МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ, ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА АЕРОНАВІГАЦІЙНИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
д-р техн. наук, проф.
_____В.Ю. Ларін
«___»_____2020 р.

ДИПЛОМНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА
ЗА ОСВІТНЬО-ПРОФЕСІЙНОЮ ПРОГРАМОЮ
«ОБСЛУГОВУВАННЯ ПОВІТРЯНОГО РУХУ»

Тема: «Оцінка інформаційних ризиків при обслугованні повітряного руху»

Виконав: _____ В. Москалюк

Керівник: д-р техн. наук, доц. _____ Ю.А. Авер'янова

Нормоконтролер: _____Г.Ф. Аргунов

Київ 2020

ЗМІСТ

ВСТУП

Актуальність. Сучасна авіація – це широке використання складних інтегрованих інформаційних систем, нових технологій систем зв’язку, навігації та спостереження для полегшення та удосконалення виконання щоденних операцій. Ці технології надали розвиток та удосконалення функціям виявлення, ідентифікації та оцінки вразливих зон та їх аналізу, що є необхідним для підвищення рівня безпеки сучасних та перспективних систем управління повітряним рухом (УПР). Важливим елементом сучасної авіації також є інновації в проектуванні та виробництві сучасних літаків, що побудовані за використанням бортових інформаційно-комунікаційних технологій які підтримують зв'язок з зовнішніми мережами для обміну даними на різних етапах виконання польоту.

Таким чином невід’ємною частиною безпечного функціонування перспективної транспортної авіаційної системи є інфраструктура для обміну інформацією, щоб забезпечити надійний обмін та поширення даних між зацікавленими сторонами управління повітряним рухом [1]. В такому контексті інформація стає одним з основних ресурсів, який потребує захисту від атак на дані про польоти, дані спостереження, планування та інші. В такому контексті аналіз та оцінювання потенційних ризиків, що спрямований на попередження руйнування конфіденційності, цілісності та доступності інформації є важливим та актуальним завданням.

Мета і завдання виконання дипломної роботи – аналіз, ідентифікація загроз та вразливостей інформації та інформаційним системам при ОПР та оцінка інформційних ризиків

Об’єкт дослідження – процес інформаційного забезпечення сучасного та перспективного ОПР

Предмет дослідження – методи та моделі оцінки ризиків в системі ОПР, властивості інформації, систем зберігання, обробки та передавання в ОПР

Методи дослідження – в роботі використані наступні методи: метод наукового дослідження, в процесі дослідження технології управління інформаційними ризиками метод порівняння, для ідентифікації загроз та вразливостей, та також результатів оцінки інформаційних ризиків метод аналізу, для якісного оцінювання ризиків метод тестування та метод матриць (матриці ризику).

Наукова новизна отриманих результатів - в роботі набула подальшого розвитку методика визначення прийняття рішення щодо наслідків можливого ризику та прийнятності, неприйнятності, або прийнятності за певних умов ризику, з урахуванням портрету потенційних зловмисників та їх мотивів.

Практичне значення отриманих результатів - результати проведеного дослідження можна використовувати для розробки рекомендацій та впровадження необхідних мір для зменшення інфораційних ризиків в процесі ОПР нарізних рівнях: міжнародному, державному, або на рівні окреитх організацій.

ABSTRACT

Explanatory Notes to Master Thesis «Information Risks Assessment at Air Traffic Control»: 88 с., 15 рис., 9 табл., 37 джерел.

Object of study – Process of information provision of modern and prospective ATC

Subject of study – methods and models of risks assessment in the system of ATC, information peculiarities, peculiarities of the systems of of information gathering, processing and sharing at ATC

Aim of the study – algorithm development for information risks assesment for the ATC tasks and development of recommendation for risks mitigation

Methods of study – in this study the next methods are used: method of scientific study

в роботі використані наступні методи: метод наукового дослідження, в процесі дослідження технології управління інформаційними ризиками метод порівняння, для ідентифікації загроз та вразливостей, та також результатів оцінки інформаційних ризиків метод аналізу, для якісного оцінювання ризиків метод тестування та метод матриць (матриці ризику).

Relevance. Сучасна авіація – це широке використання складних інтегрованих інформаційних систем, нових технологій систем зв’язку, навігації та спостереження для полегшення та удосконалення виконання щоденних операцій. Ці технології надали розвиток та удосконалення функціям виявлення, ідентифікації та оцінки вразливих зон та їх аналізу, що є необхідним для підвищення рівня безпеки сучасних та перспективних систем управління повітряним рухом (ОПР). Важливим елементом сучасної авіації також є інновації в проектуванні та виробництві сучасних літаків, що побудовані за використанням бортових інформаційно-комунікаційних технологій які підтримують зв'язок з зовнішніми мережами для обміну даними на різних етапах виконання польоту.

Таким чином невід’ємною частиною безпечного функціонування перспективної транспортної авіаційної системи є інфраструктура для обміну

інформацією, щоб забезпечити надійний обмін та поширення даних між зацікавленими сторонами управління повітряним рухом [1]. В такому контексті інформація стає одним з основних ресурсів, який потребує захисту від атак на дані про польоти, дані спостереження, планування та інші для забезпечення конфіденційності, цілісності та доступності інформації авторизованим користувачам. В такому контексті аналіз та оцінювання потенційних ризиків, що спрямований на попередження руйнування конфіденційності, цілісності та доступності інформації є важливим та актуальним завданням.

БЕЗПЕКА ПОЛЬОТІВ, ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, ОЦІНКА РИЗИКІВ, ОБСЛУГОВУВАННЯ ПОВІТРЯНОГО РУХУ, АЛГОРИТМ

РОЗДІЛ 1 СУЧАСНІ АВІАЦІЙНІ КОНЦЕПЦІЇ ТА ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОПР

Реалізація цілей майбутнього ефективного управління повітряним рухом базується на прогресі та розвитку нових технологій, систем та процедур - систем навігації та спостереження, враховує зростання щільності повітряного руху, збільшення використання безпілотних літальних апаратів, та їх експлуатаційних завдань , що в свою чергу відображено у нових концепціях та програмах УВД (концепція вільного польоту [2], нова концепція операцій на основі траєкторії [3], проект NextGen [4], проект SESAR [5]). Це також зазначається в глобальному аеронавігаційному плані [6]. В першому розділі зроблено стислий огляд сучасних авіаційних концепцій з фокусом на життєвий цикл інформаційних потоків в рамках згаданих концепцій для подальшого аналізу можливих вразливостей, загроз та оцінки інформаційних ризиків.

1.1. Програма NextGen (Аеронавігаційна система нового покоління)

Програма NextGen була запропонована федеральною авіаційною адміністрацією Сполучених Штатів Америки, як реалізація модернізованої системи повітряного транспорту наступного покоління (NextGen), що спрямована на збільшення безпеки, ефективності та передбачуваності польотів [7]. Для реалізації майбутньої системи впроваджуються нові технології та можливості для формування більш сучасної, стійкої та безпечної системи повітряного простору. На сайті FAA федеральної авіаційної адміністрації зазначається, що системи повітряного транспорту NextGen охоплює інноваційні та трансформаційні технології, які розробляються та застосовуються після ретельного тестування на безпеку. Всі оновлення NextGen впроваджуються з урахуванням пріоритетів безпеки, підвищення ефективності, поліпшення екологічних показників.

Основні міни стосуються функцій вдосконалення зв'язку, навігації та спостереження таким чином, щоб повітряне судно мало можливість отримувати вказівки з землі щодо ідентифікації часу та положення швидко, легше та з меншим ризиком помилок.

Що стосується функції зв’язку: літаки мають бути обладнання системи, які можуть точно визначити, де вони повинні знаходитись і в який час. Системи обміну даними мають допомогти пілотам та службам ОПР спілкуватися швидше, легше та з меншим ризиком помилок, ніж це можливо на перевантаженних радіо частотах.

Стосовно функцій навігації: пропонується переходити переважно супутникову навігаційну систему, яка є більш точною, ніж традиційні наземні навігаційні засоби. Супутники дозволяють дотримуватися оптимальних траєкторій польоту в будь-якому місці вильоту, крейсерської висоти, прибуття та посадки. Точні, ефективні процедури можуть скоротити час польоту, витрату палива та викиди вихлопних газів літака, одночасно доправляючи пасажирів до пунктів призначення в більш передбачуваний час.

Щодо функцій спостереження: Поточна реалізація NextGen має забезпечити служби ОПР точним розташуванням літаків та чітким баченням навколишніх умов, включаючи погодні умови та інші літаки.

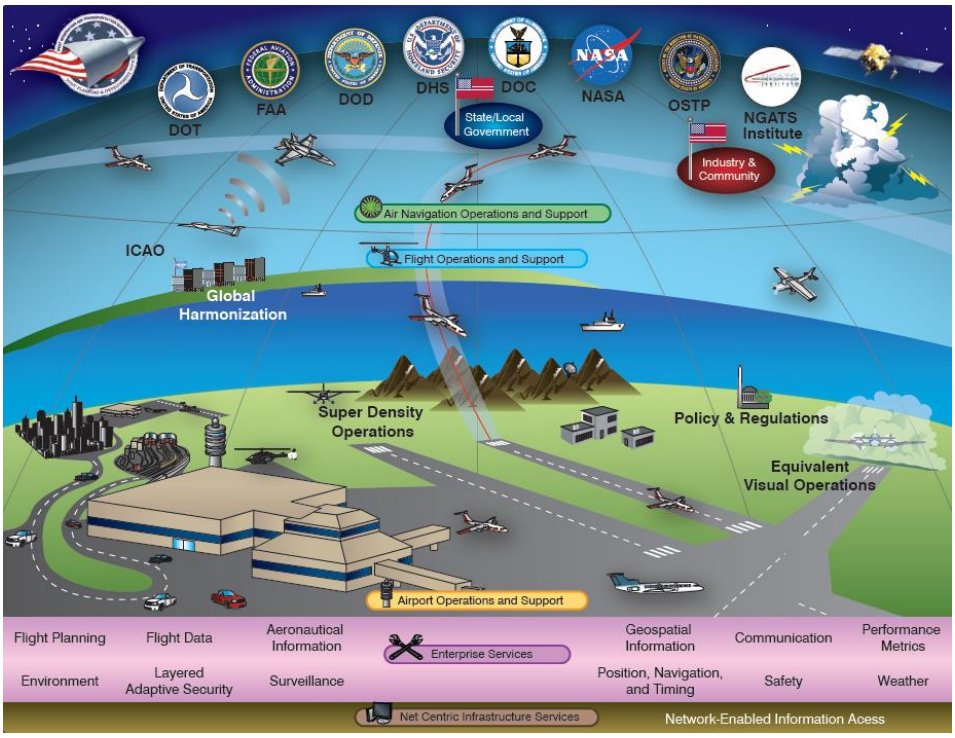

Рисунок 1.1 – Переваги та організація програми NextGen (з сайту https://www.flightliteracy.com/improvement-plans-part-one/)

1.2. ОПР концепція Free Flight

Концепція Free Flight перекладається з англійської як, вільний політ. Мета втілення концепції - підвищення безпеки польотів, пропускної спроможності повітряного простору, експлуатаційної ефективності та економічних показників. У концепції вільного польоту відповідно до рекомендації ІКАО служби УПР мають визначати характер заходів щодо вдосконалення технологій в галузі зв'язку, навігації та спостереження (CNS), що спрямовані на забезпечення організації повітряного руху (ОПР) [8].

Мета концепції - надання екіпажу повітряних судів (ПС) свободи в оперативному виборі траєкторії руху по маршруту, швидкості та профілю польоту, та в той же час забезпечити надійність, безпечне розв’язання

можливої конфліктної ситуації (потенційного ризику) з урахуванням технічної забезпеченості польотів за приладами. Отже питання цілісного інформаційного забезпечення ідентифікованих учасників ПР є важливим для реалізації концепції вільного польоту.

1.3. Загальносистемне управління інформацією (SWIM)

В документі ІКАО [9] зазначається, що концепція загальносистемного управління інформацією (SWIM) складається із стандартів, інфраструктури та управління, які дозволяють керувати інформацією, пов'язаною з УПР, обмінюватися цією інформацією між кваліфікованими сторонами за допомогою служб, що взаємодіють. SWIM забезпечує безперешкодний доступ до інформації та обмін даними між усіма провайдерами та користувачами інформації та послуг УПР. Системне управління інформацією використовує ділові практики управління інформацією із сектору інформаційних технологій та технологій зв'язку, використовує відкриті стандарти та веб-технології, і застосовує їх до УПР [10]. Такий підхід має забезпечити доступність взаємодіючих, багаторазових та керованих користувачами інформаційних послуг. На Рис.1.2 зображено цифрову парадигму концепції SWIM.

Європейська організація з безпеки повітряної навігації Евроконтроль (EUROCONTROL) підтримує розробку та впровадження SWIM відповідно до:

- інформаційних послуг
- інформаційно-технічної інфраструктури
- розробки стандартів та допоміжних матеріалів
- управління
- цивільно-військової співпраці

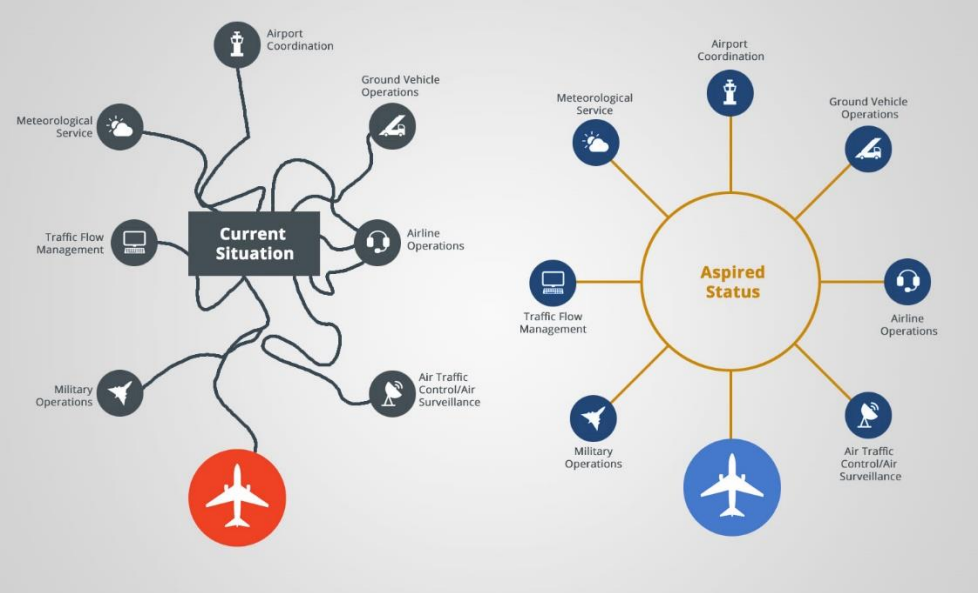

Рисунок1.2. – Схематичне порівняння сучасного УПР та за втілення концепції SWIM (зображення з вебсайту https://sky-review.ru/cifrovaya-paradigma-swim)

та сприяє науково-дослідним проектам, орієнтованим на галузеві аспекти SWIM. Зокрема, у дослідження обміну інформацією повітря-земля та динамічної взаємодії між операційними системами.

В роботах [11,12] зазначається, що FAA запропонувало програму SWIM використання супутників зв‘язку для більш ефективного обміну інформацією про робочий статус аеропортів, метеорологічний стан, польотні дані та інші спеціальні дані використання повітряного простору. Мета програми - забезпечення відповідних структур гнучкою та безпечною інформацією, а також забезпечення переходу від використання наземних систем управління повітряним рухом до супутникових в рамках концепції розвитку авіації наступного покоління (NextGen). В програмі зазначається, що використання SWIM дозволить більш ефективно забезпечити інформацією про стан повітряного простору для УПР. Ключовою послугою SWIM має стати можливість запиту та одержання поточної цільової інформації в найбільш

цікавій зоні для пілотів або авіаційних диспетчерів. Основними принципами розповсюдження інформації в рамках проекту SWIM є:

- інформація, що поширюється, має бути захищеною та розповсюджуватися системно;

- інформація, що потрібна користувачу, має бути доступною в будьякий час та в будь-якому місці;

- інформація має бути персоналізованою, відфільтрованою, цілісною та доступною за запитом;

- система має дотримуватись можливості захищеної взаємодії мереж.

Рівномірне та безперешкодне впровадження стандартів SWIM ІКАО зустрічає виклики, які обумовлюються потребою чималих фінансових коштів, часових затрат та пов‘язане із значними робочими ризиками. Обмеження сучасних систем обміну інформацією сповільнюють розвиток та втілення сучасних концепцій. До основних обмежень відносять [47]:

- інформаційний контент, що передається не є уніфікованим на міжнародному рівні, що може призвести до непорозуміння, втрати або виключення інформації з повідомлення. А отже є загрозою порушення цілісності та доступності.

- інтерфейси, що використовуються, не забезпечують необхідної гнучкості системи, що також впливають на доступність інформації;

- обмеження розміру повідомлення в сучасних системах, що сприяє втраті, а отже і цілісності;

- обмеження в доступі до оперативної інформації, що є прямою загрозою забезпечення доступності інформації авторезованими користувачами;

- низький рівень захисту інформації, що передається, зменшує кількість учасників, які б могли поширювати інформацію.

Тенденція розвитку сучасних систем обміну та передавання інформації передбачає підвищення ефективності систем передавання, тобто можливість збільшення інформаційного потоку та його надійність, доступність та конфіденційність інформації, що передається, а отже є загрозою

інформаційній безпеці. Одночасно втілення сучасних концепцій потребує розвитку систем обміну інформацією нового покоління, що здатні знаходити інформацію за конкретним запитом в залежності від обставин, а не оперувати великою кількістю даних для простого попереднього ознайомлення. Отже необхідно створювати можливість взаємодії мереж, що дозволить системі справлятися з усіма складнощами оперативного обміну інформацією з урахуванням забезпечення інформаційної безпеки та захисту інформації.

Отже, очікується, що нові системи SWIM та УВД значно активніше використовуватимуть інформаційні технології для розповсюдження всієї інформації, що стосується повітряного руху, включаючи траєкторію руху літаків та умови польоту, погоду, стан аеропортів та навігаційні засоби. Системи розроблені таким чином, щоб їх можна було розширювати, щоб при необхідності можна було додавати нові інформаційні послуги. Ці інформаційні послуги базуватимуться на відкритих стандартах і будуть доступні всім споживачам послуг з відповідними правами доступу.

З іншого боку виникає необхідність створення та підтримки служби безпеки з функціями, які використовуються системами та основними службами для забезпечення надання послуг SWIM відповідно до встановлених політик безпеки. Ці функції включають забезпечення основних цілей безпеки, а саме, забезпечення ,безпечних мережевих підключень, ідентифікації, конфіденційності, цілісності інформації.

Таким чином забезпечення інформаційної безпеки в розподіленому мережевому середовищі надання послуг, яким є система SWIM є викликом та одним з пріоритетів, тому що для користувачі системи повинні бути впевнені, що їх конфіденційні дані захищені відповідно до вимог стандартів безпеки.

1.4. Програма Collaborative Air Traffic Management Technologies

Програма Collaborative Air Traffic Management Technologies, яку з англійської можна перекласти як спільні технології управління повітряним

рухом запропонована Федеральною авіаційної адміністрацією для покращення загальної ефективності Національної системи повітряного простору, забезпечення більшої гнучкості при плануванні польотів та найкращим чином використовувати наявний повітряний простір та пропускну спроможність аеропорту [7]. Програма націлена на надання пакету комплексної інформації про переважні альтернативні маршрути з урахуванням погодних чи процедурних обмежень, на вдосконалення комунікації між службами УПР та екіпажами ПС та, на вдосконалення відображення інструкцій диспетчерам повітряного руху.

Можна виділити наступні преваги програми спільної технології управління повітряним рухом

- Пропускна спроможність. За умови майбутнього зростання кількості польотів ПС необхідно покращувати ефективність, гнучкість та передбачуваність польотів ПС, забезпечуючи при цьому відсутність негативних впливів на безпеку та приділяючи належну увагу екології. Також необхідно зазначити, що система УПР має бути стійкою до перебоїв у обслуговуванні та тимчасової втрати пропускної спроможності. Така перевага відповідає потребам УПР мінімізувати обмеження потоку руху в пікові години та місця.

- Ефективність. Забезпечення своєчасного вильоту та прибуття, а також польоту за оптимально визначеної траєкторією.

- Гнучкість. Така перевага забезпечує здатність усіх користувачів повітряного простору оперативно змінювати (корегувати) траєкторії польоту та регулювати час вильоту та прибуття, дозволяючи тим самим користуватися перевагами експлуатаційних можливостей, якщо вони виникають.

- Передбачуваність. Властивість користувачів повітряного простору та служб УПР забезпечувати стабільний та надійний рівень продуктивності. Ця властивість є важливою для користувачів, коли вони розробляють і керують своїми графіками.

Робоча компонента програми спільної технології управління повітряним рухом, в свою чергу, потребує [13]

- автоматизації використання даних щодо кількості слотів прибуття, які слід зарезервувати для позапланового попиту;

- інтегрування відображення інтегрованої погоди в коридорі на дисплей TFSM (Traffic Flow Management System);

- інтегрування інструменту планування доступності маршрутів на дисплей TFSM;

- автоматизованого інструменту підтримки прийняття рішень, який визначає обмежений повітряний простір і допомагає планувальникам руху формулювати рішення, враховуючи переваги користувачів повітряного простору;

- надає можливість передавати згенеровані зміни маршрутів до автоматичних систем УПР для їх подальшого виконання;

- зміна апаратної та програмної архітектури набору інструментів підтримки прийняття рішень для потреб служб УПР. Необхідно забезпечити інтегрований набір інструментів та відповідати архітектурі програмного забезпечення модернізованого вузла TFMS;

- збільшує інформаційне забезпечення про ситуацію та покращення прогнозування обмежень за рахунок включення даних, що надаються за допомогою механізмів широкоформатного управління інформацією (SWIM). Наприклад, інформація про стан повітряного простору спеціального користування.

Аналіз вимог щодо втілення зазначеної програми показує значне підвищення в автоматизації систем, що передають, оброблюють та відображають інформацію, використання перспективних механізмів управління інформацією, наприклад SWIM. Це, в свою чергу, означає, що такі системи є потенційно вразливими до кібер ризиків, які все частіше

виникають в авіації. А отже аналіз та оцінювання ризиків є необхідним кроком для удосконалення системи управління безпекою.

1.5. Операції на основі траєкторії (Trajectory-Based operations TBO)

Операції засновані на траєкторії [14], є переходом до використання розподіленої, спільно розробленої траєкторії, та є основою для прийняття рішень учасниками повітряного руху. Таким чином концепція операцій заснованих на траєкторії надає можливість перевести операції у бік більшої передбачуваності, коли рішення, що впливають на політ, узгоджуються між учасниками повітряного руху для забезпечення ешелонування з урахуванням пріоритетів при розподілі.

Загальні відмінності концепції операцій заснованих на траєкторії від існуючої наступні:

- Спільний доступ до інформації про траєкторію, що сприяє однаковому рішенню при узгодженні траєкторії;
- Управління інформацією про траєкторію за допомогою прийняття спільних рішень (Collaborative Decision Making CDM);
- Спільна траєкторія, якою керують є Узгодженою траєкторія. Вона використовується як загальний план польоту із загальним наміром, який слід досягти під час виконання польоту.

В [14] вказується, що учасники повітряного руху для обміну даними про повітряний та метеорологічний стани, аеродромну інформацію мають доступ до постійно обновлюваного інформаційного спільного простору на основі SWIM та нових технологічних досягненнях. Ця спільна інформація забезпечує сумісне бачення всіх учасників повітряного руху факторів, що впливають на траєкторію руху кожного польоту. Ці фактори можуть впливати на траєкторію польоту як безпосередньо, так і через рішення, що впливають на її траєкторію. Інформація, яка підлягає обміну вміщує в себе:

- інформація про фактори навколишнього середовища, що впливають на траєкторії (наприклад, вітри, конфігурація повітряного простору, пропускна спроможність аеродрому, загальні обмеження);

- інформація, що дозволяє координувати рішення між компонентами концепції (наприклад, , обмеження траєкторії, плани випробувань);

- додаткова інформація, що дозволяє вдосконалити прогнозування траєкторії (наприклад, дані, що передані літаками);

- інформація про узгодженої траєкторії, що є основою для управління та контролю цієї траєкторії.

Обмін інформацією також повинен враховувати відповідні робочі потреби. Спільний доступ до інформації про траєкторію повинен проводитись із швидкістю і в межах допусків, достатніх для досягнення бажаних рівнів продуктивності системи УПР. Інформація також надаватиметься лише уповноваженим учасникам (наприклад, обмежуючи обмін власними або конфіденційними даними). Робота в такому середовищі дає всім зацікавленим сторонам чітку видимість узгодженої траєкторії з бічними, вертикальними або часовими траєкторіями та / або загальними обмеженнями, що її визначають, а також деяких робочих факторів, які можуть на неї вплинути. Таке спільне використання та оновлення забезпечується завдяки управлінню інформацією та сучасній автоматизації.

В роботі [15] вказується, що при втілені операцій заснованих на траєкторії можна очікувати збільшення кількості польотів, змінами у льотних операціях, введенням автономних літаків. В цій роботі різниця та обґрунтування показані за допомогою наступних зображень (Рис.1.3 та 1.4.).

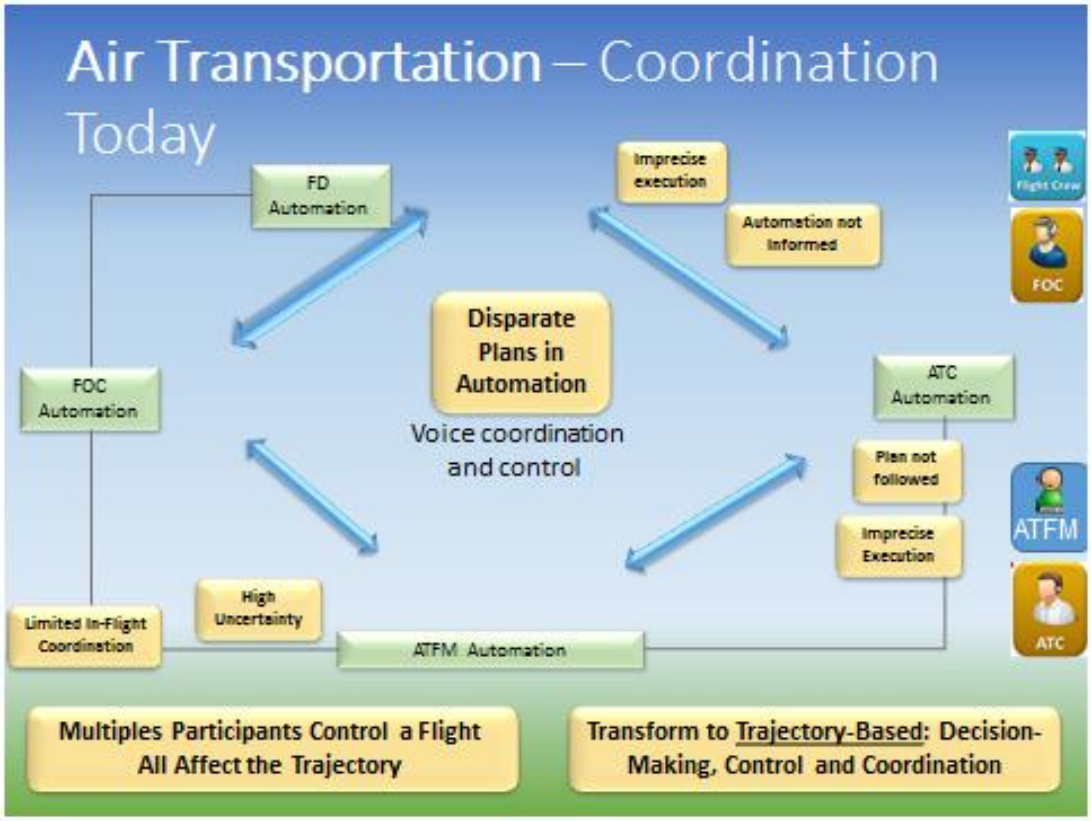

Рисунок1.3 – Схематичне зображення координації зв’язку між службами ОПР

В статті пояснюється, що зв’язок між службами управління повітряним рухом та командою ПС часто здійснюється за допомогою голосового каналу зв’язку і деякі інструкції не розпізнається автоматизованою системою, а отже не можуть бути використана при плануванні або навіть при оперативній оптимізації польоту.

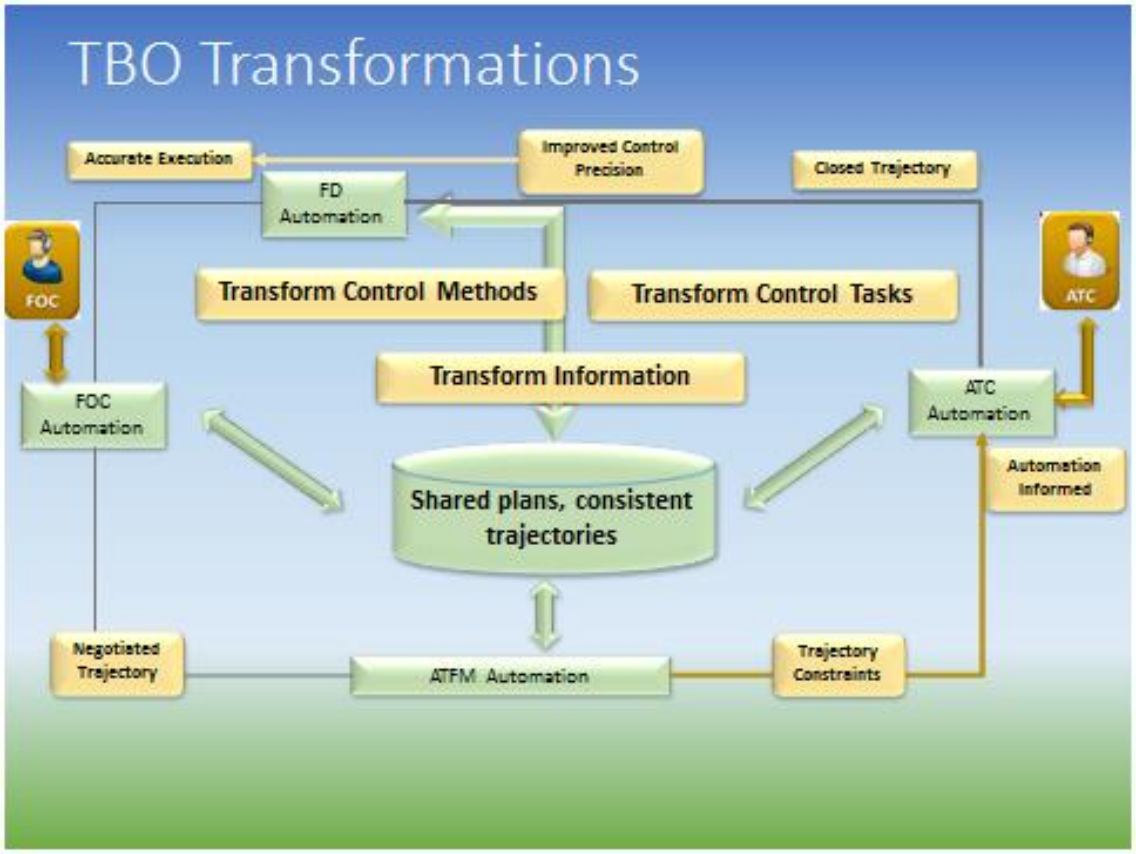

Рисунок 1.4 – Схематичне зображення координації зв’язку між службами УПР в рамках концепції операцій заснованих на траєкторії

Крім того, хоча всі мають пріоритети в окремій частині повітряного простору , їхні загальні перспективи та пріоритети не є однаковими. Я к наслідок – зниження гнучкості в роботі системи. Отже перехід до концепції операцій заснованих на траєкторії дозволить втілювати операції де прийняття, контроль та координація рішень базуються на однакових знаннях, одній і тій же інформації про траєкторію польоту.

З аналізу умов та вимог щодо втілення зазначеної концепції можна сказати, що є необхідність в автоматизації систем, що передають, оброблюють та відображають інформацію, та використання перспективних механізмів управління інформацією, наприклад SWIM. Як наслідок вразливість до кібер ризиків зростає, що потребує аналізу та оцінювання ризиків для удосконалення системи управління безпекою.

1.6. Системи автоматичного залежного спостереження (Atomatic Dependent Surveillance - ADS

З аналізу сучасних концепцій та програм ІКАО та EUROCONTROL можна побачити, що є необхідним розвиток та впровадження систем автоматичного залежного спостереження (наприклад, Atomatic Dependent Surveillance - ADS) в яких, на відміну від незалежних систем спостереження, місцезнаходження ПС визначається навігаційною системою літака з використанням GPS технологій, а надалі передається органу УПР. Концепція ADS базується на передачі даних за допомогою ліній «повітря-земля», по яких інформація автоматично передається на землю відповідному повноважному органу УПР. Зміст інформації, частота передачі даних та інші параметри визначаються на основі контракту, що встановлюється між наземним і бортовим обладнанням.

Необхідною умовою використання інформації за допомогою ADS є оснащення ПС відповідним обладнанням для експлуатації в умовах надання обслуговування ADS. Відповідні дані ADS представляються диспетчерові у формі, прийнятній для виконання функцій керування.

За допомогою системи ADS-B можна передавати дані не тільки диспетчеру, а і екіпажам ПС, а також забезпечити можливість запиту та одержання поточної цільової інформації в найбільш цікавій зоні для пілотів або авіаційних диспетчерів.

Тенденція розвитку сучасних систем обміну та передавання інформації передбачає наступні принципи:

- інформація, що поширюється, має бути захищеною та розповсюджуватися системно, отже зберігатися вимога щодо цілісності даних;

- інформація, що потрібна користувачу, має бути доступною в будь-який час та в будь-якому місц, отже зберігатися вимога щодо доступності даних і;

- інформація має бути персоналізованою, відфільтрованою та доступною за запитом, отже зберігатися вимога щодо конфіденційності даних;

- система має дотримуватись можливості захищеної взаємодії мереж.

Отже, тенденція розвитку сучасних систем обміну та передавання інформації передбачає підвищення ефективності систем передавання, тобто можливість збільшення інформаційного потоку та його надійність, безпеку тощо. Одночасне втілення сучасних концепцій потребує розвитку систем обміну інформацією нового покоління, що здатні знаходити інформацію за конкретним запитом в залежності від обставин, а не оперувати великою кількістю даних для простого попереднього ознайомлення. Таким чином необхідно створювати можливість взаємодії мереж, що дозволить системі справлятися з усіма складнощами оперативного обміну інформацією.

Висновки до розділу 1

1. Загальний процес забезпечення користувачів повітряного простору послугами системи управління повітряним рухом регламентується документами ІКАО (Doc 9854 Global Air Traffic Management Operational Concept, Глобальний аеронавігаційний план (Doc 9750) зазначають ті фактори, які потрібні для збільшені пропускної спроможності та підвищення ефективності роботи майбутньої системи управління повітряним рухом, а саме - підвищення гнучкості в інформаційному забезпеченні та збільшення робочої ефективності системи.
2. Перспективні технології забезпечення втілення сучасних концепцій та програм, такі як ADS-B не має достатніх заходів безпеки. Система ADS-B є вразливою до кібератакам, наприклад відсутність засобів безпеки ADS-B дозволяє вводити неправдиві дані польоту, а також перешкоджати бездротовому зв'язку між літаками та диспетчерською вежею, а також запобігати виявленню комерційних літаків наземними станціями ADS-B та контрольними вежами або іншими літаками.
3. Необхідно дослідити потенційні відомі загрози та ризикі сучасним та перспективним системам зберігання, обробки та поширення інформації та оцінити потенційні загрози кібербезпеці для ОПР та контролю повітряного руху.
4. Інфраструктура для обміну інформацією націлена на інформацію,як основний актив, який має бути захищеним для забезпечення надійного обміну даними між зацікавленими сторонами ОПР.
5. Обмін даними - ключова особливість майбутньої системи ОПР. Кібербезпека в ОПР стає все більш пріоритетним завданням.
6. Таким чином, можна сказати, що сучасні та перспектині підходи до збільшення пропускної спроможності та ефективності існуючої системи повітряного руху вимагають переходу до цифровізації та

автоматизації. Як результат, раніше відокремлені ІТ-системи підключаються до єдиної мережі для обміну інформацією та даними, що в свою чергу збільшується складність системи та створюються раніше невідомі взаємозалежності. Отже, обмеження управління ризиками безпеки до “традиційних” фізичних аспектів вже недостатнє для забезпечення стабільної та надійної роботи системи повітряного транспорту. Необхідно також враховувати складову кібербезпеки та розширювати її значення для розробки більш стійких та цілеспрямованих підходів щодо забезпечення безпеки авіації.

7. Ідентифікація та оцінка загроз і вразливостей систем та цілої інфраструктури є найважливішим завданням для підвищення безпеки як сучасної, так і майбутньої системи ОПР.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ ТЕХНОЛОГІЇ УПРАВЛІННЯ РИЗИКАМИ ТА ОЦІНЮВАННЯ РИЗИКІВ ПРИ ОПР

2.1. Загальні принципи управління інформаційними ризиками

Управління ризиками - є одною з складових процесу управління безпекою. Управління ризиками - це процес виявлення, аналізу, оцінки та можливого попередження ризиків, або ліквідації наслідків у випадку, якщо загроза ризику здійснилася. Процес управління ризиками є ширшим, ніж забезпечення інформаційної безпеки. Цей процес охоплює всі ризики, які можуть зупинити роботу системи включно авіаціну транспортну систему і унеможливити досягнення своїх цілей.

Мета неперервного процесу управління ризиками – визначити характеристики ризиків по відношенню до інформаційної системи та її ресурсів та обрати необхідні захисні засоби.

В даному випадку під інформаційною безпекою мається стан стан захищенності інформаційного середовища суспільства, який забезпечує його формування, використання й розвиток в інтересах громадян, організацій, держави. Таке визначення надається і в «Законі про інформацію».

Ризик прийнято визначати як поєднання ймовірності та наслідків настання несприятливих подій.

Загрозу відповідно до [16] можна визначити як стан, об’єкт або діяльність що є потенційною причиною пошкодження людей (персоналу), майна, обладнання, конструкцій, матеріальних збитки, зменшення ефективності тощо.

Взагалі загрози інформації криються в псуванні цілісності, конфіденційності, повноти та доступності інформації [16].Можна виділити наступні цілі загроз:

- Ознайомлення з інформацією, що захищається
- Модифікація інформації для задоволення корисливих цілей

- Руйнування для заподіяння матеріальної або моральної шкоди.

Можна сказати, що інформаційна безпека спрямована на створення стану вільного від загроз, як показано на Рис.2.1

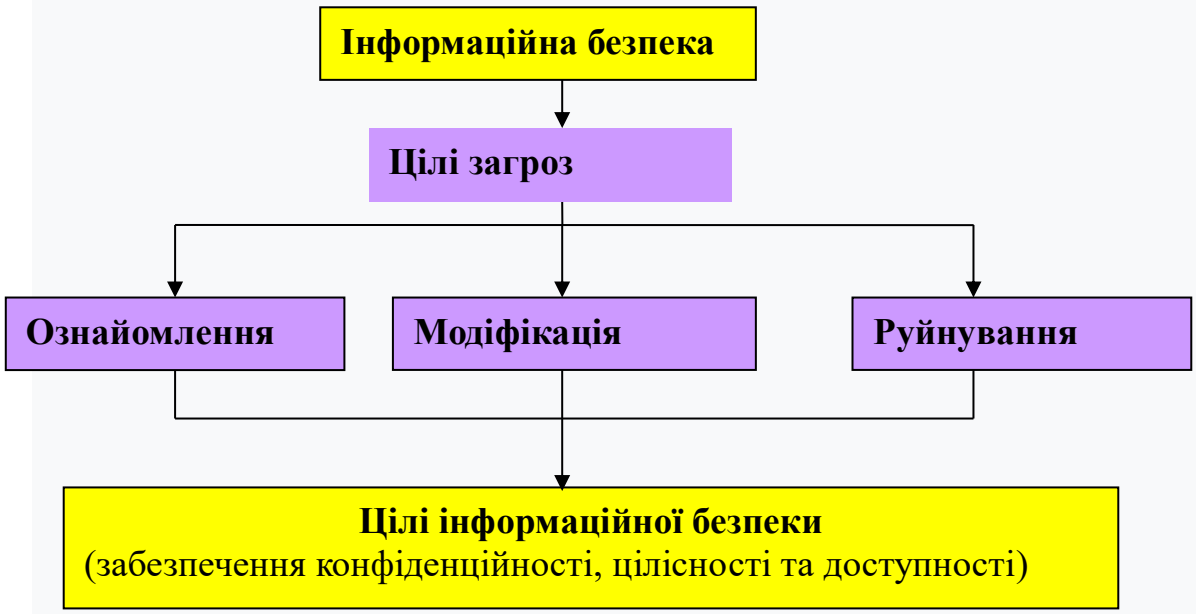

Рисунок 2.1 – Ціллі і завдання інформаційної безпеки

У галузі інформаційної безпеки ризик прийнято використовувати для вимірювання ймовірності реалізації шкідливого фактору, або дії, що впливає на роботу організації. Також прийнято оцінювати рівень впливу, або наслідків такої події. Вважається, що така шкідлива подія реалізується, коли зловмисник використовує вразливості системи. Вразливість можна визначити, як характеристики об’єкту, що можуть використовуватися для реалізації незаконного втручання.

В свою чергу вразливості впливають на зарактеристики подальших захисних дій. А залежно ві важливості, чи цінності обїєкту на який спрямована загроза сам факт реалізації ризику смає вплив на організацію чи галузь в цілому.

Отже в процесі управління ризиками прийнято враховувати наступні фактори:

• Цінність ресурсів,

• Оцінка значимості загроз

• Оцінка значимості вразливостей

• Ефективність засобів захисту

Відповідн до ціності ресурсів необхідно визначити також і рівень відповідно до якомго буде проводитися управління ризиками. Розрізняют

- Базовий рівень – на цьому рівні аналіз ризиків, що проводиться у відповідності з вимогами базового рівня захищеності. Використовується у випадках, коли інформаційна до системи немає підвищених вимог щодо інформаційної безпеки. Базовий рівень безпеки – ЦЕ обов'язковий мінімальний рівень захищеності для інформаційних систем. Критерій досягнення базового рівня безпеки це, як правило, виконання заданого набору вимог.

- Повний рівень – на цьому рівні аналіз ризиків для інформаційних систем до яких є підвищенні вимоги в галузі інформаційної безпеки. Обов’язково вміщує визначення цінності інформаційних ресурсів, оцінку загроз та вразливостей, вибір адекватних контрзаходів, оцінку їх ефективності.

Управляння ризиками авіаційної транспортної системи, звичайно необхідно проводити на повному рівню.

В загальному вигляді процес управління ризиками в інформаційних системах пожна представити за допомогою Рис. 2.2 на якому показані основні процедури та етапи аналізу.

В процесі управління ризиками збиткі, що очикуються у вападку реалізації загроз порівнюються з витратами на заходи безпеки.

Рисунок 2.2 – Приклад процесу управління ризиками в інформаційних системах

Надалі приймається рішення щодо ризику що оцінюється, який може бути

• Знижений, за рахунок використання заходам захисту

• Усунений, за рахунок відмови від використання ресурсу, що схильний до загрози

• Перенесений (наприклад, за рахунок страхування)

• Прийнятний

Системи, співробітники та процеси в будь-якій організації завжди змінюються. Отже, часом можуть з’являтися нові загрози та уразливості. Це обумовлює необхідність ітераційного підходу до процесу управління ризиками. Такий процес прийнято ділити на наступні етапи:

- Ідентифікація обєкту, що має захищатися, загроз та вразливостей
- аналіз ризиків,
- оцінювання ризиків

- вплив на ризикі,
- прийняття ризику,
- реєстрація, інформування про ризик, консультації та прийняття рішення ,
- моніторинг ризиків.

Загальний процес управління ризиками можна подати за допомогою блок-схеми, що зображена на Рис. 2.3.

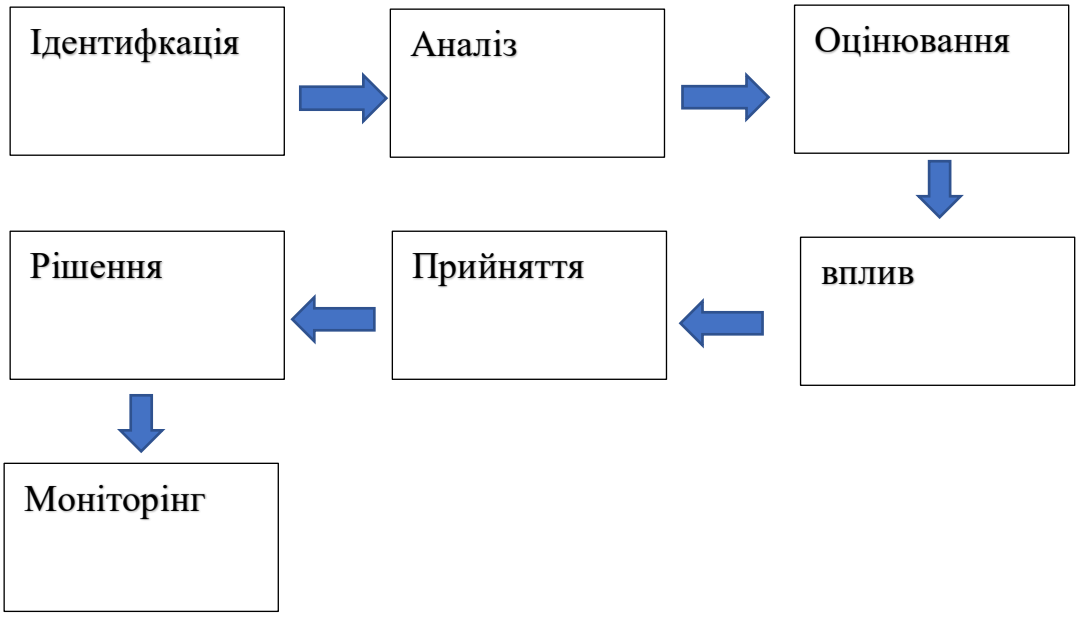

Рисунок 2.3 – Етапи процесу управління ризиками

На першом етапі, етапі ідентифікації, необхідно провести ідентифікацію та опис елементів ризику: об’єктів захисту, загроз, вразливостейю Тобто встановлюється контекст процесу оцінки ризику визначаються потенційні загрози та уразливості, які існують.

Прикладами об’єктів захисту можуть бути: інформаційні активи, програмне забезпечення, фізичні активи, сервіси, людські ресурси, нематеріальні ресурси – репутація та імідж організації.

Дані для процесу ідентифікації можна отримати

- з результатів аудиту,

- даних про події та інциденти,

- як експертне оцінювання користувачами, спеціалістами з інформаційної безпеки, IT спеціалістів, зовнішніх консультантів тощо.

На етапі Аналізу ризиків визначається вартість інформаційних активів. Проводять оцінку можливих збитків та наслідків у випадру реалізації того чи іншого ризику. Обирають шкалу оцінювання ризику. Оцінюють реалізацію загроз тощо.

На етапі оцінювання ризики визначаються, вимірюються та визначаються за пріоритетами. Ризики можуть бути кількісно визначені або якісно описані. Кількісні та якісні показники, які прийнято використовувати в авіації описано в розділі 2.2. цієї роботи. Далі визначаються вже існуючі засоби контролю та їх вплив на потенційні наслідки ризику. Завершується етап визначанням їх пріоритетів відповідно до кількісного або якісного показника.

На наступному кроці, що ми назвали етапом впливу на ризики, здійснюються необхідні заходи для запобігання, зменшення, абу усунення можливих наслідків ризику та застосування організаційних або технічних заходів щодо зменшення, корегування або, навіть, попередження ризиків. Наприклад, усунути джерело ризику, або розділити ризики зі страховою кампанією, або прийняти. Все це вже залежить від оціночного значення самого ризику.

На етапі прийняття ризику служить проводять збір всіх визначених ризиків для визнання визнаються керівниками організації та відповідними службами.

На етапі комунікації, тобто реєстрації, інформування про ризик, консультації та прийняття рішення проводиться повідомлення про існуючий ризик та втілюються заходи з управління корегуючих мір. Проводиться інформування про заходи, які вирішено втілити, контроль за діями керівників

та іншого персоналу. Ціллю даного етапу є запобігання порушень безпеки під час управління заходів по зменшенню чи усуненню ризиків.

Останній етап управління ризиками – моніторинг- призначений для відстежування та перегляду виявленних ризиків. Це потрібно для забезпечення постійно оновлювання процесу управління ризиками та впровадженню відповідних корегуючих заходів.

З дослідження загального процесу управління ризиками можна зробити висновок, що це доволі складний процес, що складається з декількох етапівю Одним ьз найважливіших етапів та складним завданням цього процесу є кількісна (іноді, навіть, якісна) оцінка виявленого ризику.

2.2. Дослідження загальних принципів оцінки ризиків

Як можна побочити з висновків підрозділу 2.1 ,оцінка ризиків є найскладнішим завданням в процесі управління ризиками.

Оцінка ризику передбачає ідентифікацію ризиків, їх аналіз та саме оцінку.

Ідентифікація ризику визначає, як, де і чому може статися потенційна загрозлива дія.

Ідентифікація ризику вимагає спочатку ідентифікації усіх потенційних обєктів що можуть бути в зоні дії ризику.

Для цього визначаються загрози, які можуть завдати шкоди раніше ідентифікованим обєктам потенційного захисту.

Відповідно до властивостей інформації, виділяють наступні загрози її безпеці:

- *загрози цілісності інформації, або інформаційній системі*. Цілісність може бути пошкоджена через знищення або модифікацію інформації чи носія інформації.

- *загрози доступності*ю Як правило така загрози реалізується за допомогою блокування, або взаглі, знищенням інформації чи носія.

– *загрози конфіденційності*. Така загроза реалізується за рахунок:

а) несанкціонованого доступу до інформації, що захищається за допомогою якого зловмисник може ознайомитися з інформацєї, що захищається;

б) витоку інформації, я праило, за допомогою технічних каналів зв'язку;

в) розголошення, часто ненавмисного.

В документі [17] наведено наступні визначення:

Ознайомлення (disclosure) — одержання користувачем або процесом інформації, що міститься в об'єкті різними способами без руйнування її цілісності.

Модифікація - Повна, або часткова зміна користувачем або процесом інформації (її структури або контенту), що міститься в об'єкті.

Знищення — видалення конфіденційної інформації таким чином, щоб дані не могли бути відновлені ніяким відомим способом.

При аналізі загроз її доцільно класифікувати за наступними показниками [18,19].:

За джерелами пходження

- природного походження;
- техногенного;
- антропогенного походження.

В інших джерелах професійної літератури з нформаційної безпеки джерела така За джерелами пходження виділяють наступні загрози:

- Природні
- Навмисні.

За характером шкоди загрози розділяють на

- Матеріальні
- Моральнію

В деяких джерелах класифкація за цією ознакою наведена наступним чином – за ступенем гіпотетичної шкоди. В такому випадку розділяють саме

- загрозу, яку визначають, як реальні чи потенційно можливі дії, які ускладнюють або унеможливлюють реалізацію відповідних інтересів у інформаційній сфері і створюють небезпеку, в нашому випадку, для системи управління безпекою авіації, життєзабезпечення її системостворюючих елементів та

- небезпеку, що визначають, як безпосередню дестабілізацію функціонування системи управління інформаційною системою , або системою управління безпекою.

За по вторюванністю вчинення розрізняют:

- повторювані загрози, це такі, які мали місце раніше;

- продовжувані загрози - це неодноразове здійснення загроз, що складається з ряду тотожних загроз, які мають спільну мету.

За сферами походження розрізняют:

- екзогенні , у аипадку, коли джерело дестабілізації системи лежить поза її межами;

- ендогенні, у випадку, коли алгоритм дестабілізації системи перебуває у самій системі.

За схожим принципом загрози поділяють За такою ознакою, як взаємодія з об’єктом на:

- Внутрішні

- Зовнішні.

За ймовірністю реалізації загрози поділяють на:

- вірогідні, це загрози, які за виконання певного комплексу умов обов'язково настануть.

- неможливі , це ті загрози, які за виконання певного комплексу умов ніколи не настануть.

- випадкові —загрози, які за виконання певного комплексу умов кожного разу протікають по-різному.

За характером реалізації:

- реальні;

- потенційні;

- здійснені;

- уявні.

За рінем детермінізму:

- закономірні загрози. Мають стійкий, повторюваний характер та зумовлені об'єктивними умовами існування та розвитку системи інформаційної безпеки;

- випадкові загрози. Можуть або трапитися або не трапитися.

За значенням:

- допустимі, що не можуть призвести до колапсу системи.

- неприпустимі, які можуть у разі їх реалізації призвести до колапсу і системної дестабілізації системи або можуть призвести до змін, що не є сумісними з подальшим існуванням системи.

За структурою впливу:

- системні - впливають на усі складові елементи системи управління безпекою;

- структурні - впливають на окремі структури системи;

- елементні - впливають на окремі елементи структури системи.

За ставленням до загроз їх поділяють на

- об'єктивнію Такі загрози підтверджуються сукупністю обставин і фактів, що об'єктивно характеризують навколишнє середовище.

- суб'єктивні. Це сукупність чинників об'єктивної дійсності, яка вважається суб'єктом управління системою безпеки загрозою. За даного випадку визначальну роль у ідентифікації тих чи інших обставин і чинників відіграє воля суб'єкта управління, який і приймає безпосереднє рішення про надання статусу або ідентифікації тих чи інших подій в якості загроз безпеці.

За об’єктом впливу загрози можна поділити на рівні

- особи;

- суспільстви;

- держави і, навіть, світу.

За характером впливу загрози поділяють на активні та пасивні.

Необхідно також визначати можливі вразливості, які можуть бути властиві елементам системи та бути використаними для реалізації загроз. Інформація про вразливості, в свою чергу, є корисною у процесі реалізації контрольних заходів щодо їх уникнути в процесі експлуатації.

В подальшому визначаються наслідки, які можуть бути спричинені реалізацією виявлених загроз. При аналізі ризиків надаються якісні та кількісний показники ризиків, що впливають на обєкти, які мають захищатися. Зазвичай ці показники включають вимірювання ймовірності події, що відбулася та вплив цієї події.

При оцінюванні ймовірності, приймаються до уваги можливі навички та мотивація зловмисника, а також труднощі у використання вразливості системи. Наприклад, ймовірність реалізації загрози некваліфікованим зловмисником вразливості спеціального програмного забезпечення для авіаційних потреб, як правило, є низько. Однак зловмисники, що спеціально підготовлені для реалізації можливої загрози мають вже інші резерви для реалізації загрози, а отже і ймовірність більшується.

При оцінюванні впливу, розглядаються можливі збиткі, що очикуються у випадку реалізації загроз. Збитки порівнюються з витратами на заходи безпеки. З цього і приймається рішення про майбутні заходи та обгрунтовується їх ефективність.

Наприклад втрата доступу до системи оперативної інформаційної підтримки користувачів повітряного руху має великий вплив на роботу авіаційної транспортної системи. Однак втрата доступу до інших менш чутливих активів, таких як маркетингові дані про індувідуальні харчові замовлення пасажирів бізнес-класу матиме менший вплив на роботу авіаційної транспортної системи в цілому.

При оцінюванні ймовірності та впливу реалізації загрози, можна оцінити рівень ризику, який породжує така реалізація.

Як вже зазаначалося, зазвичай, оцінка ризику поєднує в собі ймовірність події та її наслідків. Якщо обидва визначаються за допомогою кількісних показників, то в такому випадку, ризик, як правило, є результатом множення. Якщо обидва визначаються за допомогою якісних показників, ризик, як правило, вимірюється використовуючи таблицю з корекцією ризику [18].

Отже оцінка ризику передбачає аналіз його ймовірності та вплив загроз для забезпечення єдиного бачення рівня ризику, що впливає на роботу організації, а в нашому випадку на роботу авіаційної транспортної системи.

Після оцінювання ризиків ризик визначають як його краще описати: кількісно або якісно. Результати оцінки ризику використовуються для вирішення наступного питання, чи мають бути прийняти заходи щодо зниження ризику чи його можливого усунення та надаються пріоритети впровадження управління заходами щодо зменшення ризиків.

2.2.1 Кількісне оцінювання ризику

В загальному процесі оцінювання ризиків рекомендовано використовувати нормативну базу ISO 27002 [20] та оцінити наступні складові:

- Актив – це все, що має цінність для організації, її ділових операцій та її безперервності.
- Загроза - це потенційна причина інциденту, який може завдати шкоди системі чи організації.
- Вразливість - це слабкість активу або групи активів, які можуть бути використані однією або кількома загрозами.
- Ризик - це ймовірність того, що дана загроза використає вразливі місця активу або груп активів і тим самим завдасть шкоди організації.
- Вплив - це результат інциденту з інформаційною безпекою, спричинений загрозою, яка впливає на активи.

Приймається , що будь-яка потенційна чи реально існуюча загроза З має відповідну ймовірність її реалізації $Рз$. Для кожної загрози існує ймовірність використання існуючої вразливості $Р_В$. Ці фактори описують ймовірніть того, що загроза буде реалізована $Rз$:

$$Rз = Рз \cdot Р_В \quad (2.1)$$

Позначимо очикуваний вплив від можливої реалізації ризику як Нз. Реалізація загрози може вплинути на всю систему в цілому чи тільки на окрему складову загальної системию Це, в свою чергу, повязано з попередньою оцінкою цінності активів. Якщо припустити, що загальна вартість активу буде втрачена у випадку, коли загроза реалізується, то можна поєднати ймовірність та вплив для отримання кількісного показника ризику наступним чином:

$$R = R_З \cdot Нз = Рз \cdot Р_В \cdot Нз \quad (2.2)$$

Загроза у більшості випадків має зовнішню природу, отже ймовірність виникнення загрози не може бути змінена. Вразливості, на відміну від загрози, в більшості мають внутрішню природу, а це означає, що і ймовірність задіяння вразливості може бути зменшена і доцільно розглядати можливе інвестування їх зменшення при розробці системи захисту інформаційної системи. Іноді приймається рішення про ліквідацію наслідків реалізації можливої загрози, тобто інвестують у заходи з усунення чи зменшення наслідків ризику.

2.2.2. Якісна оцінка ризиків

Для якісної оцінки ризиків використовують так звану "матриця ризиків". Матриця відображає ймовірність матеріалізації загрози проти очікуваного впливу на систему, пов'язаного з конкретною загрозою. Простий рейтинг ризику також може бути використаний для класифікації

результуючого ризику, наприклад, якщо присвоїти кожному з оцінюванного фактору рейтинг від 0 до 8 отримаємо наступну класифікацію:

Низький ризик: від 0 до 2,

Середній ризик: від 3 до 5,

Високий ризик: від 6 до 8.

На рис. 2.4. показано приклад Матриці ризику на базі рекомендацій BS ISO/IEC 27005:2011 [21].

		Ймовірність				
Очікуваний вплив		рідка	низька	можлива	дуже ймовірна	безсумнівна
	Катастрофічний	4	5	6	7	8
	значний	3	4	5	6	7
	Помірний	2	3	4	5	6
	невеликий	1	2	3	4	4
	Незначний	0	1	2	3	3

Рисунок 2.4 – Приклад матриці ризиків

Тобто, відповідно до тблиці, подія, що має рейтинг від 0 до 2 потрапляє до зеленої зони. Подія, що має рейтинг від 3до 5 потрапляє до жовтої зони і подія, що має рейтинг від 6-8 до 2 потрапляє до червоної зони.

Прийнято, що подія, яка опинилася в так званій «зеленій» зоні не несе значного впливу і має низьку ймовірність реалізації і можлива подальша експлуатація системи з прийнятним рівнем ризику. Подія, що опинилася в червоній, навпаки часто не сумісна с подальшою експлуатацією системи. Необхідно або припинити експлуатація, або вжити невідкладних заходів із зменшення рейтингу ризику. Події, що знаходяться в жовтій зоні, це події в так званій «керованій зоні». Тобто можлива експлуатація системи враховуючи інформацію про можливі заходи, а також з впровадженням інструментів щодо зменшення впливу загроз чи усунення вразливостей. Також існує завдання не допустити перехід системи в потенційно небезпечну (червону) зону і забезпечити блокування (виключення) відповідного технічного об'єкта з вразливістю в разі загрози переходу або при переході в небезпечну зону, а також мінімізація наслідків такого переходу.

2.3. Дослідження принципів управління інформаційними ризиками в авіаційній діяльності

Управління безпекою в авіаційній галузі регламентується документами [22,23].

Відповідно до вимог стандартів ІКАО, авіаційними організаціями впроваджуються прийнятні системи управління безпекою польотів, які як мінімум [23].:

а) виявляють фактори, небезпечні для безпеки польотів (небезпечні фактори);

б) забезпечують вжиття коригуючих заходів, необхідних для витримування характеристик безпеки польотів;

в) передбачають здійснення постійного контролю і регулярної оцінки характеристик БП;

г) направлені на постійне покращення загальних показників роботи системи управління безпекою польотів.

Як видно з цих загальних принципів системи управління безпекою польотів, в авіаційній діяльності дотримуються загального підходу щодо управління безпекою та дотримуються загальних етапів управління безпекою.

В контексті управління безпекою ІКАО визначає Безпеку польотів в системі управління безпекою польотів (Safety for SMS) як стан, при якому імовірність нанесення шкоди людям чи майну знижена до прийнятного рівня та підтримується на цьому або більш низькому рівні шляхом постійного процесу виявлення небезпечних факторів та управління факторами ризику для безпеки польотів.

Забезпечення дієвої і ефективної СУБП авіаційної організації рекомендується розпочинати з прийняття політики в сфері безпеки польотів. Це є правовою складовою системи захисту, а в контексті презентованої роботи в контексті захисту інформації для УПР та безпеки польотів.

Відповідно до [23] СУБП будь-якої авіаційної організації може складатися з наступних компонентів. які показан ра Рис. 2.5.

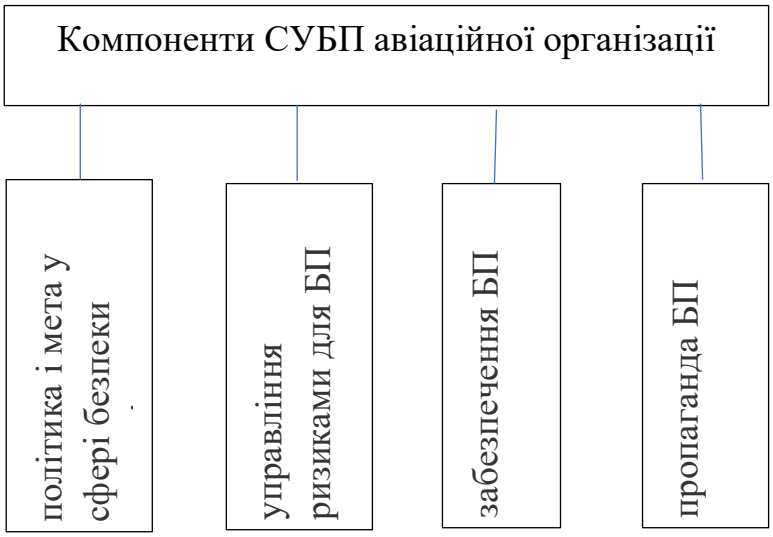

Рисунок 2.5 – Компоненти СУБП

Компоненти СУБП (Рис.2.5) рекомендовані для формування базової структури СУБП.

В свою чергу до компонентів "управління ризиками для БП" можуть бути включені наступні елементи:

а) виявлення небезпечних факторів;

б) оцінка і зниження ризику для БП;

А до компонентів "забезпечення БП" можуть бути включені наступні елементи:

а) контроль і оцінка характеристик безпеки;

б) регулювання змін;

в) постійне удосконалення СУБП;

Отже, як можна побачити, складові СУБП відповідно до рекомендацій ІКАО відповідають загальному процесу управління ризиками, а також тієї частині, що відповідає саме оцінюванні ризиків.

Зазначається, що виявлення небезпечних факторів та управління ризиками для БП є, як правило, основними процесами управління безпекою польотів.

До небезпечні факторів, які можуть бути частиною будь-якої виробничої системи, та на які потрібно звертати увагу при виявленні небезпечних факторів, зокрема відносять:

- фактори проектування, у тому числі використовувані технічні засоби та об'єкт проектування;

- правила та експлуатаційні процедури, у т. ч. документація, чек-листи, а також їх використання в реальних виробничих умовах;

- мовний зв'язок, у т. ч. технічні засоби, термінологія та мова;

- фактори персоналу, зокрема політика організації з питань прийняття на роботу, підготовки персоналу, оплати праці та виділення відповідних ресурсів;

- фактори регуляторного нагляду, зокрема застосування та забезпечення виконання авіаційних правил; сертифікація обладнання, персоналу та діяльності; відповідність нагляду;

- засоби захисту (defences), зокрема забезпечення адекватних систем реєстрації та попередження; стійкість обладнання до помилок та відмовю

З переліку видно, що перелічені в даній роботі фактори тісно повязані з інформаційними ризиками, а отже доводять доцільність оцінювання інформаційниз ризиків для УПР та безпеки польотів.

Зазначається, що виявлення небезпечних факторів є постійним, безперервним та повсякденним процесом. Він ніколи не припиняється та не призупиняється. Виявлення небезпечних факторів може бути частиною організаційних процесів, що направлені на надання послуг, що становлять бізнес авіаційної організації. А отже відповідає вимоги системи захисту бути ітераційною.

Під час оцінки небезпечних факторів рекомендується враховувати всі можливості їх виникнення від малоймовірних до дуже імовірних (неминучих). Оцінка небезпечних факторів, як правило, передбачає виникнення найгірших умов. Важливо, щоб небезпечні фактори, які оцінюються, були "імовірними" небезпечними факторами. Дуже важливо встановити межу між імовірно найгіршими умовами та такими умовами, які настільки залежать від збігу обставин, що їх не потрібно брати до уваги.

При прийнятті рішень щодо врахування небезпечних факторів рекомендується використовувати наступні визначення:

а) Найгірші наслідки. Найбільш несприятливі очікувані умови, наприклад: надзвичайно висока інтенсивність повітряного руху під час порушення виробничої діяльності внаслідок екстремальних погодних руйнувань;

б) Імовірний випадок. Існують підстави вважати, що під час виробничої діяльності виникне передбачуване поєднання екстремальних умов.

Всі виявлені небезпечні фактори рекомендуємо позначати номером та реєструвати в журналі обліку небезпечних факторів. Журнал обліку небезпечних факторів може містити опис кожного небезпечного фактора, його наслідків, оцінку імовірності та серйозності ризику для БП. Крім того в

журналі бажано вказувати необхідні засоби контролю ризику та заходи по його зниженню (у разі потреби).

Отже з аналізу документів [22,23] можна зробити висновок про можливість якісного підходу до оцінювання ризиків для забезпечення безпечної роботи авіаційної транспортної системи.

Після виявленянебезпечних факторів, пропонується оцінити ризик потенційних наслідків, до яких може призвести небезпечний фактор. Під час аналізу рекомендовано ризик оцінювати за двома критеріями: імовірність настання події чи умов, які наносять шкоду, та серйозність наслідків події чи умови, якщо вони настануть.

Процес прийняття рішення стосовно ризику та його прийнятності може здійснюватися за допомогою застосування матриці прийнятності ризику. Незважаючи на те, що матриця є необхідною для оцінки ризику, її використання, як правило, здійснюється помірковано. Формування і остаточна структура матриці, як правило, здійснюється авіаційною організацією.

Отже рекомендовано також вживати загально прийняті інструменти для оцінювання ризиків.

Після оцінки ризику, рекомендовано вжити заходів стосовно його усунення чи зниження до найменшого прийнятного рівня.

Рекомендовано авіаційним організаціям при потребі розробляти і реалізовувати засоби контролю ризиків, зокрема розробляти процедури, нові методи управління, вносити зміни в порядок підготовки персоналу, впроваджувати додаткове чи модифікувати обладнання, інші альтернативні засоби усунення/зниження ризиків.

Документи [22,23] також надають поняття Управління ризиками. Визначення, що приводять в документах, наступне: процес, який охоплює процедури оцінки і зниження ризику для БП, що пов'язані з наслідками небезпечних факторів, називається управління ризиками для БП

Згадується, що процес управління ризиками, як правило, є ключовим етапом процесу управління безпекою польотів в авіаційній організації.

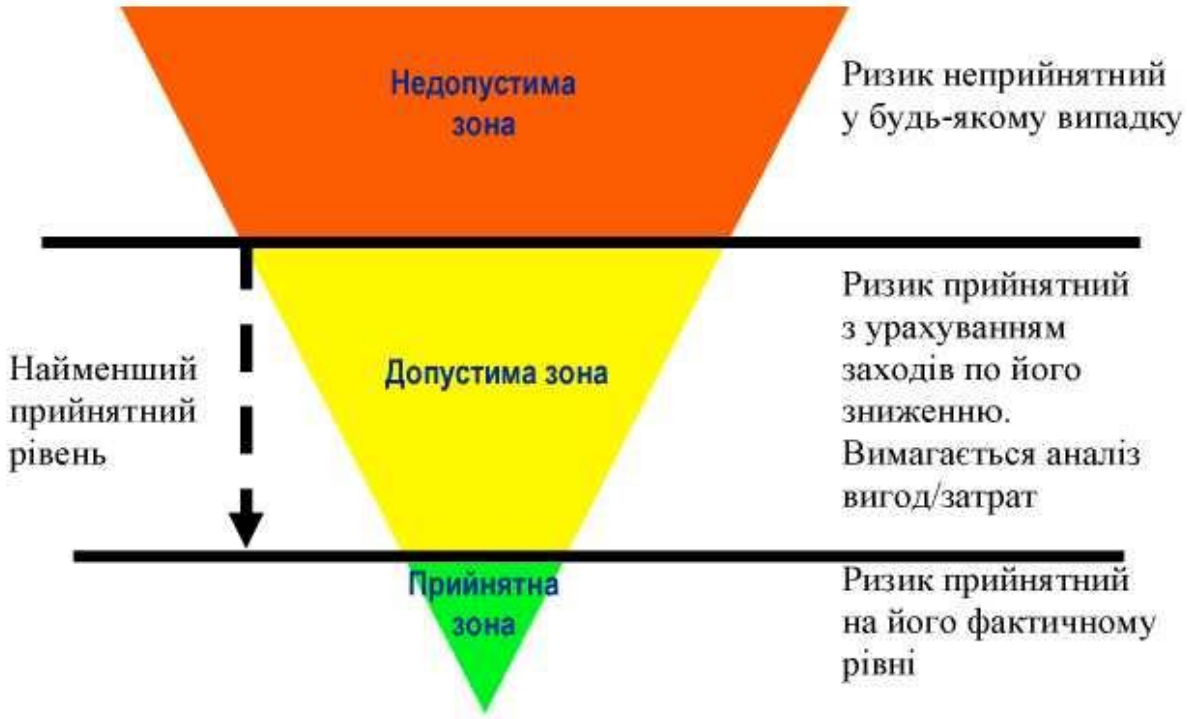

Рис. 2.6. Приклад процесу управління ризиками з [23].

В документах вказується критерій контролю ризиків. Якщо ризики, які за результатами оцінки потрапляють до недопустимої зони (червоної зони), вони є неприйнятними за будь-яких обставин. Імовірність чи серйозність наслідків небезпечних факторів потребує вжиття термінових заходів для зменшення небезпеки.

Ризики, які за результатами оцінки потрапляють в допустиму зону (позначено жовтим кольором), є прийнятними за умови, що вжиті заходи по їх зниженню гарантують, що прогнозована імовірність та серйозність наслідків небезпечного фактора перебуває під контролем організації.

В авіаційній галузі, як і в загальному випадку рекомендовано аналізувати та оцінювати вигоди/затрати для виправдовування затрачених

ресурсів для забезпечення зниження, усунення небезпечних факторів або контролю наслідків після вживаних методів

Ризики, які за результатами оцінки потрапляють в прийнятну зону (позначено зеленим кольором), рекомендують прийняти на їх фактичному рівні без вживання додаткових заходів по зменшенню чи контролю за ними.

В процессі оцінювання ймовірності ризику рекомендується з урахуванням за наступних питань [22,23]:

а) чи відбувалися раніше події, аналогічні до тієї, що розглядається, чи це одиничний випадок;

б) які інші ПС, обладнання чи компоненти такого ж типу мали подібні відмови (дефекти);

в) кількість працівників, що виконують дані процедури, чи на яких вони поширюються;

г) протягом якої частини (тривалості) виробничого часу використовується техніка, процедура чи обладнання, що оцінюється;

ґ) на скільки суттєво впливає організаційний, адміністративний чи регламентуючий процес на виникнення потенційної небезпеки.

Нижче наведено таблицю з рекомендованими значеннями щодо ймовірності виникнення загрози.

Таблиця 1 Рекомендовані значення ймовірності виникнення загрози.

Ймовірність винекнення загрози	Значення	Величина
Часто (від 1 до 10^{-3} за годину)	Трапляється часто	5
Періодично (від 10^{-3} до 10-5 за годину)	Трапляється інколи	4
Рідко (від 10^{-5} до 10^{-7} за годину)	Мала	3
Малоймовірно	Дуже мала	2

(від 10^{-7} до 10-9 за годину)		
Майже неможливо (< 10^{-9} за годину)	Неможлива	1

Інформацію для оцінбвання ймовірності рекомендується брати з бази данних з безпеки польотів, а у випадку відсутності такої бази – з урахуванням тенденцій в авіації.

Наступним кроком рекомендовано виконувати оцінку серйозності наслідків можливої реалізації ризику. Таку оцінку рекомендовано виконувати за критеріями, що наведені в таблиці 2.

Таблиця 2 Рекомендовані значення серйозності наслідків загрози

серйозність	Значення	Рівень
Катастрофічна	- значні людські жертви - зничення майна та/або обладнання	A
Небезпечна	- серйозні тілесні ушкодження; - значне пошкодження обладнання, майна - серйозне зменшення рівня безпеки польотів, настання фізичного стресу чи такого робочого навантаження, коли немає впевненості в правильному і повному виконанні завдань персоналом	B
Значна	- серйозний інцидент - незначні телесні ушкодження - суттєві зменшення рівня безпеки	C

	польотів, зниження можливостей персоналу спралятися з експлуатаційними умовами внаслідок збільшення робочогоробочого навантаження чи виникнення умов, що знижують ефективність їхньої роботи	
Незначна	- деякі пошкодження - певні виробничі обмеження - застосування правилна випадок аварійної систуації	D
Несуттєва	Несуттєві наслідки	E

При оцінюанні наслідків рекомендовано враховувати дані про ймовірну кількість загиблих, нанесення майнових чи фінансових збитків можливий вплив на природне середовище, політичні наслідки та зацікавленність з боку засобів масової інформації тощо.

Наступним рекомендаційним кроком оцінювання ризиків відповідно до авіаційних документів рекомендовано є оцінка прийнятності наслідків небезпечного фактора. Такий процес назваnр оцінкою прийнятності ризику для безпеки польотів. Рекомендовано провести два етапи оцінки прийнятності ризику:

1) загальна оцінка ризику та складання матриці прийнятності ризику. ;

2) вибір критерію прийнятності та складання матриці прийнятності ризику.

Матриця оцінки ризику - це комбіноване поєднання даних, що отримані за допомогою таблиць імовірності та серйозності ризику. Для організацій ОПР при складанні матриці пропонується враховувати вимоги до єдиного Європейського простору (Single European Sky Common Requirements). Приклад такої матриці представлено в таблиці 3.

Таблиця 3 Матриця оцінки ризику

Імовірність ризику	Серйознічть ризику				
	Катастрофічна A	Небезпечна B	Значна C	Незначна D	Несуттєва E
часто 5	5A	5 B	5 C	5 D	5 E
періодично 4	4A	4 B	4 C	4 D	4 E
рідко 3	3A	3 B	3 C	3 D	3 E
малоймовірно 2	2A	2 B	2 C	2 D	2 E
майже неможливо 1	1A	1 B	1 C	1 D	1 E

Відмінність матриці ризиків, що пропонують використовувати в авіаційній галузі від тієї, що запропонована стандартом рекомендацій BS ISO/IEC 27005:2011 [21] та зображена на Рис.2.2. полягає у використіння двох компонент для опису Ймовірності та Серйозності, а саме цифру і букву

замість тільки однієї - цифри. Такий підхід дає більш наглядний внесок двох різних факторів, що використовуються для аналізу ризиків.

На Рис. 2.7 наведено приклад матриці прийнятності ризику відповідно до [23].

Індекс ризику	Рекомендовані критерії
5A, 5B, 5C, 4A, 4B, 3A	Неприйнятний за даних умов
5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B, 2C	Прийнятний з урахуванням заходів по зменшенню ризику
3E, 2D, 2E, 1A, 1B ,1C, 1D, 1E	Прийнятний

Рисунок 2.7 – Матриця прийнятності ризику відповідно до [23].

У випадку потрапляння ризику в червону недопустиму зону рекомендується виділити ресурси для зниження наслідків впливу небезпечного фактора чи/або для зниження масштабу чи потенціалу наслідків, що можуть бути викликані небезпечним фактором чи/або взагалі припинити даний вид діяльності, якщо зменшити небезпеку неможливо.

Наступним кроком управілння ризиками в аіації є впровадження стратегій зменшення оціненого ризику. Для цього може бути прийнято рішення щодо необхідності впровадження додаткових засобів захисту, наприклад розроблення нових процедур, правил, програм підготовки персоналу, удосконалення авіаційної техніки тощо. Або рішення щодо удосконалення вже існуючих засобів захисту. Рішення також може бути

прийнято про одночасно впровадження додаткових засобів та удосконалення вже існуючих.

В подальшому в процесі управління безпекою необхідно Здійснювати безперервний контроль, тобто постійний моніторингу та оцінки характеристик безпеки польотів. В подальшому також виявляти зовнішні та внутрішні зміни, які можуть вплинути на встановлений порядок, процедури та надання послуг та проводити, так зване, регулювання змін - ідентифікація потенційної небезпеки та усунення її негативного впливу на безпеку польотів.

Управління безпекою, як неперервний процес потребує вдосконалення системи управління безпекою. Отже рекомендується забезхпечити контроль характеристик безпеки.

В складовому елементі «Пропаганда» (Рис.2.4) важливим фактором є підготовка і навчання персоналу, а також бмін інформацією між експлуатаційним персоналом і адміністрацією.

Огляд системи управління ризиками авіаційної діяльності зроблено також в роботі [24].

Висновки до розділу 2

1. Одним з найважливіших етапів управління безпекою як в загальному, так і в авіаційній галузі є процес оцінювання ризиків.

2. З дослідження загального процесу управління ризиками можна зробити висновок, що це доволі складний процес, що складається з декількох етапів. Одним з найважливіших етапів та складним завданням цього процесу є кількісна (іноді, навіть, якісна) оцінка виявленого ризику.

3. З аналізу документів [22,23] можна зробити висновок про можливість якісного підходу до оцінювання ризиків для забезпечення безпечної роботи авіаційної транспортної системи.

РОЗДІЛ 3 ДОСЛІДЖЕННЯ ОЦІНКИ ІНФОРМАЦІЙНИХ РИЗИКІВ В ПРОЦЕСІ ОПР

3.1. Аналіз інформаційних загроз та вразливостей для ОПР

Побудова єдиного інформаційного простору відповідно до нових програм та концепцій ІКАО та Евроконтролю, інтеграції наявних та перспективних систем і комплексів в єдине рішення, що дозволяє здійснювати оперативне та безпечне обслуговування повітряним рухом, збільшити ефективність систем передавання та реалізувати здатність знаходження інформації за конкретним запитом в залежності від обставин є одним з важливих завдань стратегії розвитку авіації до 2030 року.

В свою чергу, нерівномірність розвитку різних авіаційних служб та інфраструктури, різноманітність інформаційних систем та питання їх сертифікації, а також нові ризики з якими стикається авіаційна галузь є перешкодою забезпеченню необхідного рівня безпеки інформаційного забезпечення.

В умовах, що склалися є необхідність завчасного аналізу і попередження можливих небажаних наслідків, на основі оцінки можливих ризиків інформаційній безпеці ІБ. Отже, основою та важливим етапом для успішного впровадження і функціонування СУБ авіації є оцінка та аналіз ризиків ІБ.

В роботах [19, 25, 26] зроблено огляд різних авіаційних подій на різних етапах польоту та вже введені рішення щодо безпеки польотів. В роботах зазначається, що міжнародними організаціями ІКАО та Евроконтроль вже було вжито деяких заходів для захисту систем управління повітряним рухом від кібер- та інших загроз, все ще залишаються значні слабкі місця контролю безпеки, які загрожують здатності забезпечити безпечну та безперебійну роботу систем повітряного простору.

Перехід від традиційних систем організації повітряного руху, таких як радіолокаційний контроль та голосове передавання інформації, до

перспектиних систем спостереження та зв'язку, які використовують сучасні протоколи передачі даних, сприяв значному посиленню безпеці авіаційного середовища. В рамках програм європейської Sky ATM Research (SESAR) та американські американські програми NextGen впроваджуються нові протоколи управління повітряним рухом та зв'язку [27].

Як можна побачити з Частини 2 даної роботи авіація має добро розинену теорію та практику управління ризиками зосереджуючись на безпеці та фізичній безпеці. Але нещодавно було введено нову область ризиків – кібер-ризики. У 2016 році на 39-й Асамблеї Міжнародна організація цивільної авіації було оголошено про підготовчі роботи з кібербезпеки та кіберстійкості. У вересні 2017 року вийшло оновлення додатку 18 до Конвенції ІКАО з авіаційної безпеки для надання настанов, у тому числі мінімальнихзаходи для захисту критично важливих інформаційних систем від несанкціонованого доступу [28,29].

Останні дослідження показали, що кіберзагрози, швидше за все, будуть одними з головних питань з безпеки в авіації, оскільки за даними SESAR та NextGen загальна система повітряного транспорту буде масово переходити до інфраструктури, заснованої на IP та працювати відповідно до концепції мережевих операцій, лгляд яких зроблено в першій частині даної роботи, з обміном інформацією в режимі реального часу. Як вже зазаначалося інформація має розглядатися, як ресурс чи актив, а отже має важливе значення для ефективності та успішної роботи систем ОПР.

Організація цивільних аеронавігаційних служб у 2014 ВИПУСТИЛА році керівництво з кібербезпеки [30]. І ньому пояснюється, що провайдери послуг повинні враховувати кібербезпеку в управлінні повітряним рухом, включаючи кіберзагрози та ризики, мотиви суб'єктів загроз, а також деякі з можливих положень щодо управління кібер-ризиками та впровадження програми з кібербезпеки.

Отже при аналізі ризиків в даній роботі особливу увагу приділемо саме тим ризикам, що можуть виникнути на етапах життєвого циклу інформації

для забезпечення безпечного ОПР. Врховуючи діджиталізаціє сучасної авіації включно кібер-ризики.

На основі загального процесу управління ризиками та розробимо загальний алгоритм оцінювання ризиків. Запропонований алгоритм показано на Рис. 3.1.

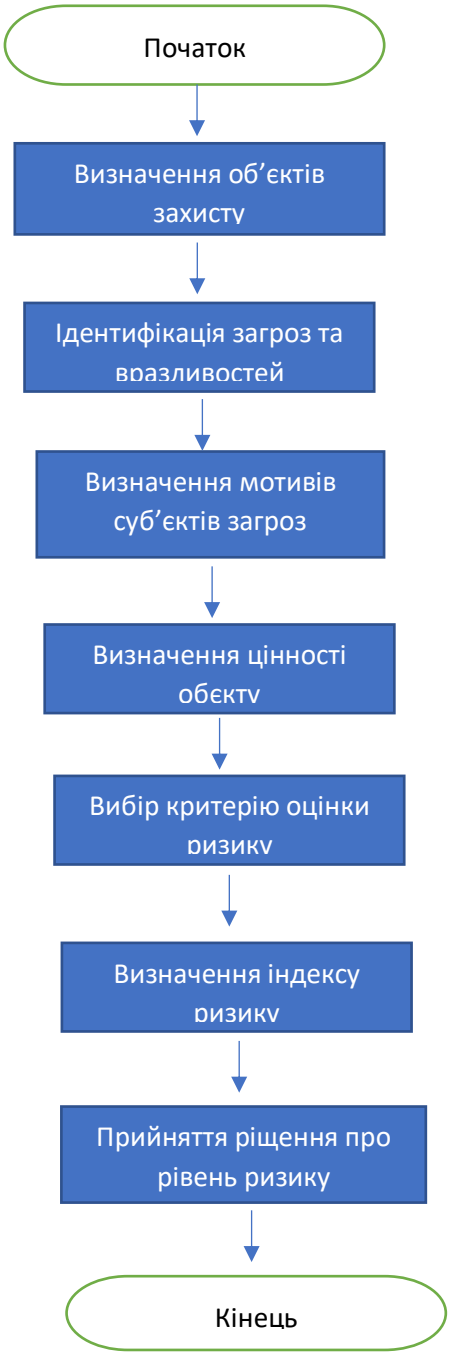

Рисунок 3.1 – Алгоритм оцінювання ризиків

Результати першого кроку – визначення об’єктів захисту наведено на в табліці 3.1. В таблиці 3.1 наведено перлік сучасних та перспективних авіаційних систем передаванням даних з зазначенням їх загальновідомих вразливостей.

Таблиця 3. 1 Визначення об’єктів захисту та їх вразливостей

Система	Опис	Вразливості
Радіолокатор первиного спостереження	Вимірює напрям та відстань до цілей за допомогою вібдитих радіосигналів	Не є кібер природи
Радіолокатор вторинного спостереження	Запиит додаткової інформації з ПС (ідентифікатор, висота, швидкість)	Прослуховування
Система попередження зіткнень	Запрос ідентифікації цілі	Прослуховування, Глушиння сигналу, спуфінг
ADSB	Транслювання інформації (ідентифікатор, висота, швидкість)	Прослуховування, Глушиння сигналу, спуфінг
GPS	Використання супутникових сигналів для позиціювання та корегування часу	Відносно слабкий сигнал, Глушиння сигналу, спуфінг, Життєвий цикл GNSS
Мультілатерація глобальної мережі (Wide Area Multilateration	Транслювання інформації (ADSB) та запит цільової послуги	перехоплення інформації втручання в роботу

(WAM)	(SSR)	інформаційних ситем

Також зазначемо деякі випадки кібер-загроз, які вже мали мсце в процесі пілотування сучасних ПС обладнанних бортовими інформаційними системами та системами зв’язку, та які використовують системи обмін даними в процесі польоту (див.розділ 1 даної роботи). Наприклад Airbus 380 та the Boeing 787 комунікацюють з багатьма мережами по всьому світу з різними рівнями захисту.

1. У 2006 році Федеральна авіаційна адміністрація (FAA) була змушена вимкнути частину своїх систем управління повітряним рухом після того, як кібератака призвела до порушення функцій її підтримки. Аудит заходів виявив, щовикористання комерційного програмного забезпечення та технологій Інтернет-протоколу для спроби модернізації операцій ставить систему перед високим ризиком для безпеки, оскільки операції не були належним чином забезпечені для запобігання несанкціонованому доступу.
2. У 2015 році експерт з безпеки в Сполучених Штатах Америки був затриманий після того, як нібито зламав систему розважальних заходів під час польоту на літаку Boeing 737-800 United Airline і одного разу успішно перезаписав код для видачі команди "підйом" .
3. У 2017 році експерт з питань кібербезпеки, який працював з Національною безпекою, успішно зламав припаркований Boeing 757 за допомогою радіочастотного зв'язку (Flight Safety Australia, 2017).

Отже такі випадки також мають бути враховані при ідентифікації загроз та вразливостей в процесі оцінки інформаційних ризиків для ОПР. В такому разі можливо виділити наступні вразливості дротовим та бездротовим взлам та мережам (наприклад, системи обслуговування кабін, пристрої екіпажу, інформаційні служби авіакомпаній, інформаційні системи для пасажирів, системи для розважальних послуг та системи технічного обслуговування,

бездротовий канал передачі даних, системи управління повітряним рухом, та домени інформаційних служб авіакомпаній):

- перехоплення інформації
- DoS атаки
- втручання в роботу системи та інші.

Відповідно до [30] для детальної оцінки інформаційних ризиків в процесі ОПР доцільно враховувати мотиви суб'єктів загроз. Для цього проаналізуєсо можливих суб’єктів та надамо деякі припущення стосовно їх мотивів та можливостей стосовно реалізувати загрозу. Для цього скористаємося напрацюваннями робіт [31,32] та власними міркуваннями, що засновані на аналізі павіаційних аипадків.

В таблиці 3.2 надано міркування стосовно суб’єктів, їх мотивів та можливостей.

Таблиця 3.2. Суб’єкти загроз, їх мотиви та можливості

суб’єкт	Мотив	Доступність ресурсів длядосягнення мети
Пасивний спотерігач	Фінансова або осовиста зацікавленість	Низька
Хактивісти та любителі	Визнння, або отримання задоволення від особистих можливостей	Низька
Інсайдери	Невдоволення ставленням або заробітною платнею, або іншім; помста; отримання додаткового заробітку	Високий
Кібер злочинці	Задоволення від особистого впливу, додаткові прибутки за допомогою шантажу чи	Висока

	залякування	
Кібер теротисти	Політична або релігійна	Середня
Держави	Знищення потенційно небезпечних об.єктів	Дуже висока

Потрібно зазначити, що в таблиці для оцінки доступності ресурсів для досягнення мети використовували найвищий з можливих рівнів. Наприклад суб'єкт інсайдер відповідно до свого персонального доступу може мати низький, середній або високий рівень доступних ресурсів. Але з точки зору потенційно можливої оцінки наслідків та ймовірності потенційно можливих дій ставимо високий рівень доступності ресурсів.

Надамо деякі пояснення стосовно опису суб'єктів та ресурсів, які доступні до їх використання. Пасивний спостерігач – як правило, використоаує загальнодоступні та приватні веб-сайти та мобільні програми, які відображають ефір, трафік та його комунікації в режимі реального часу. Можуть використовувати ADSB приймач. Ймовірність можливої шкоди можна оцінити, як низьку врахоуючи відсутність значних можливостей.

Хактивісти та любителі – їх мета- це використання дір у безпеці за допомогою існуючих простих у використанні атак із типово низькою витонченістю. Вони здатні контролювати та втручатися в авіаційні канали зв'язку. Їх мотивація часто нераціональна. Ріень ймовірності та наслідків, як правило низький, тому що такі суб'єкти можуть бути виявленні за допомогою резервних систем спостереження.

Інсайдерами можуть бути підрядники, або ділові партнери. Як наведено на реальному прикладі вище, навіть експерт з безпеки в Сполучених Штатах Америки здійснив злам системи під час польоту. Його метою міг бути бажання визнання так і демонстрація доказу вразливостей систем безпеки. Такі скб'єкти мають внутрішню інформацію про методи безпеки організації, дані та комп'ютерні системи. Враховуючи можливий доступ інсайдера до

ключових програм та інших важливих систем робить ймовірність та можливі наслідки його можливих несанкціанованих дій високим.

Кібер злочинці зазвичай прагнуть атакувати системи з метою отримання грошової вигоди. Вони часто ма.ть достатні знання з роботи систем та програмного забезпечення і часто деякі спеціальні пристрої для отримання інформації чи заподіяння шкоди. Дії таких суб'єктів безумовно потрібно враховувати при оцінюванні ризиків.

Кібер теротисти мають за мету загрожувати національній безпеці, спричиняти масові жертви, послабити економіку. або підірвати довірі до авіаційних систем. Можуть здійснювати атаки на літаки з землі та з безпечної відстані.

Держави – мають достатні знання про системи виявлення вторгнень та майже необмежені ресурси. Наслідки та ймовірність ризику оцінюється відповідно до конкретних політичних обставин і може коливатися до високого.

Для оцінки ризику також доцільно проаналізувати з якими загрозами пов'язані вказані вразливості. Як вже зазначалося, зазвичай загрози інформаційній безпеці криються в порушенні конфівенційності, цілісності та доступності, мета загроз - це:

- ознайомлення з інформацією
- модифікація інформації
- руйнування інформації.

В роботі [33] надано статистичні дані щодо суб'єктів створення загроз, які можуть бути прийняті до уваги в процесі аналізу ризиків. Дані базуються на аналізі витоку інформації таких авіакомпаній як British Airways, Delta Air Lines та Cathay Pacific в результаті діджиталізації та використання хмарних технологій для зберігання та обміну інформації. Дані представлено на діаграмі Рис.3.2.

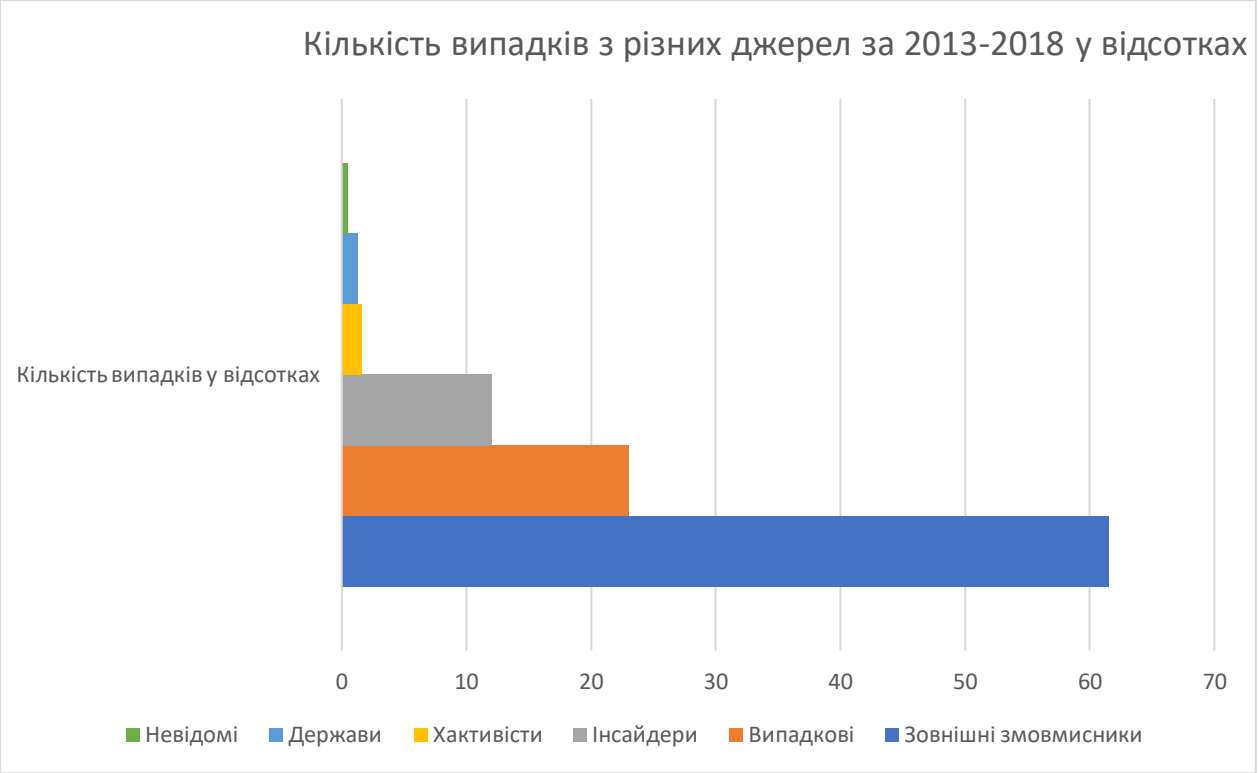

Рисунок 3.2 – Кількість випвдків, що призвела до витоку інформації з [33]

На основі аналізу та ідентифікації зароз та вразливостей в таблиці 3.3. наведено найбільш поширені вразливості інформаційних систем та систем зв'язку і управління ПС в процесі ОПР. В таблиці також показано відповідність зазначеної вразливості щодо можливої загрози, а також з цілями цих загроз.

Таблиця 3.3 Найбільш поширені вразливості інформаційних систем та систем зв'язку і управління ПС в процесі ОПР

Вразливість	Ціль загрози	Загроза
Прослуховування	ознайомлення	Порушення конфіденційності
Глушиння сигналу, Слабкий сигнал	руйнування	Порушення доступності

Спуфінг	модифікація	Порушення цілісності
Перехоплення інформації	ознайомлення	Порушення конфіденційності
Втручання в роботу інформаційних ситем	Модифікація та руйнування	Порушення цілісності та доступності
DoS атаки	руйнування	Порушення доступності

3.2. Оцінювання інформаційних ризиків для ОПР

Наступним кроком оцінювання ризиків є вибір критерію для якісної або кількісної оцінки ризиків, та саме оцінка ризиків.

Скористаємося підходом, який описаний в другом розділі даної магістерської роботи для якісного оцінювання ризиків та рекомендований документами ІКАО та Евроконтролю. Як рекомендовано за критерій оберемо ймовірність виникнення загрози та серйозності наслідків можливої реалізації ризику. Для кожної групи вразливість-загроза складемо відповідні оціночні таблиці.

Проведена оцінка базується на аналізі реальних випадків, які мали місце або, навіть, призвели до авіаційної події. Також застосовувалися елементи експертної оцінки до якої були залучені спеціалісти в галузі інформаційних систем та працівники авіаційної галузі.

В таблиці 3.4. наведено результати оцінювання ризиків відповідно до ймовірності виненкнення, а втаблиці 3.5. відповідно до серйозності наслідків.

Таблиця 3.4 Ймовірність виненкнення

Загроза	Ймовірність виникнення	Величина
Прослуховування	Періодично	4
Глушиння сигналу (навмисне і випадкове)	Періодично	4
Спуфінг	Рідко	3
Перехоплення інформації	Рідко	3
Втручання в роботу інформаційних ситем	Малоймовірно	2
DoS атаки	Малоймовірно	2

Таблиця 3.5 Серйозність наслідків

Загроза	Сер’йозність	Рівень
Прослуховування	Несуттєва	E
Глушиння сигналу	Незначна	D
Спуфінг	Значна	C
Перехоплення інформації	Несуттєва	E
Втручання в роботу інформаційних ситем	Катастрофічна	A
DoS атаки	Небезпечна	B

Прослуховування оцінено, як достатньо ймовірна ситуація завдяки широкому колу модливих учасників – може виконуватися пасивними спостерігачами, так і любителями, або, навіть кібер злочинцями. Наприклад, пасивні спостерігачі використовують відкритий характер протоколів зв'язку повітряного руху, використовують загальнодоступні та приватні веб-сайти та

мобільні додатки, які відображають повітряний трафік та комунікації в режимі реального часу. Інші зловмисники можуть використовувати дешеві приймачі SDR, щоб зібрати інформацію про повітряний рух і, в подальщому використорвувати такі дані для аналізу. Але ризик від такий дій оцінено як низький, тому що, як правило, відсутні активні дії зі сторони таких зловмисників.

Глушиння сигналу також оцінено як подія з відносно високою ймовірністтю. Така оцінка надана, тому що враховувалася природа різних сигналів та природа завад. Якщо навмисне глушіння це більш рідкісна подія, то глушіння за рахунок сумісної дії різного електромагнітного випромінення та різних природніх факторів є більш частою і ймовірною ситуацією. Сер'йозність наслідків від такої події оцінено як нижче середньої, тому що малойомірно, що таке глушіння відбудеться одночасно для всіх каналів зв'язку, а також одержання та передавання інформації.

Ймовірність спуфінгу оцінено, як середня. Така подія може бути заподіяна як активістами та любителями так і професйними злочинцями, які можуть дозволити собі вртісну апаратуру. Сер'йозність наслідків також оцінена, як середня враховуючи той факт, що,наприклад, мета любителів це використання дір в безпеці за допомогою існуючих і відносно простих у використанні атак. Все ж таки вони здатні контролювати та втручатися в авіаційні канали зв'язку. Але наслідки дій «люьителів» часто можна виявити та пом'якшити за допомогою резервних систем спостереження та протидії. Натомність ризик від дій кібертерористів та професійних злочинців, які мають на меті отримання грошової вигоди або загрозу національній безпеці вже можу бути набагато серйознішім, хоча не таким ймовірним. Отже такій загрозі надано середню оцінку серйозності наслідків.

Перехоплення інформаці, яке як і прослуховування призводить до ознайомлення з інформацією, має оціночне значення ймовірності середнє, тому що потребує додаткоого обладнання, що, в сою чергу ускладнює

моливість реалізації такої дії. Наслідок подій також оцінено, як низький завдяки відсутності активних дії зі сторони зловмисників.

Втручання в роботу інформаційних ситем може бути реалізована як інсайдерами так і кібер злочинцями і терористами. Інсайдерами можуть бути незадоволені працівники, колишні співробітники, підрядники або навіть ділові партнери. Їм допамагає той факт, що вони мають внутрішню інформацію про практику безпеки організації, дані та комп'ютерні системи. Їх мотивацією маже бути жадібність, злість, що часто призводить до непередбачуваності в їх можливих діях. Часто вони мають доступ до ключових програм та інших важливих систем. Цей фактор сприєї тому, що виконати зловмисну дію інсайдерам легше ніж кібер терористам, які мають шукати інші механізми проникнення, наприклад, створювати шкідливе програмне забезпечення. Ймовірність втручання в систему оцінено, як нижче середнього, тому що враховано факт відбіру потенційних працівників з огляду їх морально-психологічних якостей, а також складність завдіння для інщіх кібер злочинців. Але наслідки такого втручання мажуть бути дуже сер'йозними, наприклад, зміна траєкторії польоту ПС, отже загальний ризик є середнім.

DoS атаки такж можуть бути вчинені інсайдерами, кібер злочинцями та терористами. Втрата доступу, порушення доступності інформації в багатьох ипадках може призвести до повної втрати контролю. В роботі [34] проведено моделювання DoS атаки на систему курування польотом (FMS) з подальшім аналізом результатів моделювання. Результати моделювання показали, що за сценарієм неможливості отримати дані про план польоту, унеможливила доступ до карт, але працювали системи, які незалежні від супутникового сигналу, така атака призвела до підвищенного навантаження на комунікативну діяльність між диспетчерськими службами та екіпажем ПС для забезпечення навігації керованої авіадиспетчером. Прийняв до уваги той факт, що для здійснення такої події необхідно мати певні знання в інформаційних технологіях, ймовірність реалізації загрози оцінено, як

низьку, але наслідки втрати доступу по інформаційних та інших систем оцінено як сер'йозні.

Відповідно до рекомендацій для оцінки ризикі необхідно скласти матрицю оцінки ризиків за комбінованим поєднанням оцінки ймовірності та сер'йозності наслідків (таблиці 3.4 та 3.5.). Отже матриця оцінки інформаційних ризиків для ОПР в сучасних та перспективних умовах наведено в таблиці 3.6.

Таблиця 3.6. Матриця оцінки ризиків для інформації при ОПР

Загроза	Ціль	Індекс ризику
Прослуховування	ознайомлення	4E
Глушиння сигналу	руйнування	4D
Спуфінг	модифікація	3C
Перехоплення інформаці	ознайомлення	3E
Втручання в роботу інформаційних ситем	Модифікація та руйнування	2A
DoS атаки	руйнування	2B

Розмістимо загрози інформації, що було розглянуто в даній роботі з урахуванням отриманих індексів ризику відповідно до рівней прийнятності/неприйнятності, як рекомендовано в [23] та зображено на Рис.2.5 та Рис. 2.6 для процесу оцінювання ризиків. Результат показано на Рис. 3.3. Червоний колір на Рис.3.3. відповідає зоні з ризиком, що є неприйнятним в будь якому разі за даних умов. Жовтий колір відповідає зоні прийнятного ризику з урахуванням заходів щодо його зниження та аналізу

затрат/вигод.Зелений колір відповідає ризику прийнятному на його фактичному рівні

Рисунок 3.3 – Матриця ризику

Отже, в результаті аналізу та оцінки ризиків інформації для забезпечення ОПР за сучасних та перспективних вимог та умов розглянуті як можна побачити на Рис.3.3. розглянуті ризикі в більшості виявилися в жовтій зоні, що є зоною прийнятного ризику, але вимагає заходів щодо його зниження. Розділ 3.3.даної магістерської роботи присячено огляду сучасних можливостей та формулюванню можливих рекомендацій щодо зменшення ризиків інформації для забезпечення безпечного ОПР за сучасних та перспектиних вимог та умов.

3.3. Рекомендації щодо зменшення інформаційних ризиків при ОПР

Аналіз можливих ризиків інформації. що задіяна для забезпечення ОПР полягає також в оцінюванні ризиків компонент інформаційних систем та систем обробки, передавання, поширення та збереження інформації. Для цього ткі системи мають бути стійкими щодо можливих ризиків.

Ідея стійкості інформацйних систем та систем передавання та обміну інформацією, що задіяні для забезпечення ОПР до можливих ризиків полягає в оцінці того, що відбувається до, під час та після того, як система, що складається з в тому числі і з цифрових мереж, стикається із загрозою, включно кібер загрози. В різних роботах деякі дії відповідно до цілей загроз націлені на передбачливість, стійкість, винахідливість, надмірність, швидке відновлення або пристосованість. Інші враховують запобігання, готовність, реагування та відновлення. При оцінінюванні необхідно враховувати як інженерно-технічн компоненту таких систем, так і і інші компоненти: організаційну, економічну, соціальну. Програма Eurocontrol Research використовує для стійкості наступне визначення: «Стійкість - це здатність запобігати збоям, готуватися до змін і пристосовуватися до них, швидко реагувати та швидко відновлюватися від порушень, щоб забезпечити безперервність послуг на прийнятному рівні продуктивності ". Метою такого визначення є досягнення розуміння того, що питання забезпечення стійкості в більшій мірі пов'язана з управлінням ризиками, а не з їх усуненням [35]. Забезпечити стійкість – це означає забезпечити можливість працювати належним чином за умов погіршеного режиму в декількох рівнях. При цьому забезпечувати заходи з усунення вразливостей чи небезпек, або запобігання потрапляння в умови ризику. Отже важливим є розробка методів та засобів, що дозволять вийти з умов погіршеної роботи якомога швидше. В роботі [36] розглянуто набір заходів, необхідних для забезпеченнядостатньої стійкості проти різних ризиків та протиправних дій включно інформаційні ризики та

кібератаки. Ці заходи являють собою поєднання різних дій та належної поведінки до, під час та після інциденту. В документі [36] це названо «Парасоля стійкості».

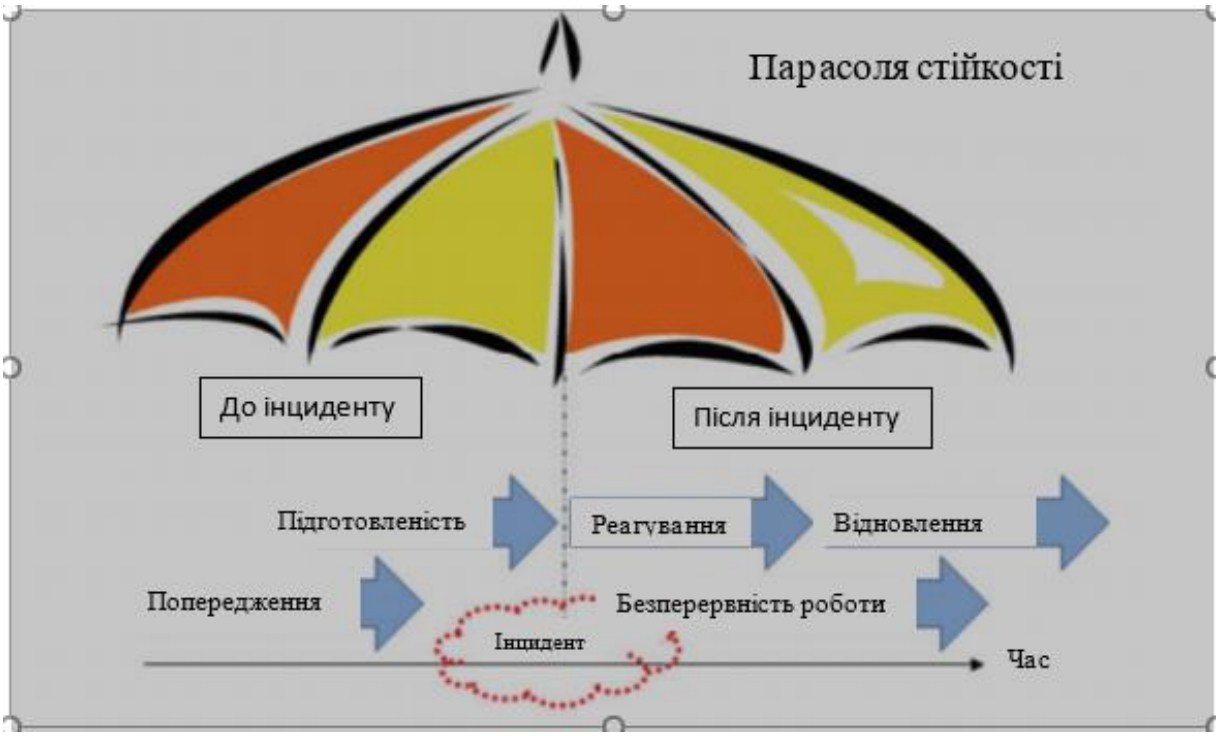

Рисунок 3.4 – Парасоля стійкості з [36]

Як можна побачити на Рис.3.4. дуже важливим в процесі забезпечення безпеки роботи інформаційних систем при ОПР є підготовленність до можливих ризиків та можливе їх попередження. Завжди кращим є попередження небажаної події, ніж відновлення роботи після інциденту та ліквідація наслідків.

За підходу, який зображено за допомогою «парасолі стійкості» важливим кроком є реагування на інцидент. Це означає, що виявляється акт небажаної дії (інцидент, атака, втручання і.т.і.), в подальшому інцидент постійно знаходиться в межах уваги та можливому викорененні вразливості або загрози, що є причиною інциденту. Одночас важливим є безперервне надання авіаційних послуг, отже, навіть після інциденту, безперервність роботи є одним з приорітетів при забезпеченні стійкості системи, або маркерів стійкості. Такий підхід є важливим, тому що при організації заходів,

що націленні на подоланні наслідків інциденту можливі обмеження, або навіть, унеможливлення послуг. В документі [36] зазначається, що на кроці «реагування» відповідні дії потрібно продовжувати доти, доки причина та навіть каскадні наслідки нападу не будуть усунені, враховані або не припинені. Наступний крок – відновлення- реалізється одразу після усунення інциденту та його наслідківю Це необхідно робити якомого швидшедля відновлення працездатності всієї системи, яка забезпечує роботу ОПР.

Концепція стійкості спочатку була впроваджена в авіації головним чином для посилення сектору безпеки, і не була детально розроблена щодо питань пов'язаних з ризиками в сучасних та перспективних інформаційних простірах для забезпечення потреб ОПР включно ризиків пов'язаних з кібербезпекою та подальшім управлінням повітряним рухом.

В даній роботі був проведений аналіз можливих ризиків для оцінування вразливостей сучасних та перспективних інформаційних систем та систем обміну та поширення інформації. В роботі [37] стійкість розглядається як здатність системи унеможливлювати або уникати пошкоджень, не зазнаючи повної відмови, включаючи аспекти захисту, зменшення наслідків та відновлення. Відповідно до вимог оцінки ризиків [32] такий процес має бути безперирвним та динамічно реагувати на результати оперативного аналізу ризиків для інформації, що використовується для забезпечення безпечного ОПР та для встановлення кіберстійкості в системі сучасного повітряного транспорту. На основі проведеного аналізу можливих ризиків та їх оцінки запропоновано наступні рекомендації щодо зменшенн, або усунення можливого небажаного впливу на роботу сучасних та перспективних інформаційних систем та систем обмину та поширення інформапціїї.

1. По перше необхідно розробити структурну та процедурну основу та рекомендації щодо постійного внутрішнього та міжорганізаційного аналізу стійкості систем включно кіберсистем. Враховуючи постійне збільшення цифрових та автоматичних систем обробки, зберігання та поширення інформації, процедури мають враховувати нові підходи до

оцінювання як кіберстійкості систем, так і вже існуючи підходи до сучасних системі.

2. Бажано створити організаційну структуру, яка об'єднує персонал усіх пов’язаних структур всередині та між організаціями повітряного руху, щоб цілісно справлятися з кіберзагрозами, що з’являються. Забезпечити співпрацю між різними структурами для обміну даними для повторного використання існуючих даних, що включають технічні, методологічні та організаційні аспекти. Забезпечити доступ до великих обсягів даних для їх перевірки та подальшої кількісної і якісної оцінки загроз, що виник через провал інформаційної безпеки. Це дозволить висунути додаткові рекомендації щодо підвищення інформаційної та кібербезпеки повітрянго простору.

3. Забезпечити розглядання та включення загроз до конфіденційності, доступності та цілісності інформації при ОПР до звітів з подальшою обробкою такої інформації.

4. Розробити нормативну базу, що узгоджується з існуючими нормами та стандартами інформаційної безпеки.

5. Розробити міждисциплінарні групи з аналізу ризиків різної природи, включно кібер-ризикі.

6. Сприяти поширенню ІТ-знаннь та обізнаності в питаннях безпеки персоналом різних структур, що задіяні в ОПР, включаючи менеджмент різного рівня, пілотів та авіадистпетчерів.

7. Розробити методологію для розробки сценаріїв загроз інформації, що необхідня для ОПР та їх застосування у навчанні, підвищенні кваліфікацйії, перевірки та підтвердженнію.

8. Приділяти увагу постійному навчанню персоналу для набуття відповідних навичок для виявлення порушень кібербезпеки та інших загроз щодо інфрмаційної цілісності, доступності та конфіденційності.

9. Процес розробки розвитку сценарієв різних загроз має бути безперервним та охоплювати різні структурні частини, що задіяні в усьому життєвому циклі інформації.

10. На початковому етапі використовувати методи математичного моделювання, імітаційного моделювання для одержання та порівняння результатів, і формулювання висновків. Розробляти методи, що дозволяють динамічно моделювати та аналізувати інформаційні ризики в складних системах, великих організаціях або навіть між кількома взаємопов'язаними організаціями, так щоб якомога більше відображати авіаційну транспортну галузь.

11. Результати моделювання доцільно інтегрувати в процес прийняття рішень та системи підтримки прийняття рішень.

12. Оскільки кіберзагрози та інші інформаційні ризики можуть мати прямий вплив на функції системи, що мають важливе значення для безпеки авіаційної галузі необхідно забезпечити узгодженість безпеки польотів та безпеки авіації.

13. Розробка та впровадження комплексного та безперервного підходу до управління ризиками.

14. Приділити увагу розробкам та покращенню методів проектування стійких до ризиків систем, які включають в себе не тільки класичні питання, такі як людський фактор, а стійкість до кібер небезбек, що є актуальним в світі розвитку сучасних цифорвих систем, що працюють з інформацією протягом всього її життєвого циклу.

15. Сприяти поширунню культури кібербезпеки, коли інформація про кіберзагрози розпізнається та повідомляється для подальшого ефективного управляння ризиками.

16. Інтегрувати існуючи та нові системи управління інформаційною безпекою (кібербезпекою) до діючої системи управління безпекою (SMS) для підвищення її ефективності. Це дозволить забезпечити неперервне керування ризиками з урахуванням нових викликів авіаційній галузі, що

з`явилися з новою цифровою ерою, яка, в свою чергу хоарактеризується і появою нових ризиків.

17. Забезпечити розглядання та включення загроз до конфіденційності, доступності та цілісності інформації при ОПР до звітів з подальшою обробкою такої інформації.

18. Сприяти створенню та впровадженню структури управління безпекою та управління ризиками та стратегії управління ризиками в інформаційних системах та системах збереження, обробки та поширення інофрмації та інших. Чітко встановлювати відповідальність за інформаційну безпеку. Впрваджувати засоби контролю безпеки.

19. Використовувати системи, що у разі необхідності можуть дублювати функції. Наприклад, перехресна перевірка висоти під час підходів на основі GNSS може бути важливим елементом захисту за умов відказу доступу до супутникових даних, або модифікації такої інформації. Це необхідно для запобігання неправильному шлях польоту за умов впливу на сигнали GNSS.

20. В педпольотний інструктаж необхідно чітко звертати увагу на дані систем управляння польотом, наприклад, висота порогу злітно-посадкової смуги. Це допоможить перехресно перевірити такі дані пеед вильотом для виявлення можливого втручання в інформаційні системи в процесі польоту.

21. При оновленні інформації на моніторах інформаційних систем для ОПР та пілотів впровадити процедуру для забезпечення достовірності отриманої інформації, наприклад, шляхом автентифікації передачі даних або дозволяючи льотному екіпажу реагувати або підтверджувати зміни безпечним способом. Це може бути доцільним в умовах вільного польоту для інформації про оновлення траєкторії польоту.

Висновки до розділу 3

1. На наш час інтегрований загальноорганізаційний підхід до управління ризиками інформаційної безпеки, який відповідає його сучасним вимогам та потребам не повністю встановленний та інтегрований до діючої системи управління безпекою (SMS).
2. За сучасних рекомендацій щодо управління ризиками не чітко встановив ролі та відповідальність за інформаційну безпеку.
3. Не існує цілісної нормативно-правової бази для забезпечення інформаційної безпеки в ОПР.
4. Доцільно проводити аналіз можливих мотивів суб'єктів загроз для покращення процесу аналізу ризиків.
5. Необхідно задіяти комплексний підхід до системи інформаційної безпеки в ОПР використовуючи як технологічні, так і організаційні, юридичні, соціальні та економічні аспекти. Тобто виконувати вимогу цілісності, неперервності , комплексності системи інформаційної безпеки. Такий підхід може забезпечити більшу ефективність та безпеку систем ОПР.

Загальні висновки

1. Сучасні та перспектині підходи до збільшення пропускної спроможності та ефективності існуючої системи повітряного руху вимагають переходу до цифровізації та автоматизації. Як результат, раніше відокремлені IT-системи підключаються до єдиної мережі для обміну інформацією та даними, що в свою чергу збільшується складність системи та створюються раніше невідомі взаємозалежності. Отже, обмеження управління ризиками безпеки до “традиційних” фізичних аспектів вже недостатнє для забезпечення стабільної та надійної роботи системи повітряного транспорту. Необхідно також враховувати складову кібербезпеки та розширювати її значення для розробки більш стійких та цілеспрямованих підходів щодо забезпечення безпеки авіації.

2. Для врахування складової кібербезпеки необхідно дослідити потенційні відомі загрози та ризикі сучасним та перспективним системам зберігання, обробки та поширення інформації та оцінити потенційні загрози кібербезпеці для ОПР та контролю повітряного руху.

3. Важливо розуміти, що сучасна інфраструктура для обміну інформацією націлена на інформацію,як основний актив, який має бути захищеним для забезпечення надійного обміну даними між зацікавленими сторонами ОПР.

4. Ідентифікація та оцінка загроз і вразливостей систем та цілої інфраструктури є найважливішим завданням для підвищення безпеки як сучасної, так і майбутньої системи ОПР.

5. Процес управління ризиками - це доволі складний процес, що складається з декількох етапів. Одним з найважливіших етапів та складним завданням цього процесу є кількісна (іноді, навіть, якісна) оцінка виявленого ризику. Враховуючи документи [22,23] можна зробити висновок про можливість якісного підходу до оцінювання ризиків для забезпечення безпечної роботи авіаційної транспортної системи.

6. Необхідно задіяти комплексний підхід до системи інформаційної безпеки в ОПР використовуючи як технологічні, так і організаційні, юридичні, соціальні та економічні аспекти. Тобто виконувати вимогу цілісності, неперервності, комплексності системи інформаційної безпеки. Такий підхід може забезпечити більшу ефективність та безпеку систем ОПР.

7. В роботи проведено дослідження та здійсноене порівняльний аналіз як загальних підходів до оцінки ризиків, так і підходів, що рекомендовані ІКАО, Eurocontrol та відповідними національними структурами до управління ризиками та складових цього процесу включно оцінки ризиків.

8. В роботі запропоновано алгоритм оцінювання ризиків, якій враховує мотиви можливих суб'єктів загроз.

9. На основі статистичних даних та аналізу авіаційних подій з відкритих джерел інформації, а також експертних думок та висновків проведено якісну оцінку ризиків щодо сучасного та перспективного інформаційного забезпечення ОПР відповідно до вимог ІКАО, Eurocontrol та відповідниз національних структур. Проведено аналіз та ідентифікацію загроз і вразливостей системам зберегання, обробки та передавання інформації, що можуть призвести до втрати конфіденційності, цілісності та доступності інформації.

10. В роботі на основі аналізу сучасних авіаційних систем зберігання, обробки та поширення інформації, а також на основі аналізу оцінки ризиків, як складового процесу управління ризиками розроблено рекомендації щодо зменшення впливу можливих загроз та ризиків сучасним та перспективним системам зберігання, обробки та поширення інформації.

11. Надані в роботі рекомендації стосуються різних аспектів системи інформаційної безпеки – організаційної, технологічної, правової, соціальної та економічної.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. FAA Next Generation Air Transportation System

https://www.slideserve.com/stella/u-s-faa-next-generation-air-transportation-system

2.. Hoekstra J. M, van Gent R.N.H.W., Ruigrok R.C.J., Designing for Safety: the Free Flight Air Traffic Management concept / National Aerospace Laboratory NLR, Amsterdam, Netherlands

www.asas-tn.org › library › nlr › nlr_hessd99

3. Global TBO Concept

https://www.icao.int

4. U.S. Next Generation Transportation System (NextGen)

https://www.icao.int

5. SESAR

https://www.sesar.eu/

6. Global Air Navigation Plan 2016-2030

https://www.icao.int/airnavigation/documents/ganp-2016-interactive.pdf

7. Програма NextGen

https://www.faa.gov/nextgen/

8. Марьин Н. П., Перспектива внедрения концепции «свободный полет»/ журнал «Проблемы безопасности полетов» (Гос НИИ «Аэронавигация»)

https://www.aviahumanfactor.ru/pbp/2/1511/perspektiva-vnedreniya-koncepcii-svobodnyy-polet.htm

9. ICAO Doc.10039

10. System-wide-information-management

https://www.eurocontrol.int/concept/system-wide-information-management

11. Аверьянова Ю.А., Яновський Ф.Й., Динамічна інтерактивна система отримання та поширення метеорологічної інформації // Електроніка та системи управління. – 2011. - №2(28). - С. 95-99.

12. Авер‘янова Ю.А., Інтерактивна глобальна мережа отримання, обміну та поширення метеорологічних даних // Вісник -К.: НАУ, 2012. Том 4- стор. 26-30.

13. Робочий план програма NextGen

http://www.faa.gov/nextgen/media/avs_nextgen_workplan_2012.pdf

14. GLOBAL TBO CONCEPT https://www.icao.int/airnavigation/tbo/PublishingImages/Pages/Why-Global-TBO-Concept/Global%20TBO%20Concept_V0.11.pdf

15. ATM Enhancements and Trajectory Based Operation (TBO), Henk Hof, Head of ICAO & Concepts Unit

https://www.aircraftit.com/articles/atm-enhancements-and-trajectory-based-operation-tbo-from-icao/

16. Ярочкин В.И., Информационная безопаснсть

https://studfile.net/preview/2204909/

17. https://zakon.rada.gov.ua/rada/show/v0528763-12#Text

18. Класифікація загроз

https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D0%B8_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8

19. Averyanova Y., Blahaja L., A Study on Unmanned Aerial System Vulnerabilities for Durability Enhancement // 2019 IEEE 5th International Conference Actual Problems of Unmanned Aerial Vehicles Developments, APUAVD 2019 - Proceedings, 2019, pp. 40-43, 8943896

20. Стандарт інформаційної безпеки ISO 27002 «I*nformation technology — Security techniques — Code of practice for information security management», 2000p*

https://www.iso.org/ru/standard/54533.html

21. Стандарт ISO/IEC 27005:2011 Information Technology – Security techniques – Information Risk Management (Інформаційні технології – технології безпеки – управління інформаційними ризиками)

https://www.iso.org/standard/56742.html

22. Annex 19 to ICAO Convention, *Safety Management*, the second edition, Montreal

23. Методичні рекомендації з впровадження систем управління безпекою польотів, Наказ, ДЕРЖАВНА АВІАЦІЙНА СЛУЖБА УКРАЇНИ, 26.07.2012 № 528

https://zakon.rada.gov.ua/rada/show/v0528763-12#Text

24. Харченко В.П, Алєескєєв О. М., Система управління ризиками авіаційної діяльності, 2018

25. Чабан Г. М., Актуальні питання попередження ризику в цивільній авіації україни // Економічна наука, Економіка та держава № 2/2019, стор. 130-134

DOI: 10.32702/2306-6806.2019.2.130

26. Air Safety Cyber Security: Why Cyber Security is a Threat for Air Safety submitted for the ISASI Rudolf Kasputin Memorial Scholarship 2019

27. M. Strohmeier et al. (2016) Assessing the Impact of Aviation Security on Cyber Power // in the 8th International Conference on Cyber Conflict Cyber Power

28. International Civil Aviation Organisation (2013) “Initial capability for ground surveillance,” in Global Air Navigation Plan 2013-20282 12. International Civil Aviation Organization (ICAO) (2017)

29. Aviation Security Manual, 10th Edition, https://www.icao.int/Security/SFP/Pages/SecurityManual.aspx

30. CANSO (2014) Cyber Security and Risk Assessment, Civil Air Navigation Services Organization

31. Strohmeier M. et al. (2016) Assessing the Impact of Aviation Security on Cyber Power// in the 8th International Conference on Cyber Conflict Cyber Power

32. Lykou G., Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management: Theories, Methods, Tools and Technologies, Critical Infrastructure Security and Resilience (pp.245-260).

33. Cathay Pacific Cyber Attack Occurs as Airline Moves to the Cloud https://neuvector.com/network-security/cathay-pacific-attack/

34. Geister R., Buch J.-P., Niedermeier D. , Gamba G., Canzian L., Pozzobon O., Impact study on cyber threats to gnss and fms systems // 31st Congress of the International Council of the Aeronautical Sciences, Belo Horizonte, Brazil, September 9-14, 2018

35. EUROCONTROL (2012) Manual for National ATM Security Oversight, Eurocontrol Publications

36. EUROCONTROL (2009) A White Paper on Resilience Engineering for ATM, https://www.eurocontrol.int/sites/default/files/article/content/documents/nm/safety/safety-awhite-paper-resilience-engineering-for-atm.pdf

37. M. Kreuzer. T. Kiesling (2017) Recommendations to Strengthen the Cyber Resilience of the Air Traffic System, ARIEL, Air Traffic Resilience