

ПОЛІТИКА ТА ЦІЛІ БЕЗПЕКИ

AMC1 ORA.GEN.200 (a) (2) та GM1 ORA.GEN.200 (a) (2).

Основною метою політики у сфері безпеки польотів є створення і впровадження в АТО «ХАК ТСОУ» Системи управління безпекою польотів та забезпечення постійного підвищення рівня безпеки польотів, запобігання помилок і необґрунтованих витрат фінансів і часу, забезпечення адміністрації достатніми аргументами для прийняття рішень, максимальне зниження ризиків, особливо на етапі прийняття рішень.

АТО «ХАК ТСОУ» є організацією, що володіє відповідною структурою, достатніми фінансовими і трудовими ресурсами, а також повноваженнями, необхідними для реалізації поставлених завдань.

Політика АТО«ХАК ТСОУ» у сфері безпеки польотів побудована на принципі - *краще забезпечити безпеку польотів, ніж усувати наслідки авіаційної події.*

ПРИНЦИПИ РЕАЛІЗАЦІЇ ПОЛІТИКИ

Принципи реалізації політики в галузі безпеки польотів це найбільш загальні, основні правила та рекомендації, якими повинні керуватися суб'єкти авіаційної діяльності для практичної організації СУБП.

Головними принципами реалізації політики з БП є:

- між безпекою польотів і комерційним успіхом АТО «ХАК ТСОУ» існує прямий зв'язок:
- реалізація політики в галузі БП будується на єдності стратегічного, тактичного та оперативного рівнів управління БП;
- авіаційним подіям можна запобігти, імовірність настання авіаційної події керована і залежить від якості роботи персоналу;
- персонал (людина) є ключовим елементом у системі забезпечення безпеки польотів;
- здоров'ю персоналу приділяється належна увага, ця складова забезпечення безпеки польотів та запобігання авіаційних подій контролюється і забезпечується;
- управлінський персонал має відповідати за стан і забезпечення безпеки польотів, а також брати участь і нести конкретну відповідальність за якість управління ризиками;
- виконання персоналом вимог і правил забезпечення безпеки польотів є необхідною умовою збереження за ним робочого місця;
- вітається і заохочується ініціатива персоналу в питаннях програми управління ризиками відносно безпеки польотів ;
- організації безперервного обміну інформацією між взаємодіючими підприємствами;
- встановлення багаторівневого контролю за діяльністю підрозділів на аеродромі;
- врахування наслідків прийнятих рішень, а також відхилень та ризиків;

- для підвищення ефективності процесу виявлення небезпечних факторів керівництво АТО гарантує проведення некаральної культури безпеки;

- відносно всіх подій, які пов'язані з безпекою польотів, повинне проводитися розслідування (метою розслідування завжди є пошук і усунення причин);

- жодна посадова особа не має права скасувати рішення командира ПС прийняте ним в інтересах безпеки польотів;

- здійснення незалежного нагляду за станом і забезпеченням безпеки польотів є обов'язковим елементом Системи управління безпекою польотів;

- всі фахівці, безпосередньо пов'язані із забезпеченням безпеки польотів повинні бути навчені за відповідними програмами і пройти процес перевірки знань.

- процес підтримки адекватної кваліфікації є безперервним.

- витрати АТО, пов'язані з відновленням його ресурсів, завжди повинні

супроводжуватися ефективною політикою управління ризиками;

- управління ризиками відносно безпеки польотів містить в собі процес ідентифікації небезпеки, визначення існуючих ризиків, пошук стримуючих факторів, оцінку ефективності способів захисту від ризику та зменшення імовірності виникнення ризику.

Головними цілями безпеки є:

- 1) Ідентифікація та аналіз небезпек, класифікація і оцінка ризиків для забезпечення максимально можливого контролю над ними.

- 2) Зменшення ризиків небезпеки для ПС, курсантів, персоналу та майна настільки низько, наскільки це реально.

- 3) Проведення постійного навчання та підготовки у сфері забезпечення безпеки.

У відповідності до головних цілей, визначені наступні цілі діяльності:

- впровадження ефективної діяльності СУБП;

- проведення систематичних робіт по виявленню, оцінці, відстеженню, моніторингу загроз, пов'язаних з діяльністю організації;

- визначення кількості і мінімізація ризиків, спричинених небезпечними умовами і людським фактором під час експлуатації, обслуговування та підтримки діяльності «ХАК ТСОУ»;

- усунення, або зведення ризиків до допустимого рівня;

- ідентифікація та документування прийнятих заходів ;

- постійні навчання та підготовка персоналу у сфері безпеки польотів ;

- відстеження і вивчення досвіду з безпеки польотів .

ПОЛІТИКА БЕЗПЕКИ

Безпека - одна з наших основних функцій. Ми прагнемо розробляти, впроваджувати, підтримувати та постійно вдосконалювати стратегії та процеси, щоб гарантувати, що всі наші авіаційні заходи відбуваються під відповідним розподілом організаційних ресурсів, спрямованих на досягнення найвищого рівня продуктивності та відповідності нормативним вимогам, забезпечуючи при цьому наші послуги .

Всі рівні управління та всі працівники несуть відповідальність за досягнення цього найвищого рівня безпеки, починаючи з Відповідального керівника АТО «ХАК ТСОУ».

Ми прагнемо:

Підтримувати управління безпекою шляхом надання всіх відповідних ресурсів, які призведуть до організаційної культури, яка сприятиме безпечній практиці, заохочуватиме ефективну звітність і комунікацію з безпеки, а також активно керувати безпекою з однаковою увагою до результатів, звертаючи увагу на результати інших систем управління організацією;

Забезпечення управління безпекою є основною відповідальністю всіх керівників і працівників;

Чітко визначити для всіх працівників, керівників та співробітників, їх відповідальність та відповідальність за забезпечення безпеки діяльності організації та ефективність нашої системи управління безпекою;

Створити та використовувати процеси ідентифікації небезпек та управління ризиками, включаючи систему звітування про небезпеку, з метою усунення або пом'якшення ризиків для безпеки наслідків небезпек, що виникають внаслідок наших операцій або діяльності для досягнення постійного поліпшення показників безпеки;

Забезпечити, щоб не було вжито жодних заходів проти будь-якого працівника, який виявляє занепокоєння щодо безпеки через систему звітування про небезпеку, якщо таке розкриття не свідчить, без будь-яких розумних сумнівів, про грубу недбалість або навмисне або свідоме нехтування правилами або процедурами;

Дотримуватися та, по можливості, перевищувати законодавчі та нормативні вимоги та стандарти;

Забезпечити наявність достатніх кваліфікованих та навчених людських ресурсів для реалізації стратегій і процесів безпеки;

Забезпечити, щоб всі працівники отримували адекватну та відповідну інформацію та підготовку з питань безпеки польотів, компетентні у питаннях безпеки та розподіляли лише завдання, які відповідають їхнім навичкам;

Встановити та виміряти продуктивність нашої безпеки у порівнянні з реалістичними показниками безпеки ;

Постійно підвищувати продуктивність нашої безпеки шляхом постійного моніторингу та вимірювання, а також регулярного перегляду та коригування цілей і завдань з безпеки, а також їх старанного досягнення;

Забезпечити, щоб системи та послуги, що постачаються ззовні, забезпечували підтримку наших операцій відповідно до наших стандартів безпеки.

Політика безпеки свідчить, що метою звітності з безпеки та внутрішніх розслідувань є поліпшення безпеки, а не призначення винних на осіб.

ЗАХИСТ ДОПОВІДАЧІВ

АТО «ХАК ТСОУ» зобов'язується працювати відповідно до найвищих стандартів безпеки. Для досягнення поставленої мети необхідно безперешкодно надавати звітність про всі аварії, інциденти, події, небезпеки, ризики та іншу інформацію, яка може поставити під загрозу безпечне ведення наших операцій. З цією метою кожен співробітник заохочується до відповідальності за будь-яку інформацію пов'язану з безпекою.

Звітування не має мати будь-якої форми покарання. Основною метою звітності є контроль ризиків і запобігання аваріям і інцидентам, а не атрибуція вини. Ніякі дії не будуть вжиті проти будь-якого співробітника, який виявляє занепокоєння щодо безпеки через систему звітності, якщо таке розкриття не виявить, поза будь-якими сумнівами, незаконне діяння, грубу недбалість або навмисне або свідоме ігнорування правил або процедур. Наш метод збору, реєстрації та розповсюдження інформації про безпеку гарантує захист в тій мірі, в якій це дозволено законом, про особу, яка повідомляє інформацію про безпеку.

Я, Філатов Сергій Миколайович, повністю приймаю обов'язки і відповідальність відповідального керівника, як зазначено в ORA.GEN.210

20.02.2019 року / /:

Відповідальний керівник:



(Філатов С.М.)

Від імені та за дорученням АТО «Харківський аероклуб ім. В.С. Гризодубової ТСО України»

Відповідальність персоналу

ORO.GEN.210(c), (d) та (e)

Персонал особисто відповідає за свої дії в питаннях забезпечення безпеки польотів в межах посадових обов'язків.

(c) АТО «ХАК ТСОУ» повинна мати достатньо кваліфікованого персоналу для виконання запланованих завдань та заходів відповідно до вимог, що застосовуються, включаючи вимоги до SMS.

(d) АТО «ХАК ТСОУ» повинна мати відповідний досвід, кваліфікацію та навчальні записи, щоб показати відповідність вищезазначеним вимогам .

(є) АТО «ХАК ТСОУ» повинна забезпечити, щоб весь персонал, знав про правила та процедури, що стосуються виконання своїх обов'язків.

У контексті SMM персонал АТО «ХАК ТСОУ», відповідальний за виконання оперативних завдань, має такі обов'язки:

- виконувати усі вимоги правил безпеки в відповідності з посадовими інструкціями, технологіями та іншими документами;
- при виявленні порушень правил безпеки польотів, небезпечних відмов обладнання та інших небезпечних факторів, джерел небезпеки та потенційних ризиків негайно інформувати безпосереднє керівництво, Керівника з безпеки;
- доповідати безпосередньому керівнику у разі невпевненості в якісному виконанні доручених завдань через недостатній рівень знань, відсутність навиків, стану здоров'я, стану обладнання і спецтехніки або з інших причин для прийняття необхідних запобіжних заходів;
- у випадку виявлення невідповідності стану ПС, аеродромного покриття, спецтехніки, обладнання, які загрожують безпеці польотів, негайно доповідати Керівнику з безпеки;
- приймати участь в удосконаленні діючих нормативних документів, надавати пропозиції з їх удосконалення.

Кожен співробітник АТО «ХАК ТСОУ» відіграє певну роль у успішному впровадженні SMS. Це не тільки «завдання декількох», а й «справи фахівців», зокрема, відповідальність кожного в АТО полягає у виявленні та повідомленні про небезпеку. Усі члени персоналу повинні інформувати Керівника з безпеки та їх лінійного керівника про будь-яку ситуацію, що вважається небезпечною для безпеки польотів та для власної безпеки або безпеки інших як в межах, так і поза АТО.

Весь персонал повинен пройти навчання і знати їхні ролі та обов'язки.

Для того, щоб кожен співробітник розумів свої ролі та обов'язки в рамках SMM, АТО «ХАК ТСОУ» визначила ролі та обов'язки, які визначені в посадових інструкціях.

Елементи, що впливають на оцінку ризику безпеки

Комунікація та консультація

Хороша комунікація в АТО «ХАК ТСОУ» та, де це доречно, із зовнішніми сторонами (клієнтами, партнерами або підрядниками) повинна допомогти забезпечити доступ до всієї відповідної інформації та допомогти у забезпеченні участі всіх, хто може бути зачеплений оцінкою ризику висновки та рекомендації. Комунікація та консультації мають відбуватися на всіх відповідних етапах процесу.

Регуляторні вимоги - ризики, рекомендовані регулюванням

Правила, взагалі, розроблені для контролю за загальними ризиками для безпеки, які виникають внаслідок специфічних або загальних небезпек, за допомогою нормативних,

технічних стандартів у сфері технології, навчання або виконання завдань. Такі ризики, які регулюються нормативними актами, не потребують подальшого розгляду в оцінці ризику АТО «ХАК ТСОУ», якщо не існує доказів того, що нормативне положення є недостатнім. Якщо регулювання не є конкретним, має декілька варіантів або безпосередньо вимагає оцінки ризику, очевидно, що небезпеку слід оцінювати, а відповідне забезпечення впроваджувати.

Галузеві стандарти

АТО «ХАК ТСОУ» розробляє стандартні операційні процедури (СОП) на основі галузевих стандартів / найкращих практик, однак повинна виконувати власну оцінку ризиків для забезпечення відповідності та пристосування СОП до своєї діяльності.

Ресурси

Наявні ресурси мають відношення як до потенціалу, так і до компетенції:

- для процесу оцінки ризику ;
- для діяльності, що оцінюється, (ПС, обладнання, персонал, фінанси тощо).

Поточні ресурси АТО «ХАК ТСОУ» з точки зору обладнання та персоналу зазвичай розглядаються в оцінці ризику.

АТО «ХАК ТСОУ» володіє відповідним обладнанням та персоналом для діяльності.

Ідентифікація небезпеки

Класифікація небезпеки

Небезпека може надходити з різних джерел, включаючи:

- природні та екологічні: погода, землетрус, вітер і пісок, морська вода, скелі, обриви, крижані споруди, бурхливі води, лави вулканів і пили тощо.
- економічні: конкуренція, тиск виробництва, тиск витрат тощо
- небезпечні умови: використання неофіційних документів або документів, що не є актуальними, брак ресурсів.
- небезпечні дії: помилки, порушення, недбалість, саботаж, надмірні / неконтрольовані зміни продуктивності.
- фізіологічні: хвороби, гіпоксія, перцептивні ілюзії, стомлюваність, депривація сну, втома, ліки, алкоголь, інтоксикація, проблеми з травленням тощо
- технологічні: проектування або технічне обслуговування, небезпечні матеріали, забруднення, вибухи тощо.
- оперативні або специфічні для місії: перешкоди, кабелі, вимогливі місця посадки (рухомі платформи / поза аеродромні майданчики), погіршення зорових характеристик .

Джерела ідентифікації небезпек

Інформація про небезпечні фактори має надходити із різних джерел, включаючи офіційні перевірки, матеріалів розслідування, пов'язаних з безпекою польотів, постійного моніторингу у повсякденної діяльності підприємства та підприємств - суміжників пов'язаної з наданням послуг, а також, з повідомлень про небезпечні фактори, які надходять від персоналу.

Небезпечні фактори також можуть бути виявлені після того як сталася авіаційна подія, інцидент або під час використання проактивних і прогностичних методів, направлених на виявлення небезпечних факторів до того, як вони спричинять виникнення АП або інциденту.

Небезпеки можуть бути ідентифіковані з різних внутрішніх і зовнішніх джерел, задаючи наступне запитання: *Які елементи, окремо або в комбінації, могли сприяти інциденту чи аварії?*

До внутрішніх джерел інформації відносяться:

- система обов'язкових повідомлень;
- система добровільних повідомлень;
- обстеження стану безпеки польотів;
- перевірки (аудити) стану безпеки польотів;
- контроль діяльності в штатних умовах з боку керівного складу;
- інформація, яка отримується персоналом в ході підготовки до ОЗП/ВЛП;
- інформація, яка отримана в процесі розслідування інцидентів та інших видів подій.

До зовнішніх джерел інформації відносяться:

- інформація, отримана під час здійснення державного нагляду та контролю;
- звіти НРБЦА за результатами розслідування АП та інцидентів;
- державна система обов'язкових повідомлень;
- державна система добровільних сповіщень про події;
- загальна система обміну інформації з БП.

Під час організації процесу виявлення небезпечних факторів використовуються всі можливі внутрішні та зовнішні джерела інформації. Виявлення небезпечних факторів та повідомлення про них стосуються кожного працівника підприємства. Кожний працівник має вміти виявляти небезпечні фактори та повідомляти про них, використовуючи систему обов'язкових або добровільних (конфіденційних) повідомлень.

Відповідальність за виявлення небезпечних факторів покладена на Керівника з безпеки та Групу дій з безпеки польотів підприємства. Виявлення небезпечних факторів є постійним, безперервним процесом, який не призупиняється і не припиняється ніколи. Існують умови, за яких процесу виявлення небезпечних факторів необхідно приділяти особливу увагу, до них відносяться:

- випадки, коли відбувається незрозуміле збільшення кількості подій, які пов'язані з БП чи порушень нормативних вимог;
- випадки, коли плануються значні виробничі зміни у тому числі основного обладнання, спецтехніки. ключових співробітників і тощо;
- проведення значних організаційних змін (зростання чи скорочення виробництва, корпоративного злиття і тощо).

Джерела ідентифікації небезпечних наслідків

Небезпеки відрізняються від наслідків небезпеки. Наприклад, купчасто-дощовики становлять небезпеку для ПС, що літає в його околицях (менше 5NM). Наслідками цієї небезпеки можуть бути: *сильна турбулентність*, яка може викликати повну втрату ПС, *блискавки*, які можуть призвести до технічних пошкоджень і / або травм, *град*, який може пошкодити конструкцію і лопаті, *сильний дощ*, що може призвести до вибуху двигуна, *обмерзання*, що збільшує масу ПС, впливає на аеродинамічний профіль, змінює профіль лопатей гвинта, і т.д.

Наслідки можуть бути описані на основі інформації про небезпеку, в якій вказується місце, час, обсяг, характер і т.д. Ідентифікація небезпеки також забезпечує систематичний огляд всіх можливих наслідків.

Для кожної небезпеки слід задати наступне питання: *Які були або могли бути можливі наслідки небезпеки?*

Якщо інформація про наслідки небезпеки була ідентифікована для конкретного виду діяльності, вона повинна бути доступною безпосередньо з джерел даних (наприклад, від повідомлених аварій і подій або з результатів вже задокументованого аналізу).

Слід відзначити, що відсутність минулих випадків / аварій не означає відсутності ризику. Тому важливо визначити основні небезпеки та оцінити ризики. Одним з ефективних способів цього є групувати подібні заходи, щоб спробувати визначити основні небезпеки.

Джерела для визначення наслідків небезпеки:

- інші оцінки ризиків, звіти про події та аварії, звіти про аудит / невідповідність, внутрішні перевірки, результати моніторингу, включаючи інформацію моніторингу польотних даних; обмін ідеями, оцінки загроз;
- чек-листи (походження має бути ідентифіковано, якщо вони використовуються, а чек-листи оцінені та переглянуті відповідно до цілей).

Процес ідентифікації небезпек

Небезпеки визначаються шляхом застосування процесів ідентифікації небезпек.

Ідентифікація небезпеки є першим кроком в процесі управління факторами ризику. Вона ґрунтується на поєднанні реактивних, проактивних і інтелектуальних (прогностичних) методах збору даних про фактори небезпек.

Існує три методи виявлення факторів небезпеки; реактивний, проактивний та прогностичний.

Реактивний - оснований на аналізі результатів минулих інцидентів або подій, які пов'язані з безпекою польотів. Виявлені фактори небезпек у ході розслідування авіаційних подій, аварій, інцидентів є чіткими індикаторами недоліків систем і, отже, можуть бути використані для визначення небезпек, які були як внесок у події або приховані.

На підставі аналізу повідомлених аварій та інцидентів слід поставити наступні запитання:

- *Які аварії чи інциденти траплялися і чому?*
- *З яких причин вони відбуваються? З-за яких причинних факторів?*
- *Які бар'єри або контроль за ризиком не вдалі, а які бар'єри працювали?*

Проактивний - оснований на аналізі існуючих або реальних ситуаціях часу, включає в себе активний пошук небезпек і оцінки пов'язаних з ними ризиків в існуючих процесах. Такий підхід повинен викликати такі запитання:

- *Які аварії та інциденти можуть статися і чому?*
- *З яких причин вони можуть виникнути?*
- *Чи відчуваємо ми себе достатньо захищеними? Будь-які дії, які ми повинні зробити зараз, щоб запобігти цьому?*

Інтелектуальний (прогностичний) - ґрунтується на збиранні даних за 3-5 років з метою виявлення можливих негативних результатів або подій, а також, аналізі системних процесів для виявлення потенційних небезпек у майбутньому для впровадження коригуючих заходів. Прогностичний підхід спрямований на виявлення та пом'якшення ризиків, перш ніж вони стануть очевидними (вирішуючи сьогодні ризики завтрашнього дня). Цей підхід ставить наступні питання:

- *Які аварії та інциденти можуть статися в майбутньому і чому?*
- *Чи відчуваємо ми себе достатньо захищеними? Будь-які дії, які ми повинні зробити зараз, щоб уникнути таких майбутніх ризиків і подій (вирішення сьогодні ризиків завтрашнього дня)?*

Небезпеки, ризики та управління ризиками

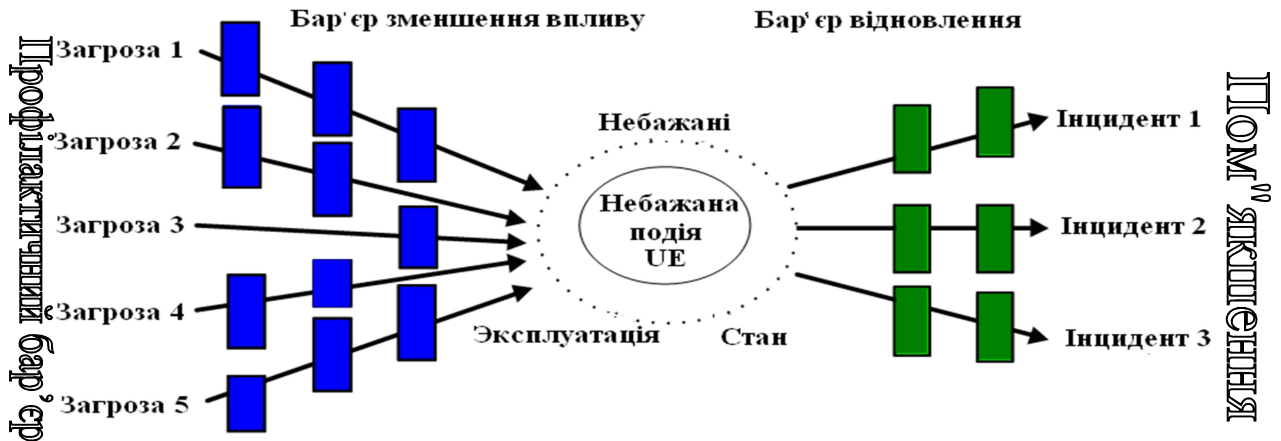
Моделювання ризику безпеки - розгляд «небажаних подій» (UE) як проміжного кроку між небезпеками та ризиками, а також інцидентами та аваріями.

Небезпеки можуть, окремо або в комбінації, призвести до «небажаних подій» (UE), якій запустить етап ескалації сценарію аварії, який називається «небажаним експлуатаційним станом» (UOS), де сценарій призвів до того, що аварії можна уникнути лише за допомогою успішних заходів відновлення або випадково.

Управління ризиками, спрямовані на запобігання «небажаним подіям» (UE) та «небажаним експлуатаційним станом» (UOS), є запобіжними бар'єрами.

Засоби контролю, які запобігають виникненню аварії в UOS, визначаються як бар'єри відновлення, тоді як засоби контролю, що пом'якшують наслідки інциденту або аварії, називаються бар'єрами для зменшення.

Цей підхід до контролю ризиків у вигляді діаграми



Малюнок 1 - Модель контролю ризику «Bow Tie»

Реєстрація небезпеки

GM4 ORA.GEN.200(a)(3)

Керівник з безпеки повинен вести реєстр (або журнал) небезпек.(Додаток 7)

Виявлення небажаних подій та небезпек

Переліки наводиться в Реєстрі небажаних подій, що прийнято в АТО «ХАК ТСОУ»

База даних з БП АТО «ХАК ТСОУ» передбачає ведення наступних форм в електронному та паперовому вигляді:

а) « Hazard Identification List » містить всі небезпечні фактори, виявлені під час аналізу подій і досліджень з БП або за допомогою будь-якого іншого джерела. Деякі небезпечні фактори можуть сприяти різним інцидентам і АП. Правильна ідентифікація, оцінка ризиків і пом'якшення наслідків небезпечних факторів має важливе значення для БП. Всім небезпечним факторам присвоюється реєстраційний номер.

Небажана подія перевіряється на небезпечні фактори, тобто чинники, які, окремо або в поєднанні, могли б призвести до авіаційної події. Небезпечні фактори обираються з «Hazard List.xls» (Додаток 12) або створюються нові записи при необхідності. Для кожного небезпечного фактору оцінюється ризик, результат позначається в області рівнів ризиків.

Засоби контролю з безпеки/ методи пом'якшення наслідків потім досліджують з метою зниження «Неприйнятного ризику» до «Допустимого ризику» або «Прийнятного ризику» або втримати «Допустимий ризик» під відповідним контролем. Методи пом'якшення наслідків записуються як Коригувальні дії, коли будуть затверджені керівництвом.

Аналіз засобів контролю з безпеки / Методів по м'якшення наслідків може також

сформувати Ре- комендації з БП. Рекомендації з БП - пропозиції по покращенню стану БП в результаті проведення коригувальний дій.

Для підтримки в актуальному стані бази даних з небезпечних факторів та їх оцінки, Керівник з безпеки забезпечують їх щорічний перегляд, про що робить помітку в базі даних.

б) Форма завершальної дії (Додаток 13)- містить список подальших дій, вжитих після завершення аналізу події або проведених досліджень з БП та видачі рішень по здійсненню контролю / пом'якшенню наслідків або Рекомендацій з безпеки. Незалежно від джерела інформації (повідомлення, події, дослідження і т.і.), коли нові небезпечні фактори виявляються, вони реєструються в «Hazard List.xls», аналізуються та підлягають подальшій обробці.

Оцінка, опис та аналіз ризиків

Ризик поєднує два виміри: ймовірність наслідків небезпеки та їх важкість. Обидва виміри мають бути оцінені.

Аналіз імовірності

Оцінка імовірності базується на наступному двосторонньому процесі:

- аналізуються наслідки небезпеки для встановлення можливих причин, що впливають на існуючі бар'єри причини, фактори та бар'єри далі аналізуються для визначення імовірності виникнення події.

У причинно-наслідковому аналізі наслідків розглядаються людські та організаційні фактори для їх можливого впливу. Зазвичай ми розглядаємо прямі причини ("небезпечні дії"), фактори робочого місця та організаційні фактори ("провокація помилок або приховані умови").

- вимоги до сертифікації;
- процедури технічного обслуговування;
- існуючі нормальні та аварійні процедури;
- технічні засоби / обладнання;
- навчання;
- інші людські та організаційні фактори.

Причинний аналіз, що підтримується, діаграмами типу "Bow Tie", виконується до рівня деталізації, необхідного для встановлення відповідних значень правдоподібності. Альтернативно, значення можуть бути оцінені на основі експертних оцінок, або на основі спостережуваних або еталонних повторень, наданих для сектора, типу операцій, типу машин і т.д. Ймовірність може бути виражена з використанням термінології, такий як «дуже низький, низький, середній, високий і дуже високий».

Таблиця яку, використовує АТО ХАК ТСОУ для визначення імовірності

Імовірність виникнення події/Probability of occurrence

ІМОВІРНІСТЬ ВИНИКНЕННЯ РИЗИКУ

Імовірність	Значення	Оцінка
Частий	Може відбуватися багато разів. Часто в авіації. (в АТО ХАК ТСОУ відбулось 3 рази на рік)	5
Нерегулярний	Може відбуватися іноді. Нечасто в авіації (в АТО ХАК ТСОУ відбулось менш ніж 3 рази на рік)	4
Віддалений	Навряд чи має місце, але можливий. Рідко в авіації (в АТО ХАК ТСОУ відбулось 1 раз на рік)	3
Неймовірний	Дуже малоімовірно. В авіації відбулось 1 раз	2
Вкрай малоімовірний	Майже виключено, що подія можлива. В авіації не відбувалось	1

Аналіз важкості

Аналізується тяжкість усіх наслідків небезпеки.

Аналіз розглядає як короткострокові, так і довгострокові наслідки, такі як вплив на природне та робоче середовище.

Наслідки групуються, наприклад, втрата або пошкодження життя / здоров'я, навколишнього середовища, матеріальних цінностей / активів, функцій та репутації.

Визначення важкості зазвичай носить описовий (якісний / порядковий термін) характер, за винятком випадків, коли відповідні розрахунки (кількісні) можуть або повинні застосовуватися. Якісний аналіз описує ланцюги подій, які можуть впливати з небезпеки та її можливі наслідки. Кількісний аналіз використовується для розрахунку ступеня збитку, який може бути викликаний.

Серйозність може бути виражена за допомогою термінології, як-от «дуже маленька, мала, середня, велика і дуже велика». Значення кожного терміну виражається у словах та / або числах / діапазонах.

Серйозність факторів ризику визначається рівнем завданої шкоди, який обґрунтовано може мати місце у вигляді наслідків або результатів виявлених факторів небезпеки показано типову таблицю оцінки ступеня серйозності факторів ризику для БП.У таблиці міститься п'ять категорій, що характеризують ступінь серйозності, опис кожної категорії з присвоєнням кожній категорії визначеного значення

Таблиці, які АТО «ХАК ТСОУ» використовує для визначення важкості:

Серйозність подій/Severity of occurrences

ВАЖКІСТЬ НАСЛІДКІВ		
Визначення	Сенс	Ступінь
Катастрофічна /Catastrophic	Нещасний випадок що призвів до смерті або знищення обладнання (людські жертви, руйнування, знищення майна)	E
Небезпечна Hazardous	Серйозні поранення або значне пошкодження обладнання(серйозне зменшення рівня безпеки, настання стресу чи такого робочого навантаження, коли немає впевненості в правильному і повному виконанні завдань персоналом)	D
Значна/Major	Серйозний інцидент або поранення (істотне зменшення запасу міцності, зниження здатності операторів переборювати несприятливі експлуатаційні умови як результат підвищення робочого навантаження або внаслідок умов, що знижують ефективність роботи)	C
Незначна/Minor	Результат незначного інциденту (перешкоди, обмеження в експлуатації обладнання, використання аварійних процедур)	B
Дрібна/Negligible	Подія з незначними наслідками	A

важкість події	значення				оцінка
	персонал	навколишнє середовище	матеріальні цінності і майно	репутація	
<u>КАТАСТРОФІЧНА</u>	Кілька смертельних випадків	Масові наслідки (забруднення, руйнування та ін.)	Катастрофічні фінансові втрати. Пошкодження > 1 млн. Євро (*)	Міжнародний вплив	E
<u>НЕБЕЗПЕЧНА</u>	Фатальність	Ефекти важко відремонтувати	Важкі фінансові втрати з довгостроковими наслідками Пошкодження <1 млн. Євро (*)	Національний вплив	D

<u>ЗНАЧНА</u>	Серйозні травми	Заслужують на увагу місцеві впливи	Значні фінансові втрати Пошкодження <250 тис. Євро (*)	Значний вплив	С
<u>НЕЗНАЧНА</u>	Легкі травми	Невеликий вплив	Фінансові втрати з невеликим впливом Пошкодження <50 К € (*)	Обмежений вплив	В
<u>ДРІБНА</u>	Поверхневі або без травм	Незначний або без наслідків	Фінансові збитки з незначним впливом Пошкодження <10 К € (*)	Легкий або без впливу	А

Вплив існуючих контрольних дій на відновлення та бар'єри, які впливають на наслідки або ланцюг наслідків, слід розглядати, як це застосовне:

- сертифікаційні вимоги (протипожежний захист);
- існуючі ненормальні та надзвичайні процедури;
- заходи вторинної безпеки (наприклад, захист від удару, засоби індивідуального захисту);
- технічні засоби / обладнання;
- навчання;
- людські та організаційні фактори;
- готовність до надзвичайних ситуацій.

Оскільки оцінка ризику прогресує, можливо, що ітераційний процес може допомогти виявити нові фактори та бар'єри. Потім вони додаються до процедури і включаються в аналіз.

Рівні ризику можуть змінюватися в часі в залежності від характеру операції (її) (машини та обладнання, процедури та документація, умови польоту, кваліфікація персоналу, тривалість завдань тощо). Комплексні та актуальні дані, такі як оцінки ризиків та описи ризиків допомагають у виконанні ефективних оцінок ризиків.

Ризики повинні бути переоцінені, зокрема, коли внесені зміни.

Опис ризику

Опис ризиків є основою для оцінки ризиків і пом'якшення. Виходячи з результатів аналізу імовірності та тяжкості, ризик описується як поєднання імовірності виникнення та супутньої тяжкості.

Залежно від методу аналізу та критеріїв прийняття ризику, опис є якісним та / або кількісним. Рівень деталізації залежить від рівня деталізації аналізу імовірності та тяжкості.

Одним з методів, що можуть бути використані для опису ризику, є матриця ризику, що поєднує ймовірність ризику та тяжкість ризику. Див. Наступний розділ.

Якщо небезпека має більше одного наслідку, ризик може бути виражений як комбінація ймовірності та тяжкості для кожного з наслідків.

Необхідно визначити й задокументувати неточності в описі ризику. Якщо аналіз базується на критичних припущеннях або інших умовах, які можуть вплинути на оцінку, вони мають бути ідентифіковані та задокументовані (якщо це необхідно у формі аналізу чутливості).

Опис ризику і аналіз на небажаному рівні подій

небезпека може призвести до « небажаних подій. »(UE), які можуть погіршитися в інцидентах і аваріях. Небезпеки можуть сприяти декільком « небажаним подіям » (UE і, як правило, пов'язані з кількома небезпеками, які мають відповідний рівень ризику. Рівень ризику, пов'язаного з UE, не є, все-таки, середнім рівнем ризику, пов'язаним з небезпеками, які сприяють ризику. Ось чому для « небажаних подій. »(UE) також застосовується окремий рейтинг ризику.

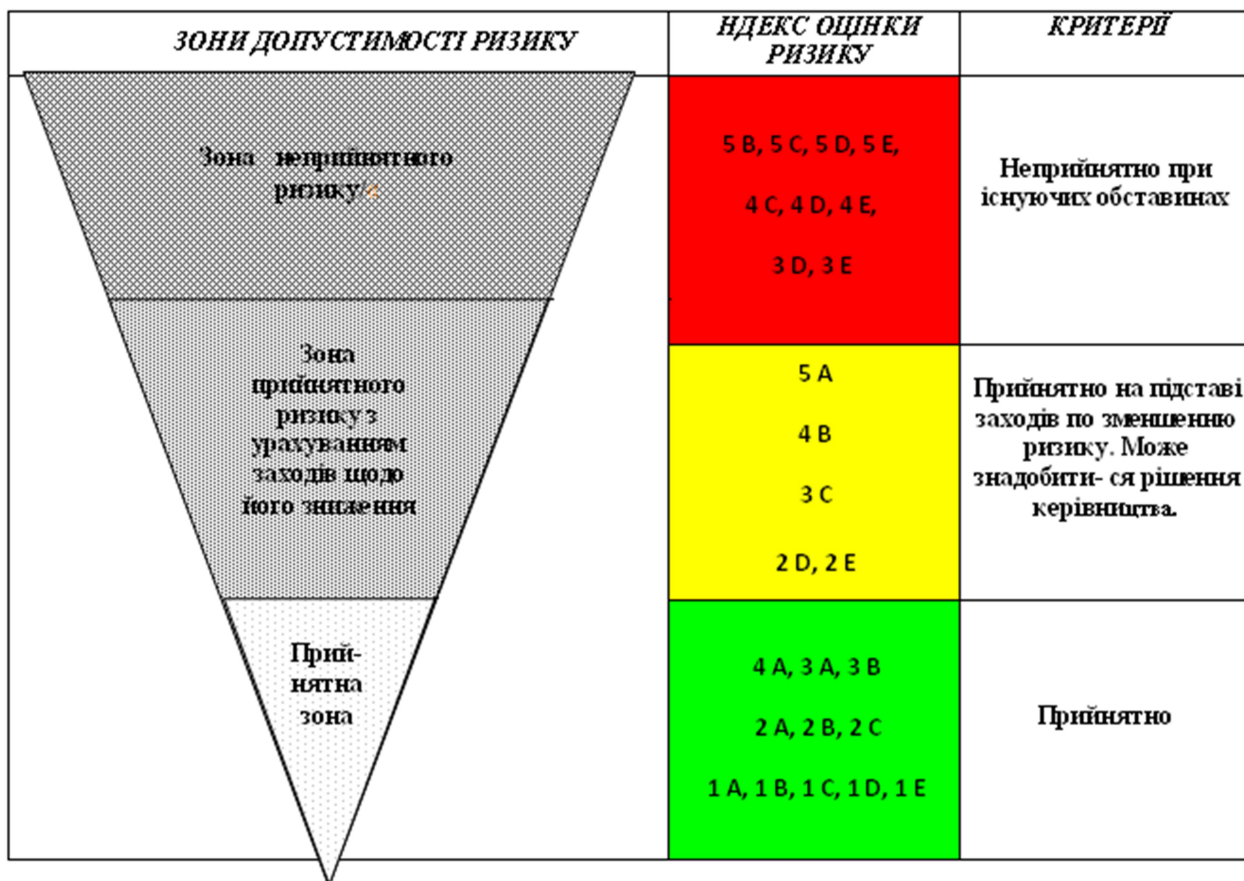
Оцінка ризиків

Результати аналізу ризиків порівнюються з критеріями прийнятності ризику.

Одним з методів, що використовується, є матриця з ризиком, що поєднує результати аналізу та критерії прийняття ризику.

Матриці прийнятності ризику, які АТО «ХАК ТСОУ» використовує :

ІМОВІРНІСТЬ РИЗИКУ	РІВЕНЬ РИСКУ				
	ДРІБНИЙ (A)	НЕЗНАЧНИЙ (B)	ЗНАЧНИЙ (C)	НЕБЕЗПЕЧНИЙ (D)	КАТАСТРОФІЧНИЙ (E)
ЧАСТИЙ (5)	5 A	5 B	5 C	5 D	5 E
НЕРЕГУЛЯРНИЙ (4)	4 A	4 B	4 C	4 D	4 E
ВІДДАЛЕНИЙ (3)	3 A	3 B	3 C	3 D	3 E
НЕЙМОВІРНИЙ (2)	2 A	2 B	2 C	2 D	2 E
ВКРАЙ МАЛОЙМОВІРНИЙ (1)	1 A	1 B	1 C	1 D	1 E



Індекс ризику	Рекомендовані критерії
5В, 5С, 5D, 5Е, 4С, 4D, 4Е, 3D, 3Е	Неприйнятний при існуючих обставинах
5А, 4В, 3С, 2D, 2Е	Прийнятний на підставі заходів по зменшенню ризику
4А, 3В, 3А, 2А, 2В, 2С, 1А, 1В, 1С, 1D, 1Е	Прийнятний

Приклад визначення індексу ризику

Серйозність РИЗИК Імовірність	А	В	С
5	5А	5В	5С
4	4 А	(4 В)	4С
3	3А	3В	3С

Приклад: Імовірність фактору ризику для безпеки польотів оцінюється як:

"Нерегулярний" (4). ; Серйозність фактору ризику для безпеки польотів оцінюється як

"Аварійний" (В).

Сукупність імовірності і серйозності (**4В**) це ризик для безпеки польотів, пов'язаний з наслідками розглянутої небезпеки.

Фактор ризику для безпеки польотів являє собою буквено-цифрову комбінацію.

Індекс ризику- 4 В де **В**- ступінь серйозності ризику; **4** - ступінь імовірності ризику.

Використання матриці «механічно», тобто без справжньої аргументації безпеки, заснованої на фактах і зв'язку між фактами, має обмежене користування. Командний аналіз серед фахівців різних областей, що мають відношення до досліджуваної операції, допомагає реалістично оцінювати ризик.

Оцінка ризику повинна базуватися на систематичному аналізі відповідної операції.

Значення червоного кольору вказують на неприйнятні рівні ризику, значення жовтого кольору - рівні допустимого ризику, а значення зеленого кодування встановлюють прийнятні рівні ризику.

Кожен рівень ризику вимагає конкретної дії, а рівні управління, які мають повноваження приймати рішення щодо переносимості ризиків для безпеки, повинні бути визначені.

I. Неприпустимий рівень ризику: червона зона в матриці: ризик занадто високий для продовження роботи.

Необхідні дії: Заборонити / призупинити операцію. Операція може бути відновлена тільки тоді, коли рівень ризику повертається до допустимого або прийняттого.

Рівні управління, які мають повноваження приймати рішення щодо переносимості ризику:

- для підтвердження оцінки ризику: Припущення, зроблені для визначення рівня ризику та його переносимості, повинні бути підтверджені Керівником з безпеки.

- для авторизації операцій: рівень управління, який має повноваження надавати дозвіл на операції на цьому рівні ризику: не застосовується: операції не можуть бути дозволені.

II. Допустимий рівень ризику: жовта зона в матриці: рівень ризику може бути допущений для операції, за умови, що відповідні заходи по зниженню ризику є в наявності.

Необхідні заходи: Ввести відповідні заходи щодо пом'якшення.

Рівні управління, які мають повноваження приймати рішення щодо переносимості ризику:

-для підтвердження оцінки ризику: Припущення, зроблені для визначення рівня ризику та його переносимості, повинні бути підтверджені Керівником з безпеки.

- для авторизації операцій: Управління, яке має повноваження надавати дозвіл на операції на цьому рівні ризику: відповідальний керівник.

III. Прийнятний рівень ризику: зелена зона в матриці нижче: ризик допустимий і може бути прийнятий для операції.

Необхідні дії: контролювати. Ризик вважається достатньо контрольованим і не потрібні додаткові заходи щодо зменшення ризику. Проте, відповідно до концепції ALARP, можуть бути вжиті заходи для подальшого зниження рівня ризику, якщо це можливо і обґрунтовано. Крім того, будь-які припущення, які використовуються для оцінки, повинні контролюватися, щоб переконатися, що вони залишаються дійсними.

Рівні управління, які мають повноваження приймати рішення щодо переносимості ризику:

- для підтвердження оцінки ризику: Припущення, зроблені для визначення рівня ризику та його переносимості, повинні бути підтверджені Керівником з безпеки.

- для авторизації операцій: Рівні керівництва, які мають повноваження надавати дозвіл на операції на такому рівні ризику: не застосовується: не вимагається спеціального дозволу: авторизація діяльності, що має «прийнятні ризики», підпадає під регулярний операційний контроль операцій.

Управління ризиками

Визначення заходів з управління ризиками (пом'якшення)

Оцінка ризику є основою для прийняття рішень щодо заходів щодо управління ризиками (пом'якшення) та оцінки ефективності цих заходів.

Заходи з управління ризиків визначають наслідки, пов'язані як з неприйнятним ризиком, так і з допустимим ризиком, і де подальші заходи зниження ризику є здійсненими і обґрунтованими.

Ідентифікація можливого пом'якшення заснована на описі та оцінці ризиків, враховуючи, зокрема, будь-які визначені неточності та критичні припущення.

Визначені контролі, які можуть усунути наслідки небезпеки, заходи зниження імовірності та заходи зі зменшення важкості. Ці заходи повинні враховувати людські фактори (підготовку та компетентність), обладнання або організаційні чинники (процедури).

Персонал АТО «ХАК ТСОУ» сприяє визначенню заходів з контролю ризику, зокрема, коли вони стосуються особистого обладнання (окуляри, шоломи та інше льотне обладнання), шляхом їх прийняття та використання.

Пріоритети управління ризиками

Заходи з управління ризиками здійснюються на основі таких пріоритетів:

- усунути наслідки небезпеки;
- зменшити ймовірність виникнення;
- зменшити тяжкість.

Типи управління ризиками

Типи управління ризику включають:

- пасивний технічний контроль (резервування системи);
- активний технічний контроль (автоматична система пожежогасіння).

Оцінка впливу на ризик

Ефект управління, що зменшує ризик, оцінюється з урахуванням:

- функціональність: чи впливає цей захід на здатність виконувати діяльність?
- надійність: чи буде цей захід ефективним за різних умов і з часом?
- можливі інші ефекти, такі як введення нових ризиків.

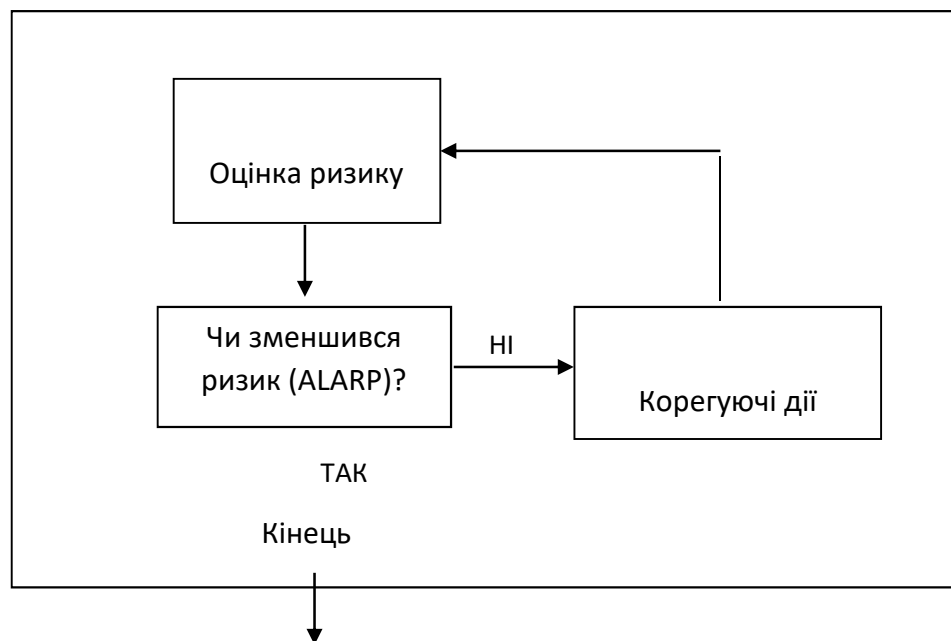
При визначенні заходів з контролю ризиків слід визначити будь-які нові ризики, які можуть виникнути в результаті впровадження таких заходів («ризики заміщення»).

Ризик повторно оцінюється з урахуванням впливу запропонованих ефектів контролю ризику, як показано в таблиці нижче:

Оцінка ризиків	Початковий рівень ризику	Управління ризиком	Наслідковий рівень ризику
Ризик 1			
Ризик 2			
Ризик 3			

Заходи не обов'язково є достатніми для повернення рівня ризику до прийнятного або допустимого рівня в першому раунді: якщо критерії прийняття ризику вимагають подальшого зменшення ризику, порівняння описує процес оптимізації. Таким чином, додаються нові засоби контролю ризику або змінюються існуючі контролю ризику, поки ризик не буде таким низьким, наскільки це практично можливо (ALARP).

Процес зменшення ризику



Концепція ALARP поєднує **технічну можливість** подальшого зниження ризику для безпеки та **вартості**; демонстрація того, що ризик безпеки - це ALARP, означає, що будь-яке подальше зниження ризику є або нездійсненим, або значно перевищує вартість.

Аналіз витрат та вигод

Заплановані заходи щодо пом'якшення повинні бути піддані аналізу витрат та вигод, що допомагає визначити найбільш відповідні заходи. Зважаючи на необхідність пом'якшення, необхідно досягти бажаних переваг безпеки та бути економічно прийнятними.

Матриця аналізу переваг простих витрат

	ВИГОДА			
		Висока	Середня	Низька
	Низька	1	2	3
	Середня	2	3	4
	Висока	3	4	5

Критерії прийнятності щодо витрат на впровадження заходів з пом'якшення та очікуваних вигод, повинні бути схвалені відповідальним керівником.

Висновок і документація

Будь-яка оцінка ризику повинна бути задокументована і містити однозначні, точні та чіткі висновки, які дозволять особам, які приймають рішення, прийняти відповідні рішення щодо зменшення контролю (див. Розділ Впровадження заходів з контролю ризиків).

Документація включає посилання на інші документи (за наявності) і вказує на необхідність подальшої роботи.

Область застосування

Документація з оцінки ризику включає в себе або посилання, як вимагається, опису наступного:

- мета оцінки ризику;
- проаналізована діяльність / питання;

- залучення персоналу та інших операторів, з якими ми взаємодіємо;
- контекст / рамки діяльності / питання;
- оцінка того, хто постраждав від діяльності / питання і як;
- використовувані дані;
- метод аналізу;
- небезпеки;
- фактори та наслідки
- невизначеності та припущення, зроблені для оцінки;
- імовірність і тяжкість;
- заходи щодо зменшення ризику;
- оцінка ризику;
- висновки.

Зміни, які можуть призвести до скасування висновків оцінки ризику

Зміни, які можуть призвести до недійсності висновку про оцінку ризику:

- значні зміни в передумовах та контексті;
- нові знання про ризики (досвід аварій і подій, повідомлення про занепокоєння з питань безпеки, дослідження, кращі методи аналізу ризиків, внутрішні інспекції, аудити і перевірки, звітування про небезпеку);
- значні зміни в даних, що використовуються для оцінки;
- значні організаційні зміни, які можуть вплинути на оцінку; і
- кілька менших змін, які разом можуть становити значну зміну.

Залежно від типу впливу та характеру змін Керівник з безпеки може прийняти рішення про переоцінку ризику.

Впровадження заходів з управління ризиками

Здійснення заходів з контролю за ризиком (пом'якшення) може, в залежності від характеру цих заходів, призвести до виконання плану з визначення того, хто відповідає,

необхідних ресурсів, кінцевого терміну і етапів впровадження. План виконання періодично переглядається до завершення або перегляду.

Моніторинг, перегляд і вдосконалення

Процес оцінки ризику контролюється з метою:

- аналіз та вивчення подій, змін та тенденцій;
- виявлення змін у внутрішньому та зовнішньому контексті, включаючи зміни самого ризику;
- забезпечення ефективності заходів щодо зменшення ризику; і
- виявлення нових ризиків.

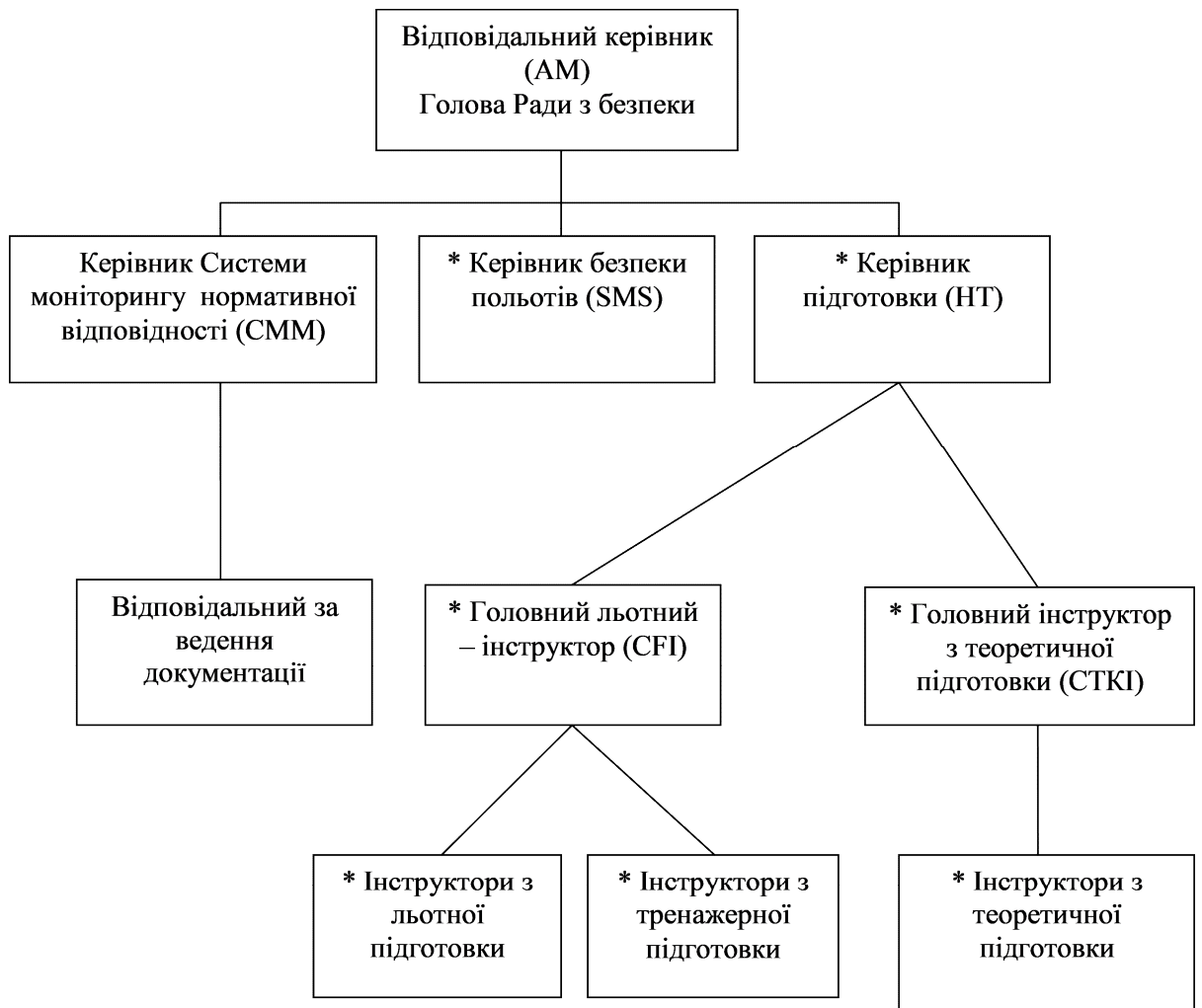
Моніторинг і перегляд можуть бути здійснені шляхом періодичних інспекцій, перевірок і аудитів, оцінки ризиків і самого процесу управління ризиками, з метою прагнення до постійного зниження рівня ризику.

Завдання цілі та рівні з безпеки польотів на 2019 - 2023 р.р.:

АТО «ХАК ТСОУ» в рамках свого плану забезпечення безпеки польотів встановлює наступні цілі і рівні безпеки:

1. Удосконалення СУБП на протязі 5 років
2. Недопущення випадків АП, НП, серйозних інцидентів на аеродромі через діяльність структурних підрозділів, що забезпечують польоти та наземне обслуговування ПС.
3. Недопущення випадків не санкціонованого зайняття ЗПС
4. Залишити показник безпеки, що стосується пошкоджень ПС на землі на рівні показника 2018 року (0%)
5. Залишити показник безпеки, що стосується FOD, який призвів до травмування людей ,пошкодження ПС, майна на рівні показника 2018 року (0%)
6. Зменшити показник безпеки , що стосується потенційно небезпечних факторів.
7. Не допустити авіаційної події і людські жертви під час виконання польотів;
8. Не допустити серйозних інцидентів з вини персоналу АТО;
9. Утримувати середній наліт на одну авіаційну подію не менше 1000 годин на рік (коефіцієнт аварійності на рівні 0,001);
10. Добитися зниження частоти відмов авіаційної техніки на землі менше 10 значних дефектів на ПС на 1000 годин нальоту;
11. Зниження кількості подій або конкретних типів інцидентів за певний період часу.

Організація управління безпекою в АТО «ХАК ТСОУ»



Рішення ради з безпеки

