

### **3.1. Рекомендації щодо удосконалення методичної бази оцінювання загроз та ризиків в авіапідприємствах**

В Україні на державному рівні ухвалено Інструкцію з оцінки ризиків та загроз безпеці цивільної авіації [4]. Вимоги Інструкції поширюються на національне відомство цивільної авіації, а також на експлуатантів аеродромів/аеропортів,

експлуатантів повітряних суден і постачальників аеронавігаційного обслуговування. На основі Інструкції експлуатанти аеродромів (аеропортів), експлуатанти повітряних суден і постачальники аеронавігаційного обслуговування розробляють свої власні керівництва та проводять оцінку ризиків і загроз. Інструкція містить методику оцінки ризиків і загроз безпеці цивільної авіації, яка повністю відповідає відповідній методиці ІКАО.

Інструкція запроваджує системний підхід до управління ризиками в галузі безпеки цивільної авіації з метою забезпечення захисту цивільної авіації від актів незаконного втручання, а також здійснення заходів авіаційної безпеки, що відповідають характеру та рівню загрози.

Разом з тим, в Інструкції не конкретизовано такі аспекти, як:

способи надання людських і матеріальних ресурсів для ефективної оцінки ризиків і загроз;

способи розроблення та впровадження відповідних превентивних заходів авіаційної безпеки для зниження ризику незаконного втручання до прийняттого рівня;

координація та співпраця (на державному рівні) органів виконавчої влади та правоохоронних органів, які беруть участь у реалізації Державної програми забезпечення безпеки цивільної авіації, з метою своєчасного отримання інформації від відомства цивільної авіації та авіаційних організацій щодо оцінки рівня ризиків та загроз відповідно до критеріїв (ймовірність та наслідки людських жертв і втрати матеріальних ресурсів унаслідок вчинення актів незаконного втручання); застосування стандартизованої методики оцінки ризиків і загроз; впровадження та просування культури безпеки авіаційними організаціями.

Тому в діяльність авіакомпаній доцільно впровадити такий механізм оцінювання загроз і ризиків.

### ***Визначення загрози та критеріїв уразливості***

Для відпрацювання методики оцінки ступеня загрози щодо визначення характеру ймовірної загрози застосовано системний, кількісний підхід. В основу

такого підходу покладено три основних принципи забезпечення АБ, а саме: визначення, реалізація та підтримка.

Під час вирішення задачі оцінки ступеня загрози використовується інформація, факти і статистичні дані спеціально уповноваженого органу з питань авіаційної безпеки цивільної авіації, служб авіаційної безпеки аеропортів та авіакомпаній, юридичних осіб, що входять до складу аеропортових комітетів із забезпечення авіаційної безпеки.

При оцінці шляхів вибору ключових моментів встановлення рівня загрози та критеріїв уразливості визначають їх чинники, які вважаються тими, що мають найбільшу вагу або значення в даному процесі.

Ключові моменти змінюються залежно від існуючої системи, що діє в регіоні, аеропорту, авіакомпанії або групі людей, на період визначення загрози та критеріїв уразливості.

Перед проведенням оцінки того, яким чином може реалізуватись загроза (наприклад акт незаконного втручання в діяльність ЦА) може бути здійснено стосовно того або іншого об'єкту, необхідно розглянути причини або мотиви, у зв'язку з якими може реалізуватись загроза, сам об'єкт та оцінити ймовірність реалізації загрози (атаки).

Наприклад, для АНВ основними мотивами можуть бути:

політичні;

релігійні;

конкурентна боротьба;

намагання отримати матеріальні коштовності (у тому числі гроші);

зведення особистих рахунків;

цікавість;

немотивована дія під впливом алкоголю або інших речовин, у тому числі наркотиків.

Основними методами здійснення актів незаконного втручання в діяльність цивільної авіації можуть бути (реалізація загрози АНВ):

руйнування або пошкодження повітряних суден, об'єктів радіонавігаційного забезпечення та інших споруд аеропорту, аеродрому, а також його служб;

створення перешкод функціонуванню повітряним суднам, об'єктам радіонавігаційного забезпечення та іншим спорудам аеропорту, аеродрому, а також їх службам, яке загрожує безпеці повітряних суден під час польоту;

фізичне знищення пасажирів, персоналу аеропортів та авіакомпаній або погіршення умов їх життєдіяльності;

крадіжка або знищення інформації, матеріальних коштовностей.

***Наступний етап полягає у створенні робочих інструментів, які призначені для надання допомоги у процесі оцінки.***

Робочий інструмент, який використовується в даній методиці, отримав назву “матриця уразливостей”. Для отримання кінцевого результату аналізу, з метою визначення заходів безпеки відповідно до рівня загрози ЦА, можуть бути об'єднані дві матриці, що надані у додатках 1, 2 до Інструкції з організації та здійснення контролю на безпеку в аеропортах України [46]. Це можливо за допомогою методики, наведеної у п. 2.4.

Для оцінки загрози безпеці аеропорту „матрицю уразливості” №1 (додаток 1), а саме в „матриці уразливості” №1 (додаток 1) відображені характеристики групи осіб, які здатні здійснити АНВ.

У матриці уразливості №2 (додаток 2, 3) відображені „категорії загроз авіаційній безпеці” та їх оціночні показники.

Її можливо модифікувати стосовно оцінки загрози щодо потенціального об'єкту, наприклад, аеропорт, або для оцінки рівня авіаційної безпеки авіакомпанії чи регіону виконання авіаційних робіт (додаток 3).

Характеристика групи

Під час відпрацювання “матриці уразливості” №1, яка характеризує деяку групу людей, необхідно виходити з припущення про те, що більшість „систем”, які складаються з людей, можливо класифікувати за п'ятьма основними ознаками, а саме:

керівництво;

сутність системи;  
інфраструктура;  
контингент;  
механізм боротьби.

Поняття „керівництво” складається, серед іншого, з ієрархічної структури групи, наявності законного політичного представництва та використання авторитета лідерів.

„Сутність системи” характеризується як намагання та поривання групи реалізувати в життя свої теоретичні цілі, а саме: політичну програму або релігійні переконання, за допомогою проведення розвідувальних операцій, придбання зброї, розширення джерел фінансування та підготовки виконавців.

Складовими частинами „інфраструктури” є:  
розмір та кількість осередків або підрозділів групи;  
налагоджена мережа зв'язку;  
ефективне використання транспортних шляхів і каналів постачання.

Під поняттям „контингент” розуміється наявність численній мережі з боку співчуваючих місцевих жителів або інших людей, які підтримують діяльність групи.

Ознака „механізм боротьби” присвоюється групі, яка веде активні дії для досягнення своїх цілей. Членів групи, які приймають участь у таких діях, можливо називати бойовиками, повітряними піратами, підривниками-смертниками, „спеціалістами”, які виготовляють вибухові пристрої.

Категорії загроз авіаційній безпеці

“Матриця уразливості” №2 складається виходячи з шести категорій загрози. Цю матрицю можливо розширити за рахунок додаткових факторів, які вважаються важливими на даний час.

До категорії загрози відносяться такі чинники:

наявність групи, яка здатна здійснити АНВ;  
дані про акції, які були здійснені проти цивільної авіації в минулому;  
наявність внутрішніх конфліктів;  
стан економічної кризи;

загальна кількість рейсів;  
рейси підвищеного ризику.

Ці ключові моменти здебільшого підходять для оцінки загрози на регіональному рівні, авіакомпаніям та аеропортам.

Після підсумовування оціночних показників, які надані категоріям загрози (додаток 3), отримують кількісний метод прогнозування ступеня загрози для мети, відносно якої здійснювався аналіз. Якщо дану суму порівняти з сумарною величиною характеристики групи, то отримаємо результат, який можна безпосередньо віднести до об'ємів відповідних заходів щодо забезпечення безпеки, які будуть спільномірні з оціночним показником ступеня загрози.

#### Заключний аналіз

Для проведення заключного аналізу необхідно:

задати критерії, які необхідно оцінити;

заповнити всі графи відповідно до оціночних показників;

скласти підсумкові значення відповідно до кожної лінійки та кожного стовпця;

призначити пріоритети заходам таким чином, щоб більшому оціночному показнику відповідала більш висока ступінь загрози та уразливості.

Будь-яка оцінка загрози повинна супроводжуватися докладним поясненням з обґрунтуванням висновків.

Добре обґрунтоване пояснення буде основою підсумкової програми щодо організації попереджувальних ефективних заходів із забезпечення захисту, охорони та безпеки пасажирів, членів екіпажу, авіаційного персоналу, повітряних суден, об'єктів аеропорту.

#### ***Адекватні заходи безпеки відповідно до рівня загрози безпеці цивільної авіації***

Додаткові заходи щодо забезпечення авіаційної безпеки аеропортів та експлуатантів можуть бути вжити як на постійній, так і на тимчасовій основі, залежно від отриманої інформації про загрозу, а також щодо аеропорту, окремої його зони або об'єкта, повітряного судна.

З урахуванням Методики, розробленої в п. 2.4 планування адекватних заходів безпеки відповідно до рівня загрози здійснюється у такій послідовності:

здійснити оцінку загрози, проаналізувати характер і ступінь загрози для аеропорту або експлуатанта, виходячи з достовірної оцінки загрози ;

визначити тривалість існування підвищеного ступеня загрози;

ознайомитися з розташуванням і функціонуванням об'єктів, які можуть піддаватися актам незаконного втручання;

здійснити облік співробітників служби авіаційної безпеки, відповідного обладнання;

проаналізувати існуючі на даний час заходи авіаційної безпеки в аеропорту;

визначити кількість рейсів і пасажирів, а також об'єм багажу та вантажу, які потребують додаткових процедур контролю на безпеку.

План адекватного посилення заходів безпеки аеропорту відповідно до рівня загрози безпеці цивільної авіації відпрацьовується аеропортовим комітетом з авіаційної безпеки завчасно.

Для розподілу зусиль (ресурсів) служби авіаційної безпеки у разі відсутності інших даних використовують таблицю 1 (додаток 4).

Ранг важливості кожного завдання або напряму встановлюється за Методикою визначення пріоритетів показників, що характеризують рівень безпеки авіатранспортної системи (п. 2.3) з урахуванням обставин, що склалися на даний час. Найбільш важливому завданню або напряму дій присвоюють найменший порядковий номер рангу важливості.

Оцінювання ризиків і загроз безпеці цивільної авіації проводиться робочою групою відомства цивільної авіації на регулярній основі. Щоб мати право брати участь у цьому органі, члени такої робочої групи повинні мати не менше трьох років практичного досвіду в галузі авіаційної безпеки, пройти навчання з управління ризиками та набути знань, що стосуються способів і засобів вчинення актів незаконного втручання.

Робоча група авіаційної організації проводить оцінку ризиків і загроз для експлуатантів аеродромів/аеропортів, експлуатантів повітряних суден і

постачальників аеронавігаційного обслуговування. Цю робочу групу має очолювати заступник директора з авіаційної безпеки.

Експлуатанти аеродромів/аеропортів, експлуатанти повітряних суден і постачальники аеронавігаційного обслуговування щоквартально оцінюють рівень ризиків і загроз.

Крім того, експлуатанти повітряних суден оцінюють рівень ризиків і загроз перед виконанням кожного польоту. Ґрунтуючись на результатах своїх власних оцінок, а також на результатах відповідних оцінок, проведених відомством цивільної авіації, експлуатанти аеродромів/аеропортів, експлуатанти повітряних суден і постачальники аеронавігаційного обслуговування запроваджують і реалізують належні заходи авіаційної безпеки для захисту цивільної авіації від актів незаконного втручання. Ці заходи мають бути співмірними з характером і рівнем загрози.

Результати, отримані в результаті оцінки ризиків і загроз, надаються відомству цивільної авіації. У разі отримання інформації про загрозу з будь-якого джерела експлуатанти аеродромів/аеропортів, експлуатанти повітряних суден і постачальники аеронавігаційного обслуговування повинні провести додаткову оцінку ризиків і загроз.

### **3.2. Методичні рекомендації щодо оцінювання факторів ризику для безпеки польотів**

Управління факторами ризику для безпеки польотів один з ключових компонентів системи управління безпекою польотів. Термін “управління факторами ризику для безпеки польотів” покликаний провести межу між зазначеною функцією та управлінням фінансовим, юридичним, економічним ризиком тощо. У цьому розділі викладаються основоположні поняття, пов'язані з факторами ризику для безпеки польотів, включно з такими питаннями:



- a) визначення фактора ризику для безпеки польотів;
- b) імовірність факторів ризику для безпеки польотів;
- c) ступінь серйозності факторів ризику для безпеки польотів;
- d) допустимість факторів ризику для безпеки польотів; а також
- e) управління факторами ризику для безпеки польотів.

Визначення фактора ризику для безпеки польотів

Фактор ризику для безпеки польотів являє собою прогнозовану ймовірність і серйозність наслідків або результатів, викликаних наявним небезпечним фактором або ситуацією. Хоча результатом може бути й авіаційна подія, "проміжна небезпечна дія/наслідок" може бути визначена як "найбільш правдоподібний результат". Засоби з виявлення подібних багаторівневих наслідків зазвичай асоціюються зі складними комп'ютерними програмами зі зменшення ризиків. Відомість зменшення ризиків для безпеки польотів, проілюстрована в додатку 2 до цього розділу, також використовує такі засоби.

### ***Реальні та потенційні ризики для безпеки польотів***

Будь-яка подія, що стосується безпеки польотів, та яка фактично призводить до авіаційної події (катастрофи чи аварії) чи серйозного інциденту, або має значення індексу ризику в середині зазначеного діапазону представлений в Таблиці 3, серйозність наслідків події за шкалою ІКАО відповідає категорії «С» і вище), визначається як подія, що складає реальний або потенційний ризик для безпеки польотів у сфері цивільної авіації України.

### **Ключові сфери ризику [48]**

**Ключова сфера ризику** – це перелік категорій, які використовуються для визначення потенційного наслідку події. До цього переліку слід віднести такі категорії.

**Зіткнення у повітряному просторі** (airborne collision): зіткнення двох повітряних суден в небі або зіткнення повітряного судна із іншим об'єктом, що знаходиться у повітряному просторі (за винятком птахів і диких тварин).

**Небезпечне просторове положення ПС (aircraft upset):** небажаний стан повітряного судна, що характеризується ненавмисним відхиленням від звичайних експлуатаційних параметрів польоту, що в кінцевому підсумку може призвести до неконтрольованого зіткнення із землею.

**Зіткнення на злітно-посадковій смузі (collision on runway):** зіткнення повітряного судна з іншим об'єктом (іншим повітряним судном, транспортними засобами тощо) або людиною, що сталося на злітно-посадковій смузі аеродрому або в іншій зоні, призначеній для посадки ПС. Це не включає зіткнення з птахами або дикими тваринами.

**Викочування (excursion):** події, при якій повітряне судно сходить зі злітно-посадкової смуги, з робочої площі аеродрому або з посадкової поверхні будь-якої іншої заздалегідь встановленої зони посадки, не підіймаючись у повітря. Це включає вертикальні посадки з сильним ударом для гвинтокрилів або повітряних суден з вертикальним зльотом і посадкою, а також аеростатів або дирижаблів.

**Пожежа, дим та розгерметизація (fire, smoke and pressurization):** події, що включають випадки загоряння, задимлення, виділення чаду або розгерметизації, які можуть створити умови, несумісні з життям людини. Це охоплює випадки загоряння, задимлення або виділення чаду у будь-якій частині повітряного судна на землі або в повітрі, які не є результатом зіткнення або зловмисних дій

**Пошкодження на землі (ground damage):** пошкодження повітряного судна в ході наземної експлуатації на будь-яких наземних зонах, окрім злітно-посадкової смуги або інших зон, призначених для посадки, а також пошкодження під час технічного обслуговування.

**Зіткнення з перешкодою в польоті (obstacle collision in flight):** зіткнення повітряного судна у повітряному просторі з перешкодами, які мають перевищення відносно земної поверхні. Перешкоди включають високі будівлі, дерева, силові кабелі, телеграфні дроти і антени, а також прив'язні об'єкти.

**Зіткнення із землею поверхнею (terrain collision):** події, при яких повітряне судно, що знаходиться у повітряному просторі, стикається із землею поверхнею за відсутності свідчень того, що екіпаж втратив контроль над повітряним судном.

Сюди входять випадки, коли на льотний екіпаж впливають зорові ілюзії або погіршена візуальна обстановка.

**Інші травми** (other injuries): події, при яких були заподіяні смертельні або несмертельні травми, які не можуть бути віднесені до будь-якої іншої сфери ризику.

**Акт незаконного втручання в діяльність цивільної авіації.** Сюди входять всі інциденти і порушення, пов'язані зі спостереженням та захистом, контролем доступу, скринінгом, реалізацією засобів контролю АБ і будь-якими іншими діями, які спрямовані на знищення повітряних суден та майна зі злим умислом і створюють загрозу або призводять до незаконного втручання в діяльність цивільної авіації та її об'єктів. Включає події, пов'язані як з фізичною безпекою, так з кібербезпекою.

### ***Імовірність факторів ризику для безпеки польотів***

Процес взяття під контроль факторів ризику для безпеки польотів починається з оцінки ймовірності того, що наслідки небезпечних факторів реалізуються під час авіаційної діяльності організації. Імовірність факторів ризику для безпеки польотів визначається як можливість виникнення або повторення небезпечної події чи результату. Визначити можливість такої ймовірності можна, наприклад, за допомогою таких запитань:

- a) Чи відбувалися в минулому події, аналогічні події, що розглядається, чи це одиничний випадок?
- b) Яке інше обладнання або компоненти цього ж типу могли б мати аналогічні дефекти?
- c) Кількість співробітників, які виконують ці процедури або яких вони стосуються?
- d) Який відсоток часу, упродовж котрого використовується обладнання або процедура, що викликає сумнів?
- e) Наскільки серйозні наслідки організаційного, управлінського або регламентуючого характеру, які могли б вказувати на наявність більш істотних факторів загрози для безпеки людей?

Будь-які чинники, що зумовлюють ці запитання, допомагають оцінити ймовірність існування небезпечних факторів з урахуванням усіх потенційно можливих сценаріїв. Визначення можливості виникнення загрози використовується при визначенні ймовірності факторів ризику безпеки польотів.

Необхідно підкреслити, що це всього лише приклад, і рівень деталізації та складності таблиць і матриць слід порівнювати з конкретними потребами та складністю виробничих завдань різних організацій. Крім того, необхідно зазначити, що в організаціях можуть використовуватися як якісні, так і кількісні критерії (до 15 різних значень).

### ***Стратегія реалізації***

Слід враховувати такі моменти в процесі виявлення небезпечних факторів:

a) фактори проектування, включно з конструкцією обладнання та розробленням завдань;

b) обмеження для людської діяльності (фізіологічні, психологічні та пізнавальні);

c) процедури та експлуатаційну практику, включно з відповідною документацією та контрольними картами, а також їхнє апробування в реальних експлуатаційних умовах;

d) зв'язок, включно з відповідними засобами, термінологією та мовою;

e) організаційні фактори, такі як політику компанії в галузі найму, підготовки та закріплення працівників, сумісність виробничих завдань і завдань із забезпечення безпеки польотів, виділення ресурсів, напружені виробничі умови та корпоративну культуру безпеки польотів;

f) фактори виробничого середовища авіаційної системи (навколишній шум і вібрацію, температуру, освітлення та наявність захисних засобів і спецодягу);

g) фактори нормативного нагляду, включно із застосуванням і забезпеченням виконання правил; сертифікацією обладнання, атестацією персоналу та затвердженням процедур;

h) систему моніторингу ефективності діяльності, здатну виявити практичний зсув або експлуатаційні відхилення;

i) фактори взаємодії "людина - машина".

Небезпечні фактори можуть бути виявлені за допомогою проактивних і прогностичних методів або в результаті розслідування авіаційних подій чи інцидентів. Є безліч джерел виявлення небезпечних чинників, які можуть перебувати як усередині організації, так і поза нею. До прикладів внутрішніх джерел виявлення небезпечних факторів, наявних в організації, належать:

a) програми моніторингу діяльності в штатних умовах (напр., аналіз польотних даних для експлуатантів повітряних суден);

b) системи добровільного та обов'язкового подання даних про безпеку польотів;

c) обстеження стану безпеки польотів;

d) перевірки стану безпеки польотів;

e) зворотний зв'язок від підготовки персоналу;

f) розслідування авіаційних подій та інцидентів і звіти про подальші дії.

До прикладів зовнішніх джерел виявлення небезпечних чинників належать:

a) галузеві звіти про події;

b) державні системи обов'язкового подання даних про інциденти;

c) державні системи добровільного подання даних про інциденти;

d) державний контроль і перевірки;

e) системи обміну інформацією.

Види технологій, що використовуються в процесі виявлення небезпечних чинників, залежать від масштабу і складності структури організації постачальника обслуговування і його авіаційної діяльності. У будь-якому разі процес виявлення небезпечних чинників постачальником обслуговування чітко описаний у документах організації про СУБП і забезпечення безпеки польотів. У процесі виявлення небезпечних факторів розглядаються всі можливі небезпечні фактори, які можуть існувати у сфері авіаційної діяльності постачальника обслуговування, включно із взаємодією з іншими системами, як усередині, так і поза організацією. Після того як буде виявлено небезпечні фактори, необхідно визначити їхні наслідки

(тобто будь-які конкретні події або результати). Інструктивний матеріал про систему добровільного та конфіденційного подання даних в організації наведено в [48].

### ***Управління факторами ризику для безпеки польотів***

Постачальники обслуговування повинні забезпечити, щоб фактори ризику для безпеки польотів, які трапляються в авіаційній діяльності, контролюються з тим, щоб досягти цільових показників ефективності забезпечення безпеки польотів. Цей процес відомий як управління факторами ризику для безпеки польотів і включає виявлення небезпечних чинників, оцінку факторів ризику для безпеки польотів та здійснення належних заходів щодо їх зменшення. Процес управління факторами ризику для безпеки польотів представлено на рис. 3.1.

У рамках компонента управління факторами ризику для безпеки польотів систематично виявляються небезпечні фактори, що існують у процесі надання продукції та послуг. Небезпечні фактори можуть бути наслідком систем, що мають дефекти в конструкції, технічних функціях, інтерфейсі користувача або взаємодії з іншими процесами та системами. Вони також можуть з'явитися внаслідок того, що наявні процеси або системи не можуть адаптуватися до змін в експлуатаційних умовах постачальника обслуговування. Ретельний аналіз цих чинників на етапах планування, проектування та впровадження може часто виявити потенційні небезпечні фактори до того, як система буде введена в експлуатацію.

Розуміння системи та її експлуатаційних умов також необхідне для досягнення високих показників ефективності забезпечення безпеки польотів. Небезпечні фактори можуть бути виявлені протягом періоду експлуатації, завдяки звітам співробітників або розслідуванням інцидентів. Аналіз небезпечних факторів має проводитися з урахуванням стану системи. Це необхідно для того, щоб уникнути приписування пригод "людському фактору", у той час як дефекти системи можуть бути не взяті до уваги, залишаючись прихованими і слугуючи причиною майбутніх і потенційно більш серйозних пригод.

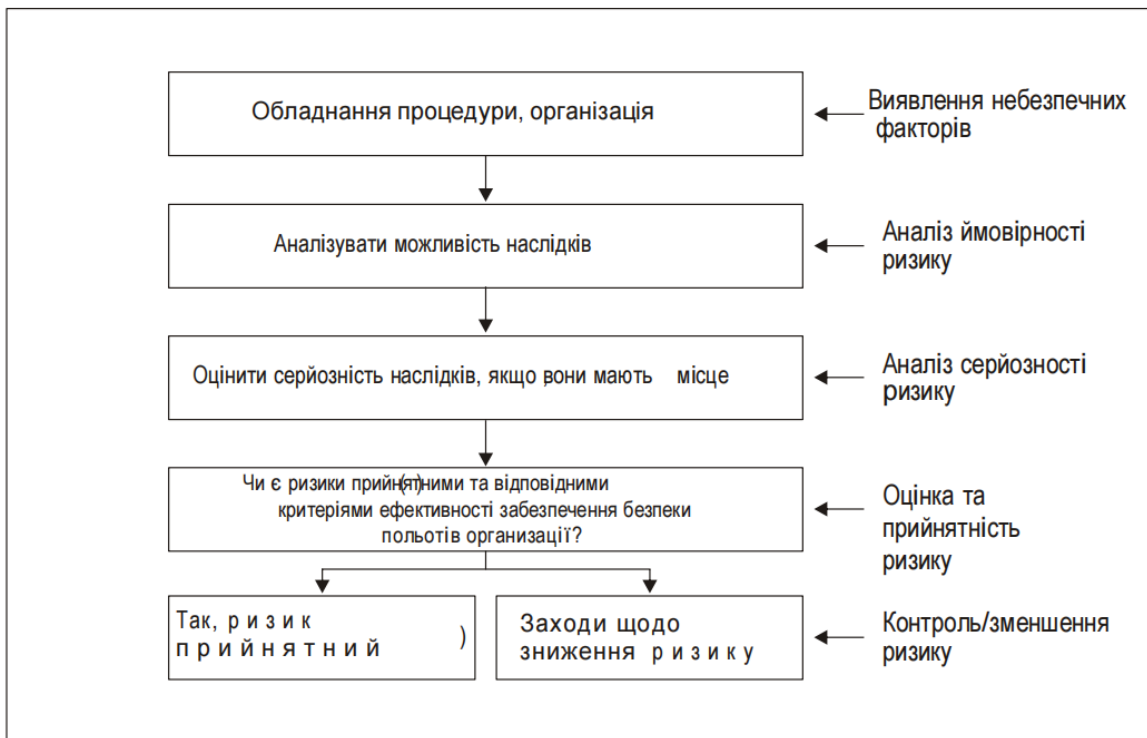


Рис. 3.1. Структура процесу управління факторами ризику

На рис. 3.2 подано повну схему процесу управління факторами ризику для безпеки польотів. Процес починається з виявлення небезпечних факторів та їхніх можливих наслідків. Потім фактори ризику оцінюються щодо ймовірності та ступеня серйозності, щоб визначити рівень фактора ризику (індекс фактора ризику для безпеки польотів). Якщо оцінені фактори ризику визнаються допустимими, робляться належні дії та експлуатаційна діяльність триває. Процес виявлення небезпечних факторів, оцінки факторів ризику та їх зменшення документується, санкціонується як належний і становить частину інформації про систему управління безпекою польотів.

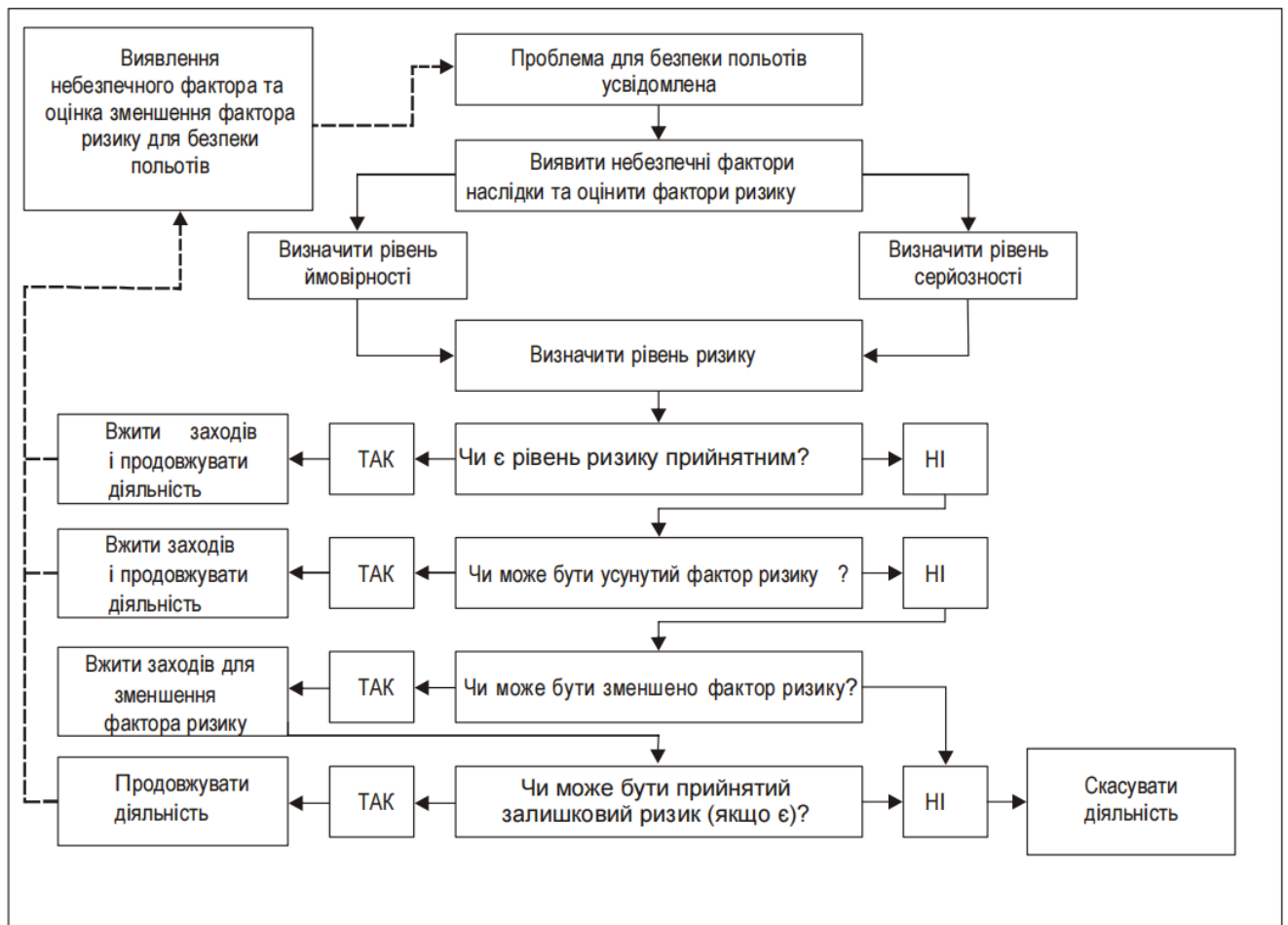


Рис. 3.2. Алгоритм управління факторами ризику при забезпеченні безпеки польотів

Якщо фактори ризику для безпеки польотів оцінюються як неприпустимі, то виникають такі питання:

а) Чи можуть бути усунені небезпечні фактори і відповідний(і) фактор(и) ризику?

Якщо відповідь позитивна, вживаються і документально оформляються відповідні заходи.

Якщо відповідь негативна, то виникає наступне запитання:

б) Чи можуть бути зменшені фактори ризику для безпеки польотів?

Якщо відповідь негативна, то здійснення відповідних заходів скасовується.

Якщо відповідь позитивна, вживаються відповідні дії щодо зменшення ризику і виникає наступне запитання:



с) Чи існує залишковий фактор ризику для безпеки польотів?

Якщо відповідь позитивна, то необхідно оцінити залишкові фактори ризику, щоб визначити ступінь їхньої допустимості та можливість їхнього усунення або зменшення, щоб забезпечити прийнятний рівень безпеки польотів.

Оцінка факторів ризику для безпеки польотів передбачає аналіз виявлених небезпечних факторів і включає два компоненти:

- а) оцінка ступеня серйозності наслідків для безпеки польотів;
- б) оцінка ймовірності того, що небезпека буде реалізована.

Інструктивний матеріал про проведення аналізу інформації про безпеку польотів у великих і складних за структурою організаціях наведено в розділі 2. Після оцінки факторів ризику, постачальник обслуговування приймає рішення, чи є необхідність вживати заходів щодо зменшення факторів ризику. Процес ухвалення рішення включає використання інструменту для визначення категорії ризику, який може мати вигляд оціночної матриці. Зразок матриці для оцінки факторів ризику (індексу) показано на рис. 3.3.

Імовірність фактора ризику	Серйозність фактора ризику				
	Катастрофічний А	Небезпечний В	Серйозний С	Невеликий D	Незначний Е
Частий 5	<b>5A</b>	<b>5B</b>	<b>5C</b>	<b>5D</b>	<b>5E</b>
Епізодичний 4	<b>4A</b>	<b>4B</b>	<b>4C</b>	<b>4D</b>	<b>4E</b>
Віддалений 3	<b>3A</b>	<b>3B</b>	<b>3C</b>	<b>3D</b>	<b>3E</b>
Мало-ймовірний 2	<b>2A</b>	<b>2B</b>	<b>2C</b>	<b>2D</b>	<b>2E</b>
Абсолютно неймовірний 1	<b>1A</b>	<b>1B</b>	<b>1C</b>	<b>1D</b>	<b>1E</b>

Рис. 3.3. Матриця оцінки факторів ризику (індекси)

Існує три загальних стратегії для зменшення факторів ризику для безпеки польотів:

а) **Уникнення ризику.** Експлуатаційна діяльність припиняється або тому, що відповідний фактор ризику для безпеки польотів є неприпустимим, або фактор ризику перевищує вигоди від продовження цієї діяльності.

б) **Зменшення ризику.** Певна схильність до ризику для безпеки польотів може допускатися, хоча при цьому ступінь серйозності або вірогідність факторів ризику повинні бути зменшені, можливо, завдяки заходам, що зменшують їхні наслідки.

в) **Локалізація наслідків ризику.** Вживаються заходи для того, щоб локалізувати можливі наслідки впливу небезпечного фактора або встановити багатошаровий захист від цих наслідків.

Стратегія зменшення чинників ризику може включати один із вищевказаних методів або поєднання декількох методів. Необхідно розглянути весь діапазон можливих заходів, щоб знайти оптимальне рішення. Необхідно також оцінити ефективність кожної альтернативної стратегії до прийняття рішення. Кожен передбачуваний варіант зменшення ризику слід проаналізувати з урахуванням таких аспектів, як:

а) **Ефективність.** Якою мірою альтернативні варіанти знижують або усувають фактори ризику для безпеки польотів? Ефективність може визначатися з урахуванням заходів захисту в галузі техніки, підготовки персоналу та регламентації діяльності, які можуть знизити або усунути фактор ризику для безпеки польотів.

б) **Витрати/вигоди.** Наскільки передбачувані вигоди від заходів зі зменшення факторів ризику перевершують витрати на них?

в) **Практичність.** Наскільки цей захід є здійсненим і доцільним з погляду наявної техніки, фінансових та адміністративних можливостей, нормативно-правових положень, політичної волі тощо?

г) **Прийнятність.** Наскільки альтернативний варіант узгоджується з уподобаннями зацікавлених сторін?

д) **Дотримуваність.** Якою мірою може бути забезпечений контроль за дотриманням нових правил, нормативних положень і експлуатаційних процедур?

е) **Довговічність.** Наскільки виявиться довгостроковим і ефективним вплив заходів зі зменшення ризиків?

г) **Залишкові фактори ризику для безпеки польотів.** Яким буде рівень фактора ризику для безпеки польотів, який залишиться після реалізації початкових заходів зі зменшення ризику і який може потребувати додаткових заходів контролю?

h) **Непередбачені наслідки.** Поява нових небезпечних чинників і відповідних чинників ризику для безпеки польотів у зв'язку з реалізацією альтернативного варіанта зменшення чинників ризику.

Варіанти матриці припустимості факторів ризику для безпеки польотів наведені на рис. 2.4 та 3.5 [48].

Після затвердження та реалізації заходів щодо зменшення факторів ризику, ця стратегія має бути інкорпорована як зворотний зв'язок у процес забезпечення безпеки польотів постачальника обслуговування. Це необхідно для забезпечення цілісності, дієвості та ефективності захисних заходів у нових експлуатаційних умовах.

Кожна дія щодо зменшення факторів ризику має постійно документуватися. Це досягається шляхом використання різних додатків: від базових електронних або звичайних таблиць до адаптованих комерційних комп'ютерних програм зі зменшення факторів ризику. Оформлені документи про зменшення факторів ризику мають затверджувати на належному управлінському рівні.

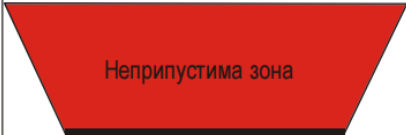


Зони прийнятності	Індекс оцінки ризику	Пропоновані критерії
 <p>Неприпустима зона</p>	<p><b>5A, 5B, 5C, 4A, 4B, 3A</b></p>	<p>Неприйнятний при існуючих обставинах</p>
 <p>Припустима зона</p>	<p><b>5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C</b></p>	<p>Прийнятний на підставі заходів зі зменшення ризику Може знадобитися рішення керівництва</p>
 <p>Припустима зона</p>	<p><b>3E, 2D, 2E, 1A, 1B, 1C, 1D, 1E</b></p>	<p>Прийнятний</p>

Рис. 3.4. Матриця припустимості факторів ризику

Діапазон індексу ризиків	Опис	Рекомендовані заходи
<b>5A, 5B, 5C, 4A, 4B, 3A</b>	Високий ступінь ризику	За необхідності негайно припинити або скоротити польоти. Реалізувати заходи щодо зниження пріоритетних ризиків, що забезпечують додаткові або посилені заходи контролю за зниженням індексу ризиків до помірного або низького рівня
<b>5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C, 1A</b>	Помірний ступінь ризику	Розробити графік проведення оцінок безпеки з метою зниження індексу ризиків до, з а можливості, низького рівня
<b>3E, 2D, 2E, 1B, 1C, 1D, 1E</b>	Низький ступінь ризику	Нинішній стан прийнятний. Жодних додаткових заходів щодо зниження факторів ризику не потрібно

Рис. 3.5. Варіант матриці припустимості факторів ризику для безпеки польотів

### 3.3. Оцінка ризику за методологією European Risk Classification Scheme (ERCS)

Традиційні методології та способи класифікації авіаційних подій та інцидентів не завжди забезпечують точну оцінку ризиків цих подій. У Регламенті (ЄС) № 376/2014 від 03 квітня 2014 р. Європейського Парламенту та Ради (далі – Регламент) визначено вимоги до класифікації ризику подій з безпеки польотів на державному рівні. Всі події, зазначені в звіті, були оцінені за методологією ERCS [49].

ERCS розроблено для підтримки уповноважених органів з питань цивільної авіації у проведенні оцінки ризиків щодо безпеки польотів, головною метою якої є гармонізований підхід з ідентифікації та класифікації ризику кожної події з безпеки польотів, дана методологія застосовується тільки для подій, які мали місце (визначення операційних ризиків).

Методологія ERCS являє собою засоби для проведення аналізу та оцінювання події з безпеки польотів для визначення на скільки результат даної події був близьким до можливого переростання в авіаційну подію. ERCS також визначає бар'єри, які завадили або не запобігли переростанню події у авіаційну подію.

Оцінка рівня ризику (ERCS score) складається із двох складових: значення рядка, що включає буквенне позначення, та числове значення стовбця. Такий принцип маркування є характерним для кожного елементу матриці ERCS та передбачає встановлення оцінки рівня ризику. Кожен елемент матриці ERCS також передбачає еквівалентне числове значення (Numerical equivalent score), яке насправді є лише числом призначеним для визначення Вірогідності (Probability) передбачуваного ризику та не пов'язаний з математичними розрахунками такої ймовірності.

Загальна оцінка рівня ризику події з безпеки польотів за шкалою матриці ERCS, представлений на рис. 3.6, формується за рахунок об'єднання значення серйозності (оцінка рядка матриці) та значення ймовірності (оцінка стовбця матриці).

Отримати оцінку ступеня серйозності (ERCS Severity score) можна шляхом поєднання Ключової сфери ризику (Key risk area) з категорією Ймовірних смертельних випадків (Potential loss of life), а оцінка ймовірності можливого наслідку події, як визначено першим кроком – оцінка серйозності (severity), шляхом застосування бар'єрної моделі, яка описує авіаційну систему в цілому.

Підрахунок балів повинен здійснюватися з використанням усієї доступної інформації про подію, наданої Доповідачем або звітуючою організацією до уповноваженого органу з питань цивільної авіації. Це передбачає необхідність постійного покращення обсягу та якості інформації про події необхідної для оцінки рівня ризику (risk score).

СЕРЬОЗНІСТЬ		КЛАСИФІКАЦІЯ (Оцінка рівня ризику за ERCS)									
Можливий наслідок події	Оцінка	Оціування оцінки ризику									
Екстремально катастрофічна АП з потенціалом до значної кількості жертв (100+)	X	X9	X8	X7	X6	X5	X4	X3	X2	X1	X0
Значна АП, з можливістю жертв та травм (20-100)	S	S9	S8	S7	S6	S5	S4	S3	S2	S1	S0
Велика АП з обмеженою кількістю жертв (2-19), доленосними* травмами або руйнуванням ПС	M	M9	M8	M7	M6	M5	M4	M3	M2	M1	M0
АП, що може спричинити поодинокі жертви, доленосні* травми або значне пошкодження ПС	I	I9	I8	I7	I6	I5	I4	I3	I2	I1	I0
АП, що може спричинити незначні та серйозні травми (не доленосні*) або незначні пошкодження ПС	E	E9	E8	E7	E6	E5	E4	E3	E2	E1	E0
Ймовірність АП відсутня	A	Не має впливу на безпеку польотів									
Відповідна оцінка бар'єрів		9	8	7	6	5	4	3	2	1	0
Сума показників ваги бар'єрів		17-18	15-16	13-14	11-12	9-10	7-8	5-6	3-4	1-2	0
ВІРОГІДНІСТЬ МОЖЛИВОГО НАСЛІДКУ ПОДІЇ											

Рис. 3.6. Загальна оцінка рівня ризику події з безпеки польотів за шкалою матриці ERCS [49]

### 3. 4. Рекомендації, що пов'язані з ризиками та загрозами безпеці цивільної авіації України, які спричинені збройною агресією Російської Федерації

У зв'язку з надзвичайно високим ризиком, який становить для безпеки цивільної авіації повномасштабна збройна агресія Російської Федерації проти України, 24 лютого 2022 року, починаючи з 2:45 за київським часом, було вжито термінових заходів щодо закриття повітряного простору України для цивільних користувачів повітряного простору. Того ж дня в Україні було оголошено воєнний стан, і надання послуг повітряного руху цивільним користувачам повітряного простору України було призупинено.

25 лютого 2022 року Рада ІКАО обговорила ситуацію, що складається в Україні, на другому засіданні своєї 225-ї сесії. Представник України також взяв участь у засіданні Ради, виходячи із зацікавленості держави в ситуації, що склалася. Рада розглянула цю тему на основі усної доповіді, представлені Президентом Ради,

а також презентації Генерального секретаря ІКАО, в якій представники отримали оновлену інформацію про експлуатаційні умови для авіації.

Рада засудила порушення територіальної цілісності та суверенітету держави - члена Організації Об'єднаних Націй, зокрема її повітряного простору, як несумісне з принципами Статуту Організації Об'єднаних Націй і статтею 1 Конвенції про міжнародну цивільну авіацію.

Рада підкреслила першорядну важливість збереження безпеки польотів і безпеки міжнародної цивільної авіації та відповідних зобов'язань держав-членів і в цьому контексті настійно закликала Російську Федерацію припинити свою незаконну діяльність, забезпечити безпеку польотів і безпеку цивільної авіації у всіх порушених районах і дотримуватися своїх зобов'язань за Чиказькою конвенцією, а також іншими відповідними міжнародними договорами в галузі цивільної авіації, а також закликав усі сторони прагнути до врегулювання кризи за допомогою мирного діалогу і дипломатичних каналів.

Рада також із глибоким сумом нагадала про людські страждання, які були заподіяні в результаті збиття рейсу МН17 на сході України 17 липня 2014 року, і підкреслив, що подібна трагедія ніколи не повинна повторитися. У тому ж контексті Рада знову підтвердила свою підтримку ініціативи Канади "Безпечніше небо", що стосується вдосконалення міжнародних зусиль із забезпечення безпеки цивільних польотів над зонами конфліктів або поблизу них.

Щодо оцінка ризиків і загроз авіаційній безпеці цивільної авіації та безпеки польотів цивільних повітряних суден під час виконання польотів над зонами збройних конфліктів або поблизу них і в контексті оголошеного в країні воєнного положення рекомендовано таке.

1 Під час планування та виконання польотів над зонами збройних конфліктів або поблизу них, а також у разі воєнного стану експлуатант повітряного судна повинен враховувати інформацію про обмеження або закриття повітряного простору органами управління повітряним рухом і причини таких обмежень та/або заборон.

2 Під час виконання польотів над зонами збройних конфліктів або поблизу них, а також у разі також у разі воєнного стану експлуатант повітряного судна

повинен оцінювати ризики і загрози щодо як навмисних (запланованих) нападів, так і ненавмисних дій проти цивільних повітряних суден.

3. У зв'язку з тим, що ЄВРОКОНТРОЛЬ розпочав реалізацію своєї нової Стратегії цивільно-військового співробітництва, в якій чітко виражена підтримка агентством цивільно-військового співробітництва в той час, коли воно стало особливо важливим і актуальним у зв'язку з неспровокованим військовим вторгненням Росії в Україну.

4. У світлі ініціатив ІКАО і з метою забезпечення авіаційної безпеки та безпеки польотів цивільних повітряних суден над зонами збройних конфліктів або поблизу них, а також у контексті воєнного стану, оголошеного в АТС, пропонується розглянути можливі заходи сприяння під егідою ІКАО, спрямовані на відновлення повномасштабного функціонування цивільної авіаційної галузі в умовах відбиття збройної агресії, розпочатої Російською Федерацією проти України.

5. Беручи до уваги досвід України в оцінці ризиків і загроз безпеці цивільної авіації та безпеки польотів цивільних повітряних суден, Раді ІКАО також необхідно розробити загальний підхід та ефективні механізми для оцінки ризиків і загроз безпеці цивільної авіації та безпеки польотів цивільних повітряних суден над або поблизу збройних зон конфліктів і в контексті воєнного стану, оголошеного в Україні.

6. Україна має закликати держави - члени ІКАО та авіаційну галузь підтримати ініціативи форуму "Безпечніше небо" та взяти в них участь, щоб об'єднати національних, міжнародних і галузевих експертів для обміну передовим досвідом і знаннями в галузі управління ризиками під час польотів цивільної авіації над зонами збройних конфліктів або поблизу них.

### **Висновки до розділу**

1. Запропоновані рекомендації щодо удосконалення методичної бази оцінювання загроз та ризиків в авіапідприємствах України. Визначено, що доцільно удосконалити існуючий методичний апарат у напрямках розроблення та впровадження відповідних превентивних заходів авіаційної безпеки для зниження



ризиків незаконного втручання до прийнятної рівня; координації та співпраці органів державної влади щодо оцінки рівня ризиків та загроз відповідно до визначених критеріїв, а також розробки стандартизованої методики оцінки ризиків і загроз.

2. Розроблено методичні рекомендації щодо управління факторами ризику для безпеки польотів, у яких визначено заходи оцінювання ризику. Зазначено, що виявлення чинників небезпеки є першим кроком в офіційному процесі збору, обліку, використання і генерування зворотної інформації про чинники небезпеки і чинники ризику у виробничій діяльності, а також те, що джерела виявлення чинників небезпеки повинні включати три методи: реагуючий, проактивний і прогностичний.

3. Наведено рекомендації щодо оцінки ризику за методологією European Risk Classification Scheme (ERCS). Констатовано, що моніторинг і вимірювання показників ефективності забезпечення безпеки польотів є щонайпершою задачею забезпечення безпеки польотів. Це є процесом, за допомогою якого ефективність забезпечення безпеки польотів організації перевіряється в порівнянні з положеннями політики і затвердженими цілями в області безпеки польотів. Моніторингом і вимірюванням результатів діяльності рекомендовано займатися експлуатаційному персоналу організації.

4. Розроблено рекомендації, що пов'язані з ризиками та загрозами безпеці цивільної авіації України, які спричинені збройною агресією Російської Федерації, в яких пропонується таке:

у разі воєнного стану експлуатант повітряного судна повинен враховувати інформацію про обмеження або закриття повітряного простору органами управління повітряним рухом і причини таких обмежень та заборон;

під час виконання польотів над зонами збройних конфліктів або поблизу них, а також у разі воєнного стану експлуатант повітряного судна повинен оцінювати ризики і загрози щодо як навмисних (запланованих) нападів, так і ненавмисних дій проти цивільних повітряних суден;

зазначено, що відповідно до нової Стратегії цивільно-військового співробітництва воно набуло особливої важливості і актуальності у зв'язку з неспровокованим військовим вторгненням Росії в Україну;

пропонується розглянути можливі заходи сприяння під егідою ІКАО, спрямовані на відновлення повномасштабного функціонування цивільної авіаційної галузі в умовах відбиття збройної агресії, розпочатої Російською Федерацією проти України.

розробити загальний підхід та ефективні механізми для оцінки ризиків і загроз безпеки цивільної авіації та безпеки польотів цивільних повітряних суден над або поблизу збройних зон конфліктів і в контексті воєнного стану, оголошеного в Україні.

підтримати ініціативи форуму "Безпечніше небо" та взяти в них участь, щоб об'єднати національних, міжнародних і галузевих експертів для обміну передовим досвідом і знаннями в галузі управління ризиками під час польотів цивільної авіації над зонами збройних конфліктів або поблизу них.

### **ЗАГАЛЬНІ ВИСНОВКИ**

6. Визначено, що у контексті воєнного стану, оголошеного в Україні, найбільш важливим фактором вважається пряма загроза галузі цивільної авіації. Імовірність загрози, що виникає внаслідок наміру та можливості нападу на цивільне повітряне судно над зоною конфлікту або поблизу неї, є ключовим фактором оцінки ризику та попередньою умовою для визначення заходів з пом'якшення наслідків, які необхідно застосувати.

7. Сучасні негативні явища найгостріше позначають проблему браку нових способів управління процесами забезпечення безпеки польотів, визначення загроз та відповідних джерел небезпеки авіаперевезень, а відтак продовжуватимуть ставати все більш актуальними.

8. Аналіз понятійно-категорійного апарату надав змогу уточнити поняття безпека на транспорті як таке, що стосується не тільки безпеки перевезень, але й безпеки всіх технологічних процесів транспортних галузей, в тому числі й економічної, та інформаційної безпеки.

9. За результатами аналізу методів оцінювання загроз та ризиків визначено, що моделювати й класифікувати джерела загроз, самі загрози та їх прояви, а також розробляти ефективні заходи протидії доцільно на основі аналізу взаємодії логічного ланцюжка: Джерело загрози → Загроза → Уразливість → Реалізація загрози (атака) → Наслідки (збиток) → Заходи протидії та представлена .

10. Аналіз узагальненої моделі забезпечення безпеки надає змогу сформулювати такі вимоги до методичного апарату ідентифікації загроз та оцінки ризиків, які містять:

оперативність оцінювання загроз та ризиків;

всебічне і повне урахування дії всіх складових загроз на рівень авіаційної безпеки;

простота, доступність і наочність отриманих розрахункових даних;

можливість прогнозування ситуації, що склалася на майбутній перебіг подій і на ймовірність виникнення аварійних та катастрофічних ситуацій;

гнучкість у використанні і можливість оперативно вводити і оцінювати нові різномірні дані, що стосуються складових авіаційної безпеки.

11. Внаслідок проведеного концептуального аналізу поняття комплексної безпеки встановлено, що діяльність із забезпечення безпеки виникає в ході вирішення протиріччя між небезпекою й потребою управляти безпекою: передбачати, запобігати, локалізувати й усувати збиток від впливу небезпеки

12. Специфічними особливостями завдання створення систем забезпечення безпеки є:

неповнота й невизначеність вихідної інформації про склад і характер загроз;

багатокритеріальність завдання, що пов'язано з необхідністю урахування великої кількості часткових показників;

наявність як кількісних, так і якісних показників, які необхідно враховувати при вирішенні завдань розробки та впровадження систем забезпечення безпеки;

неможливість застосування класичних методів оптимізації.

13. Визначено, що математична модель оцінки рівня комплексної безпеки системи може бути представлена у вигляді кортежу, який включає в себе

орієнтований граф, накладену на цей граф систему переваг одних факторів іншим і набір якісних оцінок рівнів кожного фактора в ієрархії.

14. Розроблено методику знаходження пріоритетів окремих показників, що визначають рівень небезпеки (загрози) та дають змогу:

отримувати кількісні значення пріоритетів окремих показників, що визначають рівень небезпеки (загрози) авіаційної діяльності;

отримувати оціночні значення тенденції зростання (спадання) окремих показників для певного проміжку часу.

15. Розроблено методику та алгоритм оцінки загроз та ризиків АТС, які дають змогу визначати заходи протидії інформаційним загрозам на підставі результатів аналізу можливих і виявлення актуальних загроз, оцінювання можливих ризиків, що виникають внаслідок реалізації певної загрози, можливих негативних наслідків загроз, ідентифікації можливих джерел загроз, факторів, що сприяють їх прояву (уразливостей).

16. Запропоновані рекомендації щодо удосконалення методичної бази оцінювання загроз та ризиків в авіапідприємствах України. Визначено, що доцільно удосконалити існуючий методичний апарат у напрямках розроблення та впровадження відповідних превентивних заходів авіаційної безпеки для зниження ризику незаконного втручання до прийнятного рівня; координації та співпраці органів державної влади щодо оцінки рівня ризиків та загроз відповідно до визначених критеріїв, а також розробки стандартизованої методики оцінки ризиків і загроз.

12. Розроблено методичні рекомендації щодо управління факторами ризику для безпеки польотів, у яких визначено заходи оцінювання ризику. Зазначено, що виявлення чинників небезпеки є першим кроком в офіційному процесі збору, обліку, використання і генерування зворотної інформації про чинники небезпеки і чинники ризику у виробничій діяльності, а також те, що джерела виявлення чинників небезпеки повинні включати три методи: реагуючий, проактивний і прогностичний.

13. Наведено рекомендації щодо оцінки ризику за методологією European Risk Classification Scheme (ERCS). Констатовано, що моніторинг і вимірювання

показників ефективності забезпечення безпеки польотів є щонайпершою задачею забезпечення безпеки польотів. Це є процесом, за допомогою якого ефективність забезпечення безпеки польотів організації перевіряється в порівнянні з положеннями політики і затвердженими цілями в області безпеки польотів. Моніторингом і вимірюванням результатів діяльності рекомендовано займатися експлуатаційному персоналу організації.

14. Розроблено рекомендації, що пов'язані з ризиками та загрозами безпеці цивільної авіації України, які спричинені збройною агресією Російської Федерації, в яких пропонується таке:

у разі воєнного стану експлуатант повітряного судна повинен враховувати інформацію про обмеження або закриття повітряного простору органами управління повітряним рухом і причини таких обмежень та заборон;

під час виконання польотів над зонами збройних конфліктів або поблизу них, а також у разі також у разі воєнного стану експлуатант повітряного судна повинен оцінювати ризики і загрози щодо як навмисних (запланованих) нападів, так і ненавмисних дій проти цивільних повітряних суден;

зазначено, що відповідно до нової Стратегії цивільно-військового співробітництва воно набуло особливої важливості і актуальності у зв'язку з неспровокованим військовим вторгненням Росії в Україну;

пропонується розглянути можливі заходи сприяння під егідою ІКАО, спрямовані на відновлення повномасштабного функціонування цивільної авіаційної галузі в умовах відбиття збройної агресії, розпочатої Російською Федерацією проти України.

розробити загальний підхід та ефективні механізми для оцінки ризиків і загроз безпеки цивільної авіації та безпеки польотів цивільних повітряних суден над або поблизу збройних зон конфліктів і в контексті воєнного стану, оголошеного в Україні.

підтримати ініціативи форуму "Безпечніше небо" та взяти в них участь, щоб об'єднати національних, міжнародних і галузевих експертів для обміну передовим

досвідом і знаннями в галузі управління ризиками під час польотів цивільної авіації над зонами збройних конфліктів або поблизу них.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. International Civil Aviation Organization. Annexes 1 to 18. ICAO. URL: [https://www.icao.int/documents/annexes\\_booklet.pdf](https://www.icao.int/documents/annexes_booklet.pdf).
2. Європейська конференція цивільної авіації (ЄКЦА) - Міністерство інфраструктури України. Міністерство інфраструктури України. URL: <https://mtu.gov.ua/content/evropeyska-konferenciya-civilnoi-aviaciiaksa.html?PrintVersion>.
3. Закон України "Про Державну програму авіаційної безпеки цивільної авіації" 21 березня 2017 року № 1965-VIII. Режим доступу: URL: <https://avia.gov.ua/> (дата звернення: 11.11.2023)
4. Про затвердження Інструкції з оцінки рівня загрози безпеці цивільної авіації України. Офіційний вебпортал парламенту України. URL: <https://zakon.rada.gov.ua/laws/show/z0316-19#Text>.
5. Коршук С. Звіт щодо виконання функцій нагляду за безпекою польотів у системі організації повітряного руху в Україні за 2021 рік. Київ : Державіаслужба. 23 с.
6. Кирилюк Н. Адміністративно-правове регулювання цивільної авіації України. Наукові Записки. Серія: Право. 2019. Т. 2, № 6. С. 55–60. URL: [https://www.cuspu.edu.ua/images/nauk\\_zapiski/pravo/6\\_spec\\_II\\_2019/55-60.pdf](https://www.cuspu.edu.ua/images/nauk_zapiski/pravo/6_spec_II_2019/55-60.pdf).
7. Міжнародна організація цивільної авіації. Міністерство інфраструктури України. URL: <https://mtu.gov.ua/content/mizhnarodna-organizaciya-civilnoiaviacii.html>.
8. ECAC activities. European civil aviation conference. URL: <https://www.ecacceac.org/>.
9. Home. EUROCONTROL | Supporting European Aviation | EUROCONTROL. URL: <https://www.eurocontrol.int/>.
10. Линьков А. В. Программа по оценке рисков в отношении безопасности полетов / Линьков А. В., Кармызов М. В. // Научный вестник МГТУ ГА (серия: Эксплуатация воздушного транспорта и ремонт авиационной техники. Безопасность

полетов). – 2006. – № 108. – С. 85–90.

11. Новий тлумачний словник української мови. – Т. 3. – К. : Акапіт, 1999. – 380 с.

12. Даль В. Толковый словарь живого великорусского языка / Даль В. Т. 1–4. – М., 1994. – 740 с.

13. Ожегов С. И. Словарь русского языка / С. И. Ожегов ; под ред. чл.-кор. АН СССР Н. Ю. Шведовой. – 18-е изд., стереотип. – М. : Рус. яз., 1987. – 797 с.

14. Юридична енциклопедія. – К. : Українська енциклопедія імені М. П. Бажана, 1998. – Т. 1. – 800 с.

15. ДСТУ 2156-93. Безпечність промислових підприємств. Терміни та визначення основних понять. – К. : Держстандарт України, 1993. – 32 с.

16. Туманов Г. А. Общественная безопасность и ее обеспечение в экстремальных условиях / Туманов Г. А., Фризко В. И. // Советское государство и право. – 1989. – № 8. – С. 21–25.

17. Наказ Державної служби України з нагляду за забезпеченням безпеки авіації «Про затвердження Положення про систему управління безпекою польотів на авіаційному транспорті» : від 25.11.2005 р., № 895 [Електронний ресурс]. – Режим доступу: <http://search.ligazakon.ua/doc2.nsf/link1/RE11783.html>.

18. Власюк О.С. Можливості застосування аналітичного планування для обґрунтування та підготовки рішень на вищих рівнях управління. НІСД, вип. 47, серія наукові доповіді, 1996. (71с.)

19. Семенченко А.І. Методологія стратегічного планування у сфері державного управління забезпеченням національної безпеки України: монографія.- К.: Вид-во НАДУ, 2008. – 428 с.

20. Косошов О.М. Пріоритетні напрямки державної політики щодо забезпечення безпеки національного кіберпростору / О.М.Косошов // Збірник наукових праць Харківського університету Повітряних Сил. – Х.: Харківський університет Повітряних Сил імені Івана Кожедуба, 2014.–Вип. 3 (40). – С. 127–129

21. Асанович В. Я. Информационная безопасность: анализ и прогноз информационного воздействия / В. Я. Асанович, Г. Г. Маньшин // – Мн.: Амалфея, 2006. – 204 с.

22. Кормич Б. А. Інформаційна безпека: організаційно-правові основи / Б. А. Кормич // – К. : Кондор, 2003. — 384 с.

23. Косевцов В.О. До питання оцінювання ефективності функціонування системи забезпечення воєнної безпеки держави / В.О. Косевцов, В.М.Телелим, А.А.Лобанов // Наука і оборона. – 2010. - № 3. – С. 8-12.

24. Левченко О.В. Проблеми і шляхи формування системи інформаційної безпеки держави / О.В.Левченко // Збірник наукових праць Харківського університету Повітряних Сил. – Х.: Харківський університет Повітряних Сил імені Івана Кожедуба, 2014. – Вип. 2 (39). С. 166-168

25. Романченко, І. С. Використання таксономічних методів при проведенні досліджень у воєнній справі [Текст] / І. С. Романченко, О. М. Загорка // Зб. наук. пр. ЦНДІ ЗС України. – К., 2007. – № 3 (41). – С. 5–16.

26. Елементи дослідження складних систем військового призначення [Текст] / О. М. Загорка, С. П. Мосов, А. І. Сбитнев, П. І. Стужук. – К.: НАОУ, 2005. – 100 с.

27. Корнеенко, В. П. Методы оптимизации: ученик [Текст] / В. П. Корнеенко. – М.: Высш. шк., 2007. – 664 с.

28. Ahmadi, H. Ranking the micro level critical factors of electronic medical records adoption using TOPSIS method [Text] / H. Ahmadi, M. S. Rad, M. Nilashi, O. Ibrahim, A. Almaee // Health Informatics – An International Journal. – 2013. – Vol. 2. – № 4, November. – P. 19–32.

29. Saelee, S. Biomass type selection for boilers using TOPSIS multi-criteria model [Text] / S. Saelee, B. Paweewan, R. Tongpool, T. Witoon, J. Takada, K. Manusboonpurmpool // International Journal of Environmental Science and Development. – 2014, April. – Vol. 5. – № 2. – P. 181–186.

30. Baležentis, A. Multimoora-FG: a multi-objective decision making method for linguistic reasoning with an application to personnel selection [Text] / A. Baležentis, T. Baležentis, W. K. M. Brauers // Informatica. – 2012. – Vol. 23. – № 2. – P. 173–190.



31. Качинський А. Б. Безпека, загрози та ризик / А. Б. Качинський. – К. : ПНБ РНБО ; НА СБ України, 2004. – 472 с.
32. Ту Дж. Принципы распознавания образов / Дж. Ту, Р. Гонсалес. – М. : Мир, 1978. – 411 с.
33. Кофман А. Введение в теорию нечетких множеств / А. Кофман. – М. : Радио и связь, 1982. – 432 с.
34. Гиг Дж. Ван. Прикладная общая теория систем: в 2-х томах / Дж. Ван Гиг. – М. : Мир, 1981. – Т. 2. – 730 с.
35. Заде Л. А. Понятие лингвистической переменной и его применение к принятию приближенных решений / Л. А. Заде. – М. : Мир, 1976. – 165 с.
36. Паніотто В. І. Статистичний аналіз соціологічних даних / В. І. Паніотто, В. С. Максименко, Н. М. Харченко. – К. : Вид. дім “КМ Академія” 2004. – 269 с.
37. Косошов О. М. Модель динаміки зміни рівня інформаційної безпеки системи / О. М. Косошов // 36. наук. праць. – К. : – ЦВСД НУО імені Івана Черняхівського, 2015. – № 2 (54). – С. 76–79.
38. J. N. Moderson, and P. S. Nair, Fuzzy Graphs and Fuzzy Hypergraphs. Heidelberg, Germany: Physica-Verlag Heidelberg, 2000. doi: 10.1007/978-3-7908-1854-3.
39. A. Kaufmann, Introducing to the fuzzy sets theory. Moscow, Russia: Radio i svjaz, 1982.
40. Повітряний кодекс України України (Відомості Верховної Ради України (ВВР), 2011, № 48-49, ст.536) {Із змінами, внесеними згідно з Кодексом № 4651-VI від 13.04.2012, ВВР, 2013, № 9-10, № 11-12, № 13, ст.88}
41. Манойло А.В. Государственная информационная политика в условиях информационно-психологической войны / А.В. Манойло, Петренко А.И., Фролов Д.Б. – М.: Горячая линия – Телеком, 2003. - 541с.
42. Косошов О.М. Методика визначення пріоритетів показників, що характеризують рівень загроз інформаційній безпеці держави //Збірник наукових праць Харківського університету Повітряних Сил. – Х.: Харківський університет Повітряних Сил імені Івана Кожедуба, 2014.– Вип. 2 (39). С. 162–165
43. Т.Саати, К.Кернс Аналитическое планирование, М., Радио и связь, 1991.

44. Косошов О.М. Механізми раннього попередження та нейтралізації загроз національним інтересам України в інформаційній сфері: Магістерська робота: (8.150102 “Управління суспільним розвитком”)/ НАДУ при Президентові України. Кафедра національної безпеки; Наук. кер.: А.І.Семенченко, к.т.н.,с.н.с – К., 2009 – с.83.

45. Косошов О.М. Методика визначення заходів протидії інформаційним загрозам державі у воєнній сфері / О. М. Косошов// Системи обробки інформації : збірник наукових праць. – Х.: Харківський університет Повітряних Сил імені Івана Кожедуба, 2016. – Вип. 3 (140). –С. 25 – 29.

46. Авіаційні правила України “Інструкція з організації та здійснення контролю на безпеку в аеропортах України” затверджені наказом Державної авіаційної служби України від 15 березня 2019 року № 322, URL: <https://zakon.rada.gov.ua/laws/show/z0594-19#Text>

47. ISO 22000 Food safety management systems – Requirements for any organization in the food chain, 2017, April. – Vol. 5. – № 2. – P.– 87.

48. Руководство по СУБП. Дос 9859. Издание четверте. ICAO, Монреаль, 2019.

49. Aviation Benefits Report 2019, ICAO (Report based on material of ACI, CANSO, IATA, ICAO, ICCAIA, ATAG).

50. Косошов О. М., Власенко Г. М., Гладкий К. С. Багатокритеріальний алгоритм прийняття рішення в системі забезпечення інформаційної безпеки об'єктів цивільної авіації. // Innovations and prospects in modern science. Proceedings of the 12th International scientific and practical conference. SSPG Publish. Stockholm, Sweden. 2023. Pp. 250-257. URL: <https://sciconf.com.ua/xii-mizhnarodna-naukovo-praktichna-konferentsiya-innovations-andprospects-in-modern-science-20-22-11-2023-stokgolm-shvetsiya-arhiv/>