Міністерство освіти і науки України
Національний університет “Острозька академія”
Навчально-науковий центр заочно-дистанційного навчання
Кафедра національної безпеки та політології

Кваліфікаційна робота
на здобуття освітнього ступеня магістра на тему:

“Правові та організаційні засади контррозвідувального режиму на об’єктах державної авіації”

Виконала студентка ІІ курсу, групи ЗМНб-21
спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності)
Бандура Валерія Сергіївна

Керівник – доктор юридичних наук, професор
Романов Микола Степанович
Рецензент – доктор військових наук, професор
Телелим Василь Максимович

Острог, 2025

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Актуальність обраної теми зумовлена масштабними трансформаціями безпекового середовища України, спричиненими повномасштабною збройною агресією Російської Федерації, яка супроводжується широким застосуванням методів гібридної війни, диверсійної, агентурної та кібернетичної діяльності. В умовах воєнного стану особливого значення набуває забезпечення захисту об'єктів критичної інфраструктури сектору безпеки і оборони, зокрема таких, що пов'язані з експлуатацією, управлінням та охороною об'єктів державної авіації.

Авіаційна інфраструктура є не лише логістичною або транспортною складовою державного апарату, але й виконує функції стратегічного рівня в оперативному плануванні, управлінні військовими операціями, реагуванні на надзвичайні ситуації та гарантуванні повітряного суверенітету. З огляду на це, об'єкти державної авіації — аеродроми, командно-диспетчерські пункти, центри управління, авіаційні бази тощо — становлять пріоритетні цілі для засобів розвідки, диверсійних груп і засобів високоточної зброї противника. Водночас ці об'єкти залишаються недостатньо захищеними з позицій нормативно-правового, організаційного та інституційного забезпечення контррозвідувального режиму.

Наразі в Україні відсутня уніфікована концепція або модель побудови контррозвідувального режиму в авіаційній сфері державного призначення. Законодавство не містить чіткого визначення поняття "контррозвідувальний режим", а функціональний розподіл повноважень між Службою безпеки України, Міністерством оборони України та Головним управлінням державної авіації України є фрагментарним, що ускладнює ефективну координацію міжвідомчих зусиль у сфері захисту авіаційної інфраструктури. На відміну від цивільного авіаційного сектора, де функціонує вертикальна система безпеки під керівництвом Державної авіаційної служби України, у сфері державної авіації така структура не створена, що призводить до наявності значних прогалин у нормативному полі, процедурному забезпеченні та кадровій підготовці.

Відсутність системного підходу до виявлення, оцінки та реагування на ризики у сфері державної авіації значно знижує стійкість об’єктів до сучасних загроз. З огляду на це, формування правових, організаційних та інституційних механізмів забезпечення контррозвідувального режиму на об’єктах державної авіації вимагає наукового обґрунтування, комплексного аналізу поточного стану справ, вивчення міжнародного досвіду, передусім стандартів НАТО, а також розробки пропозицій щодо нормативного врегулювання, побудови вертикалі управління, цифрової трансформації моніторингу загроз та формування культури контррозвідувальної обізнаності.

Таким чином, обрана тема має як теоретичну значущість — у контексті розвитку національної системи безпеки, так і прикладну — з огляду на необхідність впровадження нових підходів до захисту критичної інфраструктури державної авіації в умовах війни та майбутньої євроатлантичної інтеграції України.

Об’єкт і предмет дослідження є об’єкти державної авіації як елемент системи забезпечення національної безпеки та оборони України.

Предметом дослідження виступають правові та організаційні засади забезпечення контррозвідувального режиму на зазначених об’єктах в умовах гібридних загроз та євроатлантичної інтеграції.

Метою дослідження є комплексне дослідження сучасного стану, нормативно-правових основ, міжнародного досвіду, а також комплексне наукове обґрунтування та розроблення пропозицій щодо вдосконалення правових і організаційних засад функціонування контррозвідувального режиму на об’єктах державної авіації України з урахуванням сучасних викликів та міжнародного досвіду.

Дослідницькі завдання. Для досягнення мети дослідження передбачено виконання таких завдань:

1. провести аналіз чинної нормативно-правової бази у сфері авіаційної безпеки та контррозвідки;

2. визначити інституційну структуру та існуючі механізми взаємодії між суб’єктами забезпечення контррозвідувального режиму;

3. ідентифікувати ключові вразливості об’єктів державної авіації до диверсійних, технічних та інформаційних загроз;

4. здійснити порівняльний аналіз практик країн-членів НАТО, зокрема США, у сфері організації авіаційної безпеки та контррозвідувального забезпечення;

5. розробити комплекс рекомендацій щодо удосконалення системи управління, нормативного регулювання, кадрового потенціалу та цифрової трансформації механізмів забезпечення контррозвідувального режиму.

Джерельна база дослідження. У процесі дослідження використано комплекс джерел, що включає:

– нормативно-правові акти України (Конституція України, Повітряний кодекс, закони «Про контррозвідувальну діяльність», «Про національну безпеку» тощо);

– стратегічні документи (укази Президента, концепції, державні програми);

– нормативно-інструктивні матеріали Міністерства оборони України, Служби безпеки України, Державної авіційної служби України, Головного управління державної авіації);

– міжнародні джерела (ICAO Annex 17, Doc 8973, регламенти ЄС, STANAGs, доктрини НАТО AJP-2.2, AJP-3.14);

– наукові публікації, аналітичні огляди, практичні кейси з безпеки інфраструктури;

– прикладні дослідження українських і закордонних фахівців у сфері авіаційної безпеки, військової контррозвідки, кібербезпеки та ризик-менеджменту.

Методи дослідження. Методологічну основу роботи становлять загальнонаукові та спеціальні методи пізнання:

формально-юридичний метод — для аналізу норм права, що регулюють контррозвідувальну діяльність в авіаційній сфері;

системно-структурний підхід — для виявлення взаємозв'язків між елементами режиму безпеки;

порівняльно-правовий аналіз — для порівняння національного законодавства зі стандартами НАТО та ІСАО;

логіко-аналітичний метод — для узагальнення емпіричних спостережень та формулювання практичних висновків;

елементи кейс-аналізу — для вивчення окремих прикладів порушень або ефективних практик у сфері захисту авіаційних об'єктів.

Структура дослідження. Магістерська робота складається зі вступу, чотирьох розділів, висновків до кожного з них, загальних висновків, списку використаних джерел.

- У вступі обґрунтовано актуальність теми, визначено об'єкт, предмет, мету та завдання дослідження, охарактеризовано його джерельну базу, наукову новизну, методологічний інструментарій та структуру.
- Розділ 1 присвячений теоретико-правовим засадам організації контррозвідувального режиму на об'єктах авіаційної інфраструктури. В межах розділу досліджено понятійний апарат, проаналізовано національне законодавство, а також міжнародні нормативні джерела (зокрема, документи НАТО та ІСАО), які формують доктринальне підґрунтя для імплементації сучасних стандартів безпеки.
- Розділ 2 містить комплексний аналіз чинного стану нормативно-організаційного забезпечення контррозвідувального режиму в державній авіації України. Розглянуто інституційну структуру, нормативні прогалини, практику міжвідомчої взаємодії, а також типологію основних загроз і вразливостей у сучасних умовах воєнного стану.
- Розділ 3 присвячений вивченню практичних підходів країн-членів НАТО до організації контррозвідувального режиму, з фокусом на досвід Сполучених Штатів Америки. На підставі аналізу стратегій та

інструктивних документів запропоновано можливі напрямки адаптації зазначених практик до українських реалій.

- Розділ 4 розробляє цілісну модель удосконалення правових та організаційних механізмів забезпечення контррозвідувального режиму в державній авіації. Запропоновано концепцію інституційної вертикалі, шляхи нормативної гармонізації з міжнародними стандартами, системи управління ризиками, цифрові рішення моніторингу, кадрову політику, етапи впровадження та індикатори ефективності.
- У висновках до кожного розділу підсумовано результати дослідження, сформульовано практичні рекомендації та визначено вектори подальших наукових пошуків.
- У загальних висновках представлено синтетичне узагальнення результатів дослідження, оцінено потенціал реалізації запропонованих заходів у межах державної політики безпеки та окреслено перспективи інтеграції в євроатлантичну безпекову систему.

РОЗДІЛ 1. ТЕОРЕТИКО – ПРАВОВІ ЗАСАДИ КОНТРРОЗВІДУВАЛЬНОГО РЕЖИМУ НА ОБ'ЄКТАХ ДЕРЖАВНОЇ АВІАЦІЇ

1.1. Державна авіація як складова сектору безпеки і оборони: поняття, об'єкти, система управління

Державна авіація України становить окремий підсектор авіаційної діяльності, який функціонує в межах сектору безпеки і оборони держави та призначений для забезпечення національної безпеки, обороноздатності, охорони громадського порядку, реагування на надзвичайні ситуації та виконання інших спеціальних завдань, покладених на уповноважені державні органи. Згідно з положеннями Повітряного кодексу України, авіація поділяється на цивільну та державну, при цьому "державною авіацією" визначено авіацію, що використовує повітряні судна з метою виконання функцій із забезпечення національної безпеки і оборони держави та захисту населення, які покладаються на Збройні Сили України, інші військові формування, утворені відповідно до законів України, Міністерство внутрішніх справ України, Національну поліцію України, Службу безпеки України, центральний орган виконавчої влади, що реалізує державну політику у сфері цивільного захисту, органи охорони державного кордону України, митні органи [1].

У контексті національного законодавства державна авіація виконує функції, які не притаманні цивільному повітряному транспортові, — передусім це завдання оборонного, правоохоронного та спеціального характеру. Відтак, державна авіація є специфічним функціональним елементом системи національної безпеки, який потребує особливого нормативного регулювання, включаючи питання допуску до польотів, експлуатації повітряного простору, технічного обслуговування, зберігання боєприпасів, інженерного захисту, інформаційної безпеки тощо.

Об’єктами державної авіації, з точки зору безпеки та оборони, є не лише повітряні судна, але й відповідна інфраструктура: аеродроми, вертодроми (військові, спільного використання), авіаційні бази, інженерно-авіаційні склади, злітно-посадкові смуги, командно-диспетчерські пункти, пункти бойового управління, сховища та склади авіаційних боєприпасів, технічні парки та ремонтні підрозділи [2]. З урахуванням міжнародної практики, особливо стандартів НАТО, які орієнтовані на авіацію Збройних Сил країн-членів[1], до об’єктів державної авіації також слід зараховувати інформаційно-комунікаційні системи управління польотами, об’єкти радіолокації, об’єкти енергозабезпечення, транспортно-логістична інфраструктура, а також персонал, допущений до роботи з критично важливими елементами безпеки [3,4].

Система управління державною авіацією України має багаторівневу структуру. На рівні формування державної політики та нормативного регулювання провідну роль відіграє Кабінет Міністрів України, який забезпечує реалізацію державної політики у сфері авіації. Координацію та міжвідомчу взаємодію на стратегічному рівні забезпечує Міністерство оборони України через делегування повноважень до Головного управління державної авіації України (ГУДАУ), яке виконує завдання з розробки політики, регламентації, нагляду та гармонізації діяльності державної авіації відповідно до національних інтересів та міжнародних зобов’язань України, а також завдань визначених статтею 7 Повітряного кодексу України[2]. Не зважаючи на ключову роль

[1] Слід зазначити, що стандарти НАТО застосовуються до авіації Збройних Сил країн-членів і не охоплюють інші авіаційні формування. В Україні ж “державна авіація” включає не лише авіацію Збройних Сил, а й авіацію інших ЦОВВ, тому положення документів НАТО у подальшому розглядатимуться з урахуванням національної специфіки.

[2] Відповідно до статті 7 Повітряного кодексу України Міністерство оборони України регулює питання державної авіації в частині реєстрації та допуску державних повітряних суден та літальних апаратів, аеродромів та злітно-посадкових майданчиків, підтримання льотної придатності державних повітряних суден, допуску авіаційного персоналу до виконання польотів та проведення робіт із забезпечення польотів, охорони повітряних суден, виконання та забезпечення польотів, пошуку та рятування, випробування та прийняття в експлуатацію нових типів повітряних суден, призначених для використання в державній авіації, та здійснює нормативно-правове регулювання зазначених питань за погодженням із заінтересованими центральними органами виконавчої влади, які експлуатують державні повітряні судна. Окрім цього, якщо розробник, виробник не виконує своїх обов'язків із супроводження експлуатації виробів авіаційної техніки, компонентів та обладнання, підтримання їх льотної придатності, Міністерство оборони України вживає необхідних заходів для забезпечення безпеки польотів та підтримання льотної придатності державних повітряних суден шляхом заборони експлуатації екземплярів або типу виробів авіаційної техніки, компонентів та обладнання, прийняття відповідальності на себе за виконання вищезазначених функцій, визначення відповідальної організації за виконання таких функцій.

Головного управління державної авіації України, як уповноваженого органу Міністерства оборони України з питань державної авіації, до його компетенції не входять питання охорони об'єктів державної авіації (виключно охорона повітряних суден). В той час як питання авіаційної безпеки ключовий напрямок діяльності Державної авіаційної служби України, що за своїм призначенням є органом авіаційної влади для цивільної авіації (аналогічний ГУДАУ). Безпосереднє керівництво діяльністю у сфері державної авіації здійснюють відповідні міністерства і відомства, до складу яких входять авіаційні формування, — насамперед Міністерство оборони України, Міністерство внутрішніх справ України, Служба безпеки України [1].

Таким чином, державна авіація становить складну функціональну систему, інтегровану в архітектуру сектору безпеки і оборони держави, яка вимагає особливого режиму охорони, контролю доступу та контррозвідувального забезпечення. Її об'єкти потребують системного правового регулювання та захисту, з огляду на високий ступінь загроз з боку диверсійно-розвідувальних структур, кіберінструментів і засобів технічної розвідки, що використовуються в умовах гібридної війни.

1.2. Поняття та правова природа контррозвідувального режиму в Україні

Поняття "контррозвідувальний режим" не має чіткого визначення у чинному законодавстві України. Ні Закон України "Про контррозвідувальну діяльність", ні інші нормативно-правові акти спеціального характеру не містять юридичного тлумачення цього терміну. Водночас його застосування фіксується на рівні стратегічних документів, затверджених актами Президента України[3].

[3]Указ Президента України №310/2017 "Про рішення Ради національної безпеки і оборони України від 13 вересня 2017 року "Про Концепцію забезпечення контррозвідувального режиму в Україні";
Указ Президента України №56/2022 "Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про Стратегію забезпечення державної безпеки".

Крім того, відповідне поняття трапляється в аналітичних та наукових дослідженнях, присвячених питанням забезпечення національної безпеки.

Наукове тлумачення контррозвідувального режиму подається як системне поняття, що охоплює сукупність спеціальних адміністративно-правових, організаційних та технічних заходів, які забезпечують унеможливлення або ускладнення розвідувально-підривної діяльності іноземних спецслужб, захист від внутрішніх загроз, а також сприяють реалізації функцій держави у сфері безпеки.

З правової точки зору контррозвідувальний режим може бути кваліфікований як особливий правовий режим, що встановлює спеціальні правила поведінки, обмеження і зобов'язання в окремих сферах суспільних відносин. Його правова природа виявляється у взаємодії дозволів, заборон і зобов'язань, які закріплюються нормативними актами або внутрішньовідомчими документами органів безпеки та оборони. За змістом він є одним із підвидів режиму забезпечення державної безпеки [3].

Контррозвідувальний режим має комплексну структуру. Він включає елементи таких режимів, як: режим охорони державної таємниці, режим охорони державного кордону, прикордонний режим, режим виїзду з України та в'їзду в Україну, внутрішньо-об'єктовий режим, митний режим, режим внутрішньої безпеки, паспортний режим, режим перебування іноземців в Україні, режим користування повітряним транспортом, пропускний режим, режим надзвичайного стану в Україні, режим радіоелектронної безпеки тощо [7].

Його функціонування передбачає впровадження організаційно-правових заходів на об'єктах, що мають стратегічне або оборонне значення, включаючи об'єкти державної авіації. Контррозвідувальний режим охоплює як статичну складову (правові норми, що регулюють порядок діяльності), так і динамічну складову (безпосереднє застосування режимних заходів Службою безпеки України та іншими суб'єктами сектора безпеки).

Впровадження контррозвідувального режиму покликане забезпечити: боротьбу з розвідувально-підривною діяльністю іноземних спецслужб,

запобігання терористичним та диверсійним загрозам, захист критичної інфраструктури, удосконалення механізмів інформаційної безпеки. Ця система спрямована не лише на реагування на загрози, а й на усунення передумов для їх виникнення [6]. Контррозвідувальний режим є не лише результатом законодавчого процесу, але й продуктом стратегічного аналізу загроз, який трансформується у конкретні профілактичні, оперативно-розшукові, технічні й інформаційно-аналітичні заходи. Його структура включає як загальнонаціональні, так і локальні (об'єктові) рівні реалізації. Загальнонаціональний рівень визначається базовими законами України — зокрема, Законом України "Про контррозвідувальну діяльність", Законом України "Про Службу безпеки України", Законом України "Про державну таємницю", Конституцією України, міжнародними договорами, ратифікованими Україною, а також указами Президента України та постановами Кабінету Міністрів. На локальному рівні контррозвідувальний режим реалізується через систему наказів, інструкцій, розпоряджень відомств і адміністрацій відповідних об'єктів (підзаконних актів).

У контексті об'єктів державної авіації контррозвідувальний режим має свою специфіку. По-перше, він охоплює захист об'єктів, які поєднують як військову, так і інфраструктурну (транспортну, енергетичну, комунікаційну) цінність. По-друге, на таких об'єктах функціонують особливі процедури доступу, охорони, технічного нагляду та інформаційної ізоляції. По-третє, ці об'єкти часто є цілями для технічної, агентурної та кіберрозвідки з боку противника, що вимагає високого рівня уніфікації правового режиму з національними та міжнародними стандартами.

Таким чином, хоча поняття контррозвідувального режиму й не закріплене в законодавстві, його активне використання на рівні стратегічного управління національною безпекою та в науковому дискурсі свідчить про формування відповідної правової доктрини. Необхідним кроком є подальше закріплення поняття на рівні закону з визначенням принципів, суб'єктів, повноважень і процедур реалізації цього режиму в контексті національної системи безпеки.

1.3. Нормативно-правові основи організації безпеки та контррозвідки в авіації: військовий та цивільний компоненти

Система забезпечення безпеки в авіаційній сфері України регламентується широким колом нормативно-правових актів, що охоплюють як військовий, так і цивільний компоненти авіації. Ці компоненти функціонують на підставі різних нормативних підходів, проте мають спільну мету — захист державної безпеки, попередження актів незаконного втручання та забезпечення безперервності авіаційної діяльності.

У військовому сегменті правову основу становлять положення Кримінального кодексу України, Кодексу України про адміністративні правопорушення, а також галузеві нормативні акти, що регулюють захист об'єктів державної авіації, допуск до інформації з обмеженим доступом, охорону державної таємниці та контррозвідувальні заходи в межах відповідальності Збройних Сил України, Служби безпеки України, інших військових формувань, утворених відповідно до Законів України тощо. Особливе значення мають Укази Президента України № 310/2017 та № 56/2022, що закріплюють Концепцію забезпечення контррозвідувального режиму і Стратегію забезпечення державної безпеки відповідно [6, 8].

У цивільному авіаційному секторі безпекові та контррозвідувальні питання регулюються, перш за все, Повітряним кодексом України та Законом України "Про Державну програму авіаційної безпеки цивільної авіації". На підзаконному рівні функціонує ціла система актів: постанови Кабінету Міністрів України, накази, видані уповноваженими органами, зокрема Міністерством розвитку громад, територій та інфраструктури України[4], Державної авіаційної

[4] З 2 грудня 2022 року Міністерство інфраструктури України реорганізоване шляхом приєднання до нього Міністерства розвитку громад та територій України, з утворенням Міністерства розвитку громад, територій та інфраструктури України. Зміни здійснено відповідно до постанови Кабінету Міністрів України від 02.12.2022 № 1343 "Деякі питання оптимізації системи центральних органів виконавчої влади", [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1343-2022-п.

служби України, Служби безпеки України, Міністерства внутрішніх справ України (включно з Національною поліцією України), а також документи, що визначають порядок сертифікації суб’єктів авіаційної діяльності, проведення розслідувань авіаційних подій, контроль доступу до об'єктів, охорону повітряних суден, порядок реагування екіпажу на надзвичайні ситуації тощо.

На міжнародному рівні ключову роль відіграють положення Конвенції Міжнародної організації цивільної авіації (ICAO) (Чиказької, Токійської, Гаазької, Монреальської), додатки до Конвенції про міжнародну цивільну авіацію, зокрема Додаток 17 ICAO та Додаток 19 ICAO, а також відповідні керівництва (ICAO Docs 8973, 10118, 10084, 9807, 9808 тощо), що встановлюють глобальні стандарти та практики у сфері авіаційної безпеки.

Військовий компонент системи забезпечення безпеки в авіаційній сфері України здебільшого ґрунтується на стандартах НАТО, однак його застосування обмежується виключно авіаційними підрозділами Збройних Сил України, які є складовою державної авіації. Водночас, як було зазначено в підпункті 1.2 розділу 1 цієї роботи, на локальному рівні реалізація контррозвідувального режиму здійснюється шляхом впровадження системи відомчих нормативно-правових актів (наказів, інструкцій, розпоряджень), виданих органами управління відповідних об’єктів. Такий підхід обумовлює існування варіативності у використанні механізмів правового регулювання, зокрема застосування різних процедур, інструментів і методик у сфері забезпечення безпеки.

Досвід країн - членів НАТО свідчить про доцільність застосування у сфері забезпечення контррозвідувального режиму об’єктів державної авіації принципів та підходів, що закладені у документах цивільної авіації, зокрема у стандартах та рекомендованих практиках ICAO, а також у відповідному законодавстві Європейського Союзу (Регламент ЄС № 300/2008 тощо) [9]. Такий підхід сприяє уніфікації методів, гармонізації процедур та забезпеченню взаємосумісності в рамках міжвідомчої і міжнародної взаємодії, однак не

виключає адаптації до національних умов і специфіки правового середовища кожної держави.

Таким чином, нормативно-правове забезпечення авіаційної безпеки в Україні має розгалужену структуру та охоплює як внутрішньодержавні положення, так і міжнародні зобов'язання. Умовна інтеграція контррозвідувальних заходів у системи авіаційної безпеки як у військовому, так і цивільному сегментах є ключовою умовою для формування єдиної концепції забезпечення стійкості до гібридних загроз у повітряному просторі держави[5].

1.4. Вплив стандартів та рекомендованих практик ICAO на формування системи охорони та безпеки в авіаційній сфері, включаючи військову

Міжнародна організація цивільної авіації (ICAO) відіграє ключову роль у формуванні глобальної політики у сфері авіаційної безпеки. Її нормативні документи — зокрема Додатки 17 та 19 до Конвенції про міжнародну цивільну авіацію (Чиказької конвенції), а також Посібник з авіаційної безпеки (ICAO Doc 8973) — формують нормативно-правову основу для забезпечення авіаційної безпеки на міжнародному рівні. У вказаних документах закладено принципи управління ризиками, реагування на загрози, захисту об'єктів цивільної авіації від актів незаконного втручання, а також організацію доступу, охорони, моніторингу та розслідувань подій [10, 11, 12].

Ці стандарти ICAO були імплементовані в національне законодавство України, зокрема в Закон України "Про Державну програму авіаційної безпеки цивільної авіації" [13]. Вказаний закон встановлює структуру відповідальних органів, систему сертифікації, міжвідомчу координацію, контроль доступу до

[5] Зокрема див.: Постанова Кабінету Міністрів України від 6 грудня 2017 р. № 954 "Про затвердження Положення про використання повітряного простору України", [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/954-2017-п#n12.

об’єктів та заходи реагування на загрози, що безпосередньо корелює з положеннями Додатком17 ІСАО. Таким чином, норми ІСАО стали основою для побудови національної системи авіаційної безпеки в цивільному секторі.

У військовій сфері питання охорони об’єктів державної авіації[6] врегульовано наказом Міністерства оборони України від 21.03.2016 №152, яким затверджено Порядок організації охорони об’єктів державної авіації. Цей документ визначає базові вимоги до охорони повітряних суден, аеродромів, будівель, інженерних споруд, а також встановлює порядок несення служби, обліку та зберігання зброї, доступу та протидії несанкціонованому зльоту. Його положення, безумовно, становлять основу фізичного захисту військових авіаційних об’єктів, однак документ є замкненим у відомчому правовому полі та не враховує низку ключових положень міжнародних безпекових стандартів.

Зокрема, наказ Міністерства оборони України від 21.03.2016 № 152 не містить прямих посилань на стандарти ІСАО чи документи НАТО (AJP-3.14[7], STANAG 3117 тощо). Він не включає положення щодо аналізу загроз, управління ризиками, технологічного моніторингу, а також не закріплює ролі контррозвідки як складової безпеки — на відміну від Спільної доктрини НАТО – AJP-3.14, у якій контррозвідувальні заходи прямо визначаються як елемент захисту сил.

Більше того, у порівнянні з цивільною програмою безпеки, зазначений наказ не встановлює інституційного механізму міжвідомчої координації, чіткого розподілу обов’язків або процедури взаємодії між органами управління. У цьому контексті наказ залишається фрагментарним щодо інтеграції з євроатлантичними підходами до охорони об’єктів. Окрім цього на підставі цього

[6] Охорона об’єктів державної авіації - діяльність з організації та практичного здійснення заходів охорони, спрямованих на забезпечення недоторканності, цілісності державних повітряних суден (далі - ДПС), будівель, споруд, територій та іншого рухомого і нерухомого майна аеродромів державної авіації з метою запобігання та (або) недопущення чи припинення протиправних дій щодо них, збереження їх належного стану, припинення несанкціонованого використання та доступу до них сторонніх осіб, забезпечення бойової готовності (готовності до виконання завдань за призначенням) авіаційних частин.

[7] NATO STANDARD Allied Joint Publication-3.14 (AJP-3.14) Allied Joint Doctrine for Force Protection.

наказу, з урахуванням організаційної структури, специфіки завдань, які покладаються на підпорядковані авіаційні частини, органи управління авіації центральних органів виконавчої влади та органи управління авіації Збройних Сил України розробляють власні інструкції з охорони об'єктів державної авіації, що затверджуються наказами їх керівників, що в свою чергу призводить до використання різних підходів та механізмів для реалізації охорони об'єктів державної авіації, як це зазначалось у підрозділі 1.1 розділу 1.

Водночас, як свідчить практика країн — членів НАТО, ефективне забезпечення безпеки державної авіації, особливо в умовах гібридних загроз, передбачає застосування комплексного підходу, що поєднує як військові, так і цивільні стандарти. Зокрема, європейське законодавство (Регламент ЄС № 300/2008) [9] та стандарти ІСАО широко використовуються в державних структурах країн Альянсу не лише у цивільній, а й у військовій авіації — у частині процедур доступу, управління інцидентами, сертифікації безпекових служб тощо. Такий підхід забезпечує уніфікацію процедур, гармонізацію законодавства та підвищення взаємосумісності між союзниками.

З огляду на зазначене, можна констатувати: хоча наказ Міністерства оборони України від 21.03.2016 № 152 створює національну базу охорони авіаційних об'єктів, він не забезпечує повної відповідності стандартам ІСАО і НАТО (Таблиця 1). Його вдосконалення має здійснюватися шляхом адаптації до міжнародних підходів, розширення функціоналу безпеки за рахунок елементів контррозвідки, ризик-менеджменту та міжвідомчої інтеграції.

Критерій / Елемент	**ICAO Додаток 17 / Doc 8973**	**NATO AJP-3.14 / інші військові стандарти**	**Наказ МОУ від 21.03.2016 №152**
Управління ризиками	Визначено як обов'язковий компонент системи безпеки.	Частина оцінки загроз, формування Плану реагування на загрозу, інцидент або надзвичайну ситуацію (Response Plan).	Не передбачено.
Контроль доступу до об'єктів	Обов'язкові вимоги до перевірки, контролю та верифікації.	Включає фізичний, електронний контроль, ідентифікацію осіб.	Передбачено патрулювання, допуск згідно списків.
Захист об'єктів від актів незаконного втручання	Основна мета стандарту.	Включено до завдань захисту сил (Force Protection).	Формально передбачено, але без аналізу загроз.
Використання технічних засобів охорони	Камери, тривожні системи, сканери.	Системи виявлення, оповіщення, обмеження доступу.	Відсутня згадка про сучасні технічні засоби.
Міжвідомча координація	Зазначено обов'язкову взаємодію з іншими органами.	Обов'язкова взаємодія між військами, контррозвідкою, цивільними.	Не передбачено.
Контррозвідувальні заходи	Не є основним предметом регулювання, але елемент превентивних заходів безпеки.	Визначено як обов'язкова складова (AJP-2, DoD 5240.6).	Не передбачено.
Розподіл відповідальності	Детально регламентовано програмою авіабезпеки.	Є поділ між командирами, силами безпеки, контррозвідкою.	Частково регламентовано (посадові обов'язки).
Навчання і сертифікація персоналу охорони	Обов'язкові тренінги, вимоги до компетентності.	Військова підготовка + спеціальні брифінги з контррозвідкою.	Відсутнє.
Впровадження стандартів ICAO/NATO	Вихідна точка для розробки національних програм.	Стандарти НАТО адаптують стандарти ICAO з урахуванням військових завдань.	Відсутнє посилання на ICAO або НАТО.
Гнучкість / адаптація до загроз (Threat-Based Planning)	Передбачено адаптацію заходів залежно від ризику.	Основа оперативного планування в НАТО.	Статичний підхід, без врахування сценаріїв загроз.

Таблиця 1. Порівняння ключових положень міжнародних та національних стандартів у сфері авіаційної безпеки

ВИСНОВКИ ДО РОЗДІЛУ 1

У результаті проведеного теоретико-правового аналізу контррозвідувального режиму на об’єктах державної авіації можна зробити такі узагальнення:

1. Державна авіація України є структурним компонентом сектору безпеки і оборони держави, що має спеціальне функціональне призначення — забезпечення національної безпеки, обороноздатності та реагування на надзвичайні ситуації. Її об’єктами виступають не лише повітряні судна, а й складна інфраструктура, яка потребує системної охорони, технічного захисту та контррозвідувального забезпечення.

2. Поняття “контррозвідувальний режим”, хоч і не закріплене в чинному законодавстві України, має сформовану наукову інтерпретацію як комплекс спеціальних адміністративно-правових, технічних і організаційних заходів, спрямованих на виявлення, попередження та нейтралізацію розвідувально-підривної діяльності проти держави. Його впровадження є невід’ємною складовою гарантування безпеки об’єктів критичної інфраструктури, включаючи авіаційні об’єкти.

3. Нормативно-правове забезпечення контррозвідувального режиму в авіації в Україні ґрунтується на поєднанні військових і цивільних джерел права. У військовому сегменті превалює внутрішньовідомче нормативне регулювання, у той час як у цивільному — впроваджені міжнародні стандарти ІСАО, які стали основою національної програми авіаційної безпеки. Водночас спостерігається фрагментація регуляторної бази, недостатня гармонізація між цивільними та військовими підходами, що створює ризики в контексті міжвідомчої взаємодії.

4. Стандарти та рекомендовані практики ІСАО (особливо Додатки 17 і 19, Doc 8973) вже імплементовані в цивільний авіаційний сектор України, проте їх застосування у сфері державної авіації є обмеженим. Наказ МОУ № 152 не інтегрує підходи ІСАО або НАТО щодо управління ризиками, кіберзахисту,

аналізу загроз і контррозвідувальної діяльності, що істотно знижує його відповідність сучасним викликам.

5. Практика країн НАТО демонструє доцільність поєднання цивільних і військових авіаційних стандартів в умовах гібридних загроз. Це дозволяє підвищити стійкість авіаційної інфраструктури до диверсій, шпигунства, кіберзагроз і несанкціонованого доступу. Такий підхід вимагає адаптації чинного законодавства України та оновлення існуючих нормативних актів, зокрема щодо організації охорони об’єктів державної авіації.

Таким чином, забезпечення контррозвідувального режиму на об’єктах державної авіації України потребує доктринального переосмислення, оновлення нормативної бази та імплементації кращих практик, що використовуються країнами-членами НАТО й міжнародними авіаційними організаціями, з метою формування єдиної системи авіаційної безпеки, стійкої до сучасних загроз.

РОЗДІЛ 2. СТАН І ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КОНТРРОЗВІДУВАЛЬНОГО РЕЖИМУ НА ОБ'ЄКТАХ ДЕРЖАВНОЇ АВІАЦІЇ В УКРАЇНІ

2.1. Організаційна структура суб'єктів контррозвідувального забезпечення в авіаційній сфері

Забезпечення контррозвідувального режиму в авіаційній сфері України є складовою загальнодержавної системи національної безпеки, що реалізується через чітко визначений інституційний механізм. Правове підґрунтя діяльності відповідних суб'єктів визначається низкою нормативно-правових актів, серед яких ключове місце посідає Закон України "Про контррозвідувальну діяльність". Згідно з цим законом, провідним органом у сфері контррозвідки виступає Служба безпеки України, яка несе відповідальність за виявлення, запобігання та нейтралізацію розвідувально-підривної діяльності іноземних спецслужб, захист об'єктів критичної інфраструктури, зокрема тих, що належать до авіаційного сектору [16].

Поряд з цим, у межах сектору оборони функції контррозвідувального забезпечення об'єктів державної авіації здійснюються спеціалізованими підрозділами Служби безпеки України, насамперед підрозділами Департаменту військової контррозвідки, що діють у взаємодії з командуваннями Збройних Сил України та інших військових формувань, утворених відповідно до Законів України. Вони відповідають за організацію та реалізацію заходів із захисту авіаційних частин, аеродромів, пунктів управління та інших об'єктів, що мають стратегічне значення. У цьому контексті до їх функціональних обов'язків належить виявлення і нейтралізація диверсійних та агентурних загроз, запобігання витоку інформації з обмеженим доступом, протидія технічній розвідці, фільтраційна робота з персоналом, а також оперативний моніторинг безпекової ситуації в умовах дії правового режиму воєнного стану. Реалізація зазначених завдань відбувається у взаємодії з підрозділами Військової служби

правопорядку та органами військового управління авіації Збройних Сил України, що забезпечує комплексний характер контррозвідувального захисту в авіаційній сфері.

У сфері цивільної авіації формування системи безпеки ґрунтується на положеннях Повітряного кодексу України, Закону України "Про Державну програму авіаційної безпеки цивільної авіації", постанові Кабінету Міністрів України від 26.06.2019 № 550 "Про затвердження Порядку взаємодії Державної авіаційної служби з правоохоронними органами з питань забезпечення безпеки цивільної авіації"[8]. Організаційним центром реалізації політики авіаційної безпеки виступає Державна авіаційна служба України, яка забезпечує нормативне регулювання, контроль за впровадженням стандартів ІСАО, сертифікацію служб авіаційної безпеки суб'єктів авіаційної діяльності, а також моніторинг рівня загроз. Крім того, до реалізації безпекових заходів у цивільній авіації залучаються Національна поліція, Державна прикордонна служба, підрозділи Національної гвардії України та Служба безпеки України тощо, як зокрема зазначено в постанові Кабінету Міністрів України від 09.06.2021 № 594 "Деякі питання Міжвідомчої комісії з авіаційної безпеки цивільної авіації", що формує багатовекторну систему контролю і протидії ризикам.

У рамках як військової, так і цивільної підсистем, функціонують внутрішньовідомчі структури безпеки, які діють на основі наказів, інструкцій і положень відповідних міністерств та відомств. Наприклад, у військовому секторі застосовується наказ Міністерства оборони України №152 від 21.03.2016, що визначає порядок організації охорони об'єктів державної авіації. Документ встановлює правила фізичної охорони територій, розподіл функцій між підрозділами, протоколи реагування на загрози та особливості пропускного режиму. Разом з тим, цей акт не містить системних положень щодо інтеграції

[8] Постанова КМУ від 26.06.2019 № 550 визначає організацію взаємного інформування, планування і проведення спільних заходів щодо виявлення, припинення і попередження правопорушень у галузі цивільної авіації, надання допомоги правоохоронними органами державним інспекторам та особам, уповноваженим на проведення перевірок, у виконанні ними службових обов'язків щодо інспектування і перевірок та припинення незаконних дій осіб, які перешкоджають виконанню зазначених обов'язків.

контррозвідувальних заходів, чим обумовлена необхідність його вдосконалення у відповідності до міжнародних стандартів, як зазначалось в розділі 1 цієї роботи.

Варто зазначити, що ефективність реалізації контррозвідувальних заходів значною мірою залежить від міжвідомчої взаємодії. У поточній моделі взаємодії державних структур спостерігається як формалізована координація на рівні Ради національної безпеки та оборони України, так і практична співпраця в межах реалізації програм авіаційної безпеки, організації спільних навчань, обміну розвідувальною інформацією. Проте аналіз функціональної взаємодії демонструє наявність певної фрагментарності у розподілі відповідальності, що може призводити до дублювання повноважень або, навпаки, до утворення прогалин у системі захисту.

Отже, організаційна структура суб'єктів контррозвідувального забезпечення в авіаційній сфері України характеризується високим рівнем інституційної складності та багаторівневою природою. Її ефективне функціонування потребує чіткої нормативної регламентації, постійної координації між задіяними відомствами та адаптації до змін у зовнішньому безпековому середовищі. Водночас, інтеграція національного досвіду в рамки міжнародної практики, зокрема через урахування стандартів НАТО та ІСАО, є передумовою формування цілісної та взаємосумісної системи авіаційної безпеки, як з країнами-членами так і під час використання аеродромів подвійного призначення.

2.2. Оцінка чинного законодавства України у сфері авіаційної безпеки й контррозвідувального режиму

Нормативно-правове регулювання авіаційної безпеки в Україні характеризується подвійною структурою, що розділяє підходи до цивільної та державної авіації. У сегменті цивільної авіації законодавство демонструє помітну орієнтацію на міжнародні стандарти та рекомендовані практики, передусім Міжнародної організації цивільної авіації (ІСАО) та правових актів

Європейського Союзу. Україна, як договірна держава ІСАО, імплементувала ключові положення Конвенції про міжнародну цивільну авіацію (Чиказької конвенції), включаючи Додатки 17 та 19, у національні нормативно-правові акти. Це стосується, зокрема, Державної програми авіаційної безпеки, системи управління ризиками, процедур контролю доступу, сертифікації служб авіаційної безпеки, а також підготовки та підвищення кваліфікації персоналу, відповідального за реалізацію безпекових заходів.

Натомість державна авіація, яка охоплює авіаційні компоненти Збройних Сил України, Національної поліції України Національної гвардії України, Державної прикордонної служби України, Служби безпеки України, Державної служби з надзвичайних ситуацій та інших військових формувань, утворених відповідно до Законів України, функціонує на основі фрагментованої нормативної бази, що значною мірою відокремлена від цивільної парадигми безпеки. У чинному законодавстві відсутнє єдине положення, яке б регламентувало уніфіковані підходи до забезпечення авіаційної безпеки на об'єктах державної авіації. Також не існує повноцінної інтеграції з міжнародними безпековими стандартами, що позбавляє національну систему гнучкості та взаємосумісності в умовах багатонаціональних операцій чи переходу до стандартів НАТО.

Окремо варто наголосити, що чинне законодавство України не містить повноцінного нормативного визначення контррозвідувального режиму, який, згідно з міжнародною практикою, є одним із ключових елементів забезпечення національної безпеки, особливо в секторах, пов’язаних з інфраструктурою подвійного призначення. Єдиними документами, який офіційно закріплює поняття “контррозвідувальний режим”, залишається Указ Президента України № 310/2017, що вводить у дію рішення Ради національної безпеки і оборони України “Про Концепцію забезпечення контррозвідувального режиму в Україні” та Указ Президента України № 56/2022 “Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року “Про стратегію забезпечення державної безпеки”. Ці документи, однак, мають переважно стратегічний і

політичний характер, і не створюють детальної нормативно-правової рамки для практичної реалізації відповідних заходів у конкретних секторах, зокрема в авіаційній галузі.

У правовому полі авіаційної безпеки цивільного спрямування міститься низка спеціалізованих актів, які визначають механізми оцінки загроз, взаємодії між суб'єктами авіаційної безпеки та силовими структурами, охорони повітряних суден та об'єктів інфраструктури, здійснення контролю на безпеку тощо. Такі положення, за формою і змістом, частково відповідають положенням Додатку 17 ІСАО і європейських регламентів, зокрема Регламенту ЄС № 300/2008. Однак подібних уніфікованих нормативів у державному авіаційному сегменті не існує.

Ще однією критичною прогалиною є недостатній рівень нормативної координації між органами, відповідальними за реалізацію контррозвідувального забезпечення (Службою безпеки України), і тими, хто відповідальний за впровадження стандартів НАТО у секторі оборони (Міністерство оборони України). Згідно з доктринальними документами НАТО, зокрема Спільною доктриною НАТО AJP-2.2 (Counterintelligence)[9], контррозвідувальні заходи мають становити інтегральну частину будь-якої концепції захисту критичної інфраструктури, включаючи об'єкти державної авіації. В українському ж контексті ця доктрина не лише не імплементована, але й не визнана на нормативному рівні, що свідчить про розрив між доктринальною рамкою НАТО та чинним українським законодавством.

Водночас положення вищезгаданої доктрини НАТО, так само як і підходи, зафіксовані в AJP-3.14 (Joint Doctrine for Force Protection), містять конкретні рекомендації щодо поєднання фізичних, інформаційних, інженерних та

[9] Див. Перелік чинних стандартів НАТО, передбачених Цілями партнерства, що прийняті в Міністерстві оборони України, Збройних Силах України та інших складових сектору безпеки і оборони: AJP-2.2 «Allied Joint Doctrine for Counter-Intelligence and Security Procedures» серед впроваджених документів відсутня, що свідчить про її неадаптованість у національну нормативно-правову базу на момент публікації. URL: https://mod.gov.ua/diyalnist/normativno-pravova-baza/perelik-standartiv-nato-ta-standartiv-u-sferi-oboroni-derzhav-chleniv-nato-prijnyatih-u-skladovih-sektoru-bezpeki-i-oboroni

контррозвідувальних компонентів безпеки, який в свою чергу імплементований в діяльність Міністерства оборони України та Збройних Сил України як службовий документ, про те не впроваджений в повсякденну діяльність підрозділів, в тому числі і авіаційних. Ігнорування таких положень в українському нормативному полі створює ризики неуніфікованого реагування на загрози, недостатньої готовності до протидії підривній діяльності іноземних спецслужб і втрати сумісності з партнерами по НАТО у сфері контррозвідувальної діяльності.

Таким чином, загальна оцінка чинного законодавства свідчить про існування розвиненої нормативної основи в цивільному секторі, але водночас – про нормативну невизначеність у державній авіації, зокрема у контексті забезпечення контррозвідувального режиму. Уніфікація підходів, впровадження міжнародних стандартів (як ICAO, так і НАТО), а також нормативне врегулювання міжвідомчої взаємодії між Міністерством оборони України та Службою безпеки України є ключовими передумовами для підвищення ефективності системи безпеки авіаційної сфери України в умовах гібридних загроз та воєнного стану.

2.3. Практика взаємодії Служби безпеки України, Міністерства оборони України, Головного управління державної авіації України та інших суб'єктів

Забезпечення контррозвідувального режиму на об'єктах державної авіації України вимагає комплексної взаємодії між ключовими суб'єктами сектору безпеки і оборони. Серед них першочергове місце належить Службі безпеки України (СБУ) як спеціальному органу, відповідальному за здійснення контррозвідувальної діяльності відповідно до Закону України "Про Службу безпеки України" та Закону України "Про контррозвідувальну діяльність" [16, 17]. Однак ефективність цієї діяльності на об'єктах авіаційної інфраструктури значною мірою залежить від рівня координації з іншими відомствами —

насамперед Міністерством оборони України, Головним управлінням державної авіації України (ГУДАУ), командуваннями видів Збройних Сил України (таких як, Командуванням Повітряних Сил, Командуванням Сухопутних військ, Командуванням військово-морських Сил тощо), а також іншими структурами, що володіють та експлуатують об'єкти державної авіації. На сьогоднішній день, не існує жодного відкритого[10] нормативно-правового акту, який би в свою чергу регулював таку взаємодію на рівні державної авіації.

В умовах правового режиму воєнного стану, який діє на території України, зростає потреба в оперативній координації між зазначеними суб'єктами задля своєчасного виявлення, попередження та нейтралізації загроз диверсійного, агентурного, інформаційного чи технічного характеру. З практичної точки зору, така взаємодія реалізується у формі міжвідомчої співпраці: спільних оперативно-тактичних заходів, обміну розвідувальною інформацією, погодження режимних вимог до об'єктів авіації, а також участі представників Служби безпеки України в оцінці вразливості об'єктів. У сучасних умовах актуалізується більш тісна взаємодія авіаційних підрозділів сектору безпеки і оборони з представниками уповноважених органів, зокрема військової контррозвідки та Служби безпеки України, що зумовлено зростанням рівня загроз та необхідністю комплексного реагування на виклики у сфері національної безпеки.

Головне управління державної авіації України виконує функції координуючого органу у сфері реалізації політики держави щодо діяльності об'єктів державної авіації, а також забезпечує доведення відповідних нормативно-правових актів до авіаційних частин, підпорядкованих Міністерству оборони України та іншим центральним органам виконавчої влади. Водночас, як було зазначено раніше, питання забезпечення авіаційної безпеки не належать до компетенції цього органу, що прямо визначено положеннями статті 7 Повітряного кодексу України. На відміну від цього, аналогічний орган у сфері

[10] Під терміном *відкритий документ* у цьому контексті мається на увазі такий нормативно-правовий акт чи інструктивний матеріал, який не має грифа обмеження доступу (наприклад, "для службового користування" або вищого рівня секретності) і є загальнодоступним для ознайомлення.

цивільної авіації — Державна авіаційна служба України — наділений відповідними контрольними та координаційними повноваженнями у сфері авіаційної безпеки.

Цей розподіл функціоналу є чітко закріпленим, зокрема, у Положенні про взаємодію в контрольованій зоні авіаційних суб'єктів служб авіаційної безпеки з підрозділами центральних органів виконавчої влади щодо забезпечення авіаційної безпеки, затвердженому наказом Державної служби України з нагляду за забезпеченням безпеки авіації № 482 від 05.07.2006 [18]. У цьому документі визначено механізми взаємодії між суб'єктами авіаційної діяльності, підрозділами авіаційної безпеки та представниками силових структур у межах об'єктів цивільної авіації. Це дозволяє уникати дублювання повноважень, сприяє ефективному обміну інформацією та уніфікації протоколів реагування. Наявність такого нормативного механізму у цивільному секторі є прикладом, якого наразі бракує у державній авіації, де взаємодія залишається поза межами формального правового поля.

В свою чергу, Міністерство оборони України, через інші структурні підрозділи, здійснює реалізацію режимних та охоронних заходів на рівні частин, аеродромів та інших об’єктів інфраструктури, зокрема через впровадження інструкцій, планів охорони та систем контролю доступу.

Попри наявність правових засад для взаємодії, на практиці часто спостерігається недостатній рівень уніфікації процедур, брак єдиної платформи для інформаційної взаємодії, а також розмежування відповідальності між учасниками контррозвідувального режиму. Серед чинників, що знижують ефективність міжвідомчої взаємодії, можна відзначити: різні підходи до класифікації загроз; відсутність спільних стандартів оцінки ризиків; обмежений доступ до інформації внаслідок відомчих обмежень. Крім того, реалізація контррозвідувальних функцій на об’єктах, що перебувають у підпорядкуванні інших центральних органів виконавчої влади, часто ускладнюється через відсутність формалізованих механізмів співпраці із Службою безпеки України та/або Головним управлінням державної авіації України.

Водночас, позитивним прикладом міжвідомчої взаємодії є участь представників Служби безпеки України у погодженні заходів авіаційної безпеки на стратегічно важливих об’єктах та проведенні комплексних навчань з протидії диверсіям та актам незаконного втручання. Також варто відзначити спільну діяльність у сфері сертифікації служб безпеки на об’єктах цивільної авіації, яка здійснюється за участі Служби безпеки України, Міністерства розвитку громад, територій та інфраструктури України та Державної авіаційної служби України відповідно до Авіаційних правил України.

Таким чином, взаємодія між ключовими суб’єктами контррозвідувального забезпечення авіаційної сфери України, хоча і має законодавче підґрунтя, потребує подальшої інституціоналізації, узгодження підходів та гармонізації процедур, з урахуванням міжнародного досвіду та потреб воєнного часу. З огляду на зростання загроз в умовах гібридної війни, нагальною є розробка міжвідомчих доктрин або регламентів, що визначатимуть порядок реагування, обміну інформацією та реалізації заходів із забезпечення стійкості та захисту авіаційної інфраструктури державного значення.

2.4. Аналіз виявлених вразливостей і загроз диверсійного, технічного та інформаційного характеру

Забезпечення контррозвідувального режиму на об’єктах державної авіації потребує системного підходу до виявлення, класифікації та нейтралізації загроз, які можуть мати диверсійний, технічний або інформаційний характер. Кожна з цих категорій загроз створює специфічний спектр ризиків для об’єктів критичної авіаційної інфраструктури, і потребує відповідного інструментарію оцінки та реагування.

Виявлені на практиці вразливості свідчать про наявність значних прогалин у комплексному захисті таких об'єктів, зокрема у сфері фізичної безпеки, протидії дронам, охорони периметра, забезпечення технічними засобами охорони та кадрового ресурсу. Одним із ключових викликів є недостатня

оснащеність авіаційних об'єктів системами протиповітряної оборони та засобами протидії безпілотним літальним апаратам, що створює потенційні “вікна уразливості” для здійснення диверсій. Додатково, спостерігається фрагментарність у застосуванні сучасних інженерно-технічних рішень охорони: периметри багатьох об’єктів не мають належного зонування, відсутні інтегровані системи виявлення, сигналізації, відеоспостереження та реагування. Крім цього, існує суттєвий дефіцит кадрового забезпечення заходів охорони та оборони — підрозділи фізичної охорони не завжди мають достатній штат, оснащення і підготовку для ефективного реагування на потенційні загрози [31]. Відсутність уніфікованих інструкцій і стандартів взаємодії між силами охорони, військовою контррозвідкою та іншими суб’єктами безпеки створює прогалини у загальній структурі забезпечення стійкості.

Загрози диверсійного характеру пов’язані з можливістю умисного пошкодження, знищення або виведення з ладу критичних об’єктів та систем. До таких загроз належать акти підривної діяльності, проникаючі дії агентурного характеру, фізичне знищення повітряних суден, інфраструктури аеродромів чи логістичних вузлів. Їх джерелами можуть бути як зовнішні ворожі сили, так і внутрішні деструктивні елементи.

Технічні загрози виникають внаслідок недосконалості, несправностей або недостатнього захисту систем управління, засобів зв’язку, енергопостачання та аеродромного обладнання. Особливо небезпечними є такі сценарії, як втручання в систему управління польотами, блокування злітно-посадкової смуги, підміна технічних сигналів або навігаційних даних.

Інформаційні загрози охоплюють широкий спектр ризиків, пов’язаних із витоком, підміною або блокуванням інформації. В умовах цифровізації в дальності авіації, відповідно до практики НАТО, функціонування автоматизованих систем управління, зокрема в сфері забезпечення охорони, логістики та планування польотів, є критично залежним від цілісності та захищеності інформаційних потоків. Як відзначається в дослідженні С.А. Леуса

та О.Є. Архипова, ключовими аспектами інформаційної безпеки є збереження конфіденційності, цілісності та доступності даних.

У роботі зазначається, що ризики реалізуються на перетині трьох чинників: наявності загроз, наявності вразливостей та ймовірності їх експлуатації. При цьому загроза без вразливості є неактивною, а вразливість без загрози — неактуалізованою, що дозволяє застосувати модель взаємозв'язку "загроза — вразливість — ризик" до сектору авіаційної безпеки в цілому [19].

Вразливості можуть виникати внаслідок:

— недосконалості політик і процедур безпеки;

— недостатньої взаємодії та комунікації між учасниками забезпечення авіаційної безпеки;

— помилок в проєктуванні об'єктів державної авіації, організації функціонування систем охорони, оповіщення тощо;

— недостатнього захисту каналів зв'язку;

— неналежного контролю фізичного доступу до об'єктів;

— недостатня підготовка особового складу контррозвідувальній обізнаності[11][20].

Ці вразливості типові як для автоматизованих систем управління технологічними процесами, так і для інформаційних та охоронних систем у державній авіації. Більше того, вразливості процедурного характеру (наприклад, брак інструкцій, неузгодженість нормативних документів, відсутність стандартів реагування) часто становлять не меншу загрозу, ніж технологічні.

У контексті гібридних загроз, актуальними залишаються сценарії комплексного характеру — коли диверсійна діяльність поєднується з технічним саботажем або інформаційною атакою. Наприклад, використання безпілотних літальних апаратів для спостереження або ж наприклад, доставки

[11] Безпосереднє формулювання терміну "контррозвідувальна обізнаність" (Counterintelligence Awareness) містить Директива Департаменту оборони США № 5240.06, яка визначає її як рівень усвідомлення особою інформації про загрози, методи та ознаки діяльності іноземних розвідувальних служб, а також вимоги доповідати про таку інформацію.

вибухонебезпечних предметів через фізичний доступ до інфраструктури — це не лише технічна загроза, а й прояв інформаційної вразливості.

Варто звернути увагу, що в умовах воєнного стану зростає ймовірність реалізації складних, скоординованих атак, зокрема з використанням соціальної інженерії, кіберзасобів та внутрішніх агентів. Відповідно, вимоги до контррозвідувального режиму повинні охоплювати як традиційні охоронні заходи, так і елементи оцінки ризиків, що базуються на ідентифікації вразливостей та сценарному аналізі можливих загроз.

У дослідженні Кравченка Р.М. проаналізовано окремі нормативно-правові акти, що регулюють суспільні відносини в сфері контррозвідувального забезпечення Армії Сполучених Штатів Америки, задля пошуку правових рішень, які могли б бути адаптовані до національного законодавства в інтересах підвищення ефективності контррозвідувального пошуку органів військової контррозвідки Служби безпеки України. Автор проаналізувавши окремі нормативно-правові акти Сполучених Штатів Америки, в сфері контррозвідувального режиму зазначає, що ключовими елементами ефективної моделі є нормативне закріплення обов'язку всього особового складу проходити регулярні контррозвідувальні інструктажі, а також невідкладно інформувати уповноважені підрозділи про ознаки шпигунства, диверсійної або терористичної діяльності. Змістовним ядром цієї системи є інституціоналізований механізм взаємодії між військовослужбовцями, командуванням і військовою контррозвідкою, що доповнюється юридичною відповідальністю за порушення вимог. У Сполучених Штатах Америки також застосовується категоризація повідомлень за ступенем імовірності загроз, що дозволяє органам військової контррозвідки формувати емпіричну базу для стратегічного аналізу. За таких умов командири зобов'язані не лише організовувати контррозвідувальні тренування, але й контролювати повноту їх реалізації. Автор приходить до висновку, що імплементація аналогічних інструментів в Україні, зокрема в оборонно-авіаційному секторі, сприятиме підвищенню оперативної чутливості системи безпеки, попередженню інфільтрації та своєчасному реагуванню на

сучасні гібридні загрози [21]. Проте, на жаль, механізми які описані в зазначеній статті або відсутні в Збройних Силах України та інших складових сектору безпеки та оборони, або реалізовані лише частково — переважно у контексті державної таємниці. В умовах сьогодення, нормативне закріплення обов'язковості проходження контррозвідувальних інструктажів, щорічного тренування, створення уніфікованих протоколів доповіді про загрози, а також включення до підготовки особового складу компонентів контррозвідувальної обізнаності тощо, крім зобов'язань, які виникають в зв'язку з отриманням допуску до державної таємниці значно вплинуть на систему забезпечення державної безпеки, в першу через забезпечення безпеки критично важливих об'єктів – об'єктів державної авіації.

Таким чином, аналіз виявлених вразливостей і загроз диверсійного, технічного та інформаційного характеру на об'єктах державної авіації України засвідчує критичну потребу в переосмисленні й посиленні чинної системи забезпечення контррозвідувального режиму. Виявлені проблеми у фізичній охороні, технічному оснащенні, кадровому забезпеченні, а також недосконаліть нормативно-організаційних механізмів координації дій між суб'єктами безпеки створюють системні ризики в умовах воєнного стану та гібридних загроз. Інтеграція іноземного досвіду, зокрема практики Сполучених Штатів Америки щодо впровадження обов'язкових інструктажів, інституційної взаємодії та обов'язковості доповідей про підозрілі ситуації, є доцільною в контексті адаптації моделі постійного контррозвідувального моніторингу до національного законодавства.

Запровадження нормативних актів, які б регламентували чіткий порядок виявлення, фіксації та реагування на загрози, формалізація процедур навчання та доповіді, створення автоматизованих систем оцінки ризиків — це лише окремі напрями, що мають бути імплементовані для досягнення стійкості. Особливе значення матиме включення складової контррозвідувальної обізнаності до підготовки особового складу не лише у контексті державної таємниці, а як системного елементу оборонної культури. Комплексний підхід до усунення вразливостей у поєднанні з ефективною міжвідомчою взаємодією дозволить сформувати дієву систему превенції загроз для критичної авіаційної інфраструктури України.

ВИСНОВКИ ДО РОЗДІЛУ 2

У процесі опрацювання матеріалу другого розділу було з’ясовано, що система забезпечення контррозвідувального режиму на об’єктах державної авіації України залишається складним і багатовимірним феноменом, в межах якого співіснують нормативно-правові, інституційні, процедурні та технологічні складові. Проведений аналіз дозволив встановити низку критичних структурних та процедурних дисфункцій, які суттєво знижують ефективність реалізації контррозвідувальних заходів у воєнний час, зокрема в авіаційному секторі як такому, що є об'єктом підвищеної уразливості в умовах гібридної агресії.

Передусім, виявлено фрагментарність організаційної моделі суб’єктів контррозвідувального забезпечення. У контексті державної авіації спостерігається паралельне функціонування військових, правоохоронних і розвідувальних структур, які здійснюють охоронно-контррозвідувальні функції без достатньо чіткого розмежування повноважень, що унеможливлює формування уніфікованої вертикалі управління та призводить до дублювання завдань або, навпаки, до появи “сірих зон” управлінської відповідальності. При цьому особливо помітною є асиметрія між інституційною побудовою цивільного та військового авіаційного сектору, де перший має чіткі механізми взаємодії та координації (на прикладі Державної авіаційної служби України та її взаємодії з силовими структурами), а другий — позбавлений нормативно унормованої координаційної моделі.

У межах аналізу чинного законодавства встановлено, що нормативна база, яка регулює діяльність у сфері забезпечення безпеки державної авіації, є не тільки фрагментованою, а й концептуально незавершеною. Особливо критичною видається відсутність закріплення у національному праві поняття та вимог до “контррозвідувального режиму” як системної категорії, що охоплює не лише сукупність організаційних заходів, але й формалізовані моделі управління ризиками, моніторингу загроз і оперативного реагування. Це свідчить про нормативний вакуум, який унеможливлює повноцінну імплементацію

міжнародних стандартів — передусім у частині доктринальних положень НАТО (зокрема AJP-2.2 та AJP-3.14), а також в аспекті гармонізації з підходами ICAO та EASA.

Практика міжвідомчої взаємодії, що аналізувалася у підрозділі 2.3, демонструє як потенціал, так і слабкі ланки функціонального партнерства між Службою безпеки України, Міністерством оборони України, Головним управлінням державної авіації України та іншими структурами. Хоча наявні позитивні кейси співпраці — наприклад, у формі погодження режимних заходів, спільних навчань чи сертифікації служб безпеки на об'єктах цивільної авіації — проте системність та уніфікованість таких підходів у державному секторі відсутні. Залишається нерозв'язаним питання нормативного закріплення процедур інформаційного обміну, розмежування зони відповідальності та впровадження єдиної доктринальної основи взаємодії у сфері контррозвідки для авіаційних об’єктів.

Поглиблений аналіз вразливостей і загроз диверсійного, технічного та інформаційного характеру засвідчив наявність системної незахищеності об’єктів державної авіації. Особливо проблемною є ситуація із забезпеченням фізичного захисту (недостатність інженерних рішень, відсутність сучасних систем спостереження та реагування), нестача кадрових і ресурсних можливостей для організації режимних заходів, а також вразливість каналів зв’язку та систем управління. Значна частина загроз реалізується на тлі процедурних вразливостей — неузгодженості нормативних актів, дефіциту інструктивної бази, відсутності уніфікованих протоколів реагування, що в комплексі створює критичні “зони ризику”.

Окремо заслуговує на увагу досвід країн-членів НАТО, зокрема Сполучених Штатів Америки, де контррозвідувальна обізнаність та превентивна безпека є елементами оборонної культури. Наявність обов’язкових програм інструктажів, категоризація ризиків, юридично зобов’язуюча відповідальність за повідомлення про загрози — ці компоненти формують високий рівень операційної стійкості системи, до якого Україна має прагнути у процесі

нормативної адаптації. Відсутність аналогічних механізмів в українських Збройних Силах та інших структурах оборонного сектору ставить під сумнів ефективність існуючих процедур реагування, знижуючи загальну контррозвідувальну резильєнтність державної авіації.

Таким чином, підсумовуючи зміст другого розділу, можу констатувати: система забезпечення контррозвідувального режиму на об'єктах державної авіації України потребує концептуального оновлення, заснованого на принципах міжвідомчої інтеграції, нормативної гармонізації з міжнародними стандартами та формалізації контррозвідувального режиму як самостійної правової категорії. В умовах воєнного стану та з урахуванням тенденцій гібридної війни, вкрай важливо закласти нормативно-інституційну основу для формування сталої, надійної та оперативно адаптивної системи захисту критичної інфраструктури авіаційного профілю.

РОЗДІЛ 3. МІЖНАРОДНИЙ ДОСВІД І СТАНДАРТИ НАТО ЩОДО КОНТРРОЗВІДУВАЛЬНОГО ЗАБЕЗПЕЧЕННЯ АВІАЦІЙНИХ ОБ'ЄКТІВ

3.1. Стандарти та рекомендована практики ICAO, регламенти Європейського агентства з безпеки авіації (EASA) та стандарти НАТО у сфері забезпечення безпеки авіації

Забезпечення безпеки державної авіації у країнах-членах НАТО ґрунтується на принципах, що поєднують міжнародні норми цивільної авіації та військові стандарти Альянсу. Водночас, у переліку стандартів НАТО відсутній прямий аналог стандартів та рекомендованих практик ICAO, зокрема Додаток 17 та Doc 8973, які визначають підходи до захисту цивільної авіації від актів незаконного втручання. Це пояснюється тим, що нормативна база НАТО спрямована на забезпечення ефективності спільних операцій військових структур різних родів військ, включаючи авіаційні та розвідувальні (контррозвідувальні) підрозділи, а також на реалізацію заходів колективної оборони.

З практичної точки зору, система авіаційної безпеки країн-членів НАТО, з якими я працювала, базується на фундаментальних принципах ICAO та Європейського агентства з безпеки авіації (European Union Aviation Safety Agency (EASA)), інтегрованих із обов'язковими процедурами Альянсу. Така синергія дозволяє не тільки зберігати відповідність міжнародним стандартам, а й адаптувати процеси безпеки до специфічних умов військових операцій.

Окрім Додатку 17 до Чекагської конвенції – "Авіаційна безпека" та Doc 8973 "Керівництво з авіаційної безпеки ICAO" стратегічний вектор розвитку міжнародної системи авіаційної безпеки визначає Глобальний план ICAO з авіаційної безпеки (Global Aviation Security Plan — GASP). Цей документ окреслює багаторічну стратегію щодо підвищення стійкості авіаційної галузі до загроз, зокрема актів незаконного втручання, кіберзагроз, терористичних атак тощо. В GASP виділені 6 глобальних пріоритетних області (Рисунок 1, Рисунок

2), на яких держави-учасниці, промисловість та інші зацікавлені сторони мають сконцентрувати свої зусилля:

- Підвищення обізнаності про ризики та реагування на них: Розробка ефективних і сталих політик та заходів через виявлення, розуміння й управління ризиками. Використання оцінки ризиків дозволяє зосереджувати зусилля там, де вони мають найбільший вплив, і завчасно виявляти нові загрози.
- Підтримка сильної та ефективної культури безпеки: Формування позитивної безпекової поведінки серед персоналу. Безпека розглядається як основна цінність, спільна відповідальність усіх, що передбачає усвідомлену і проактивну поведінку.
- Розвиток і просування ролі людського фактора: Інвестування в персонал, інтеграція принципів людського фактора в політики та заходи з безпеки. Визнання професійної ролі фахівців з авіаційної безпеки та необхідних для цього компетенцій.
- Поліпшення технологічних ресурсів та сприяння інноваціям: Сприяння розвитку технологічних рішень та інновацій, які можуть покращити ефективність безпеки, одночасно забезпечуючи інтеграцію людського чинника й операційну ефективність.
- Удосконалення нагляду та забезпечення якості: Встановлення та підтримка ефективних процесів контролю якості та нагляду на глобальному, національному та локальному рівнях, що є критично важливими для сталої безпеки.
- Посилення співпраці та підтримки: Інтеграція ефективної співпраці між державами, галуззю та іншими зацікавленими сторонами. Розбудова потенціалу для досягнення ключових результатів у сфері безпеки більш ефективно та скоординовано.

GASP забезпечує уніфікацію політик у сфері безпеки на глобальному рівні через систему стратегічних цілей, серед яких:

- розвиток національних програм безпеки (National Aviation Security Plan – NASP);
- вдосконалення систем моніторингу та реагування на інциденти;
- посилення міжнародного обміну інформацією про загрози;
- зміцнення партнерств між державними, військовими та приватними структурами.

Рисунок 1. Глобальні пріоритетні області Глобального плану ICAO з авіаційної безпеки

Глобальний план забезпечення авіаційної безпеки ICAO є стратегічною основою для розробки, оновлення та імплементації національних програм авіаційної безпеки (NAPs) у державах-членах ICAO. Його основна мета уніфікувати підходи до безпеки на глобальному рівні, сприяти узгодженості між країнами у впровадженні стандартів і рекомендованих практик ICAO, забезпечити основу для розробки національних планів, адаптованих до локальних умов, загроз та ресурсів. Країни-члени ICAO, зокрема члени НАТО, використовують GASP як орієнтир для гармонізації національних програм із

глобальними цілями, включаючи оцінку ризиків, розвиток культури безпеки, впровадження інновацій та посилення міжвідомчої взаємодії.

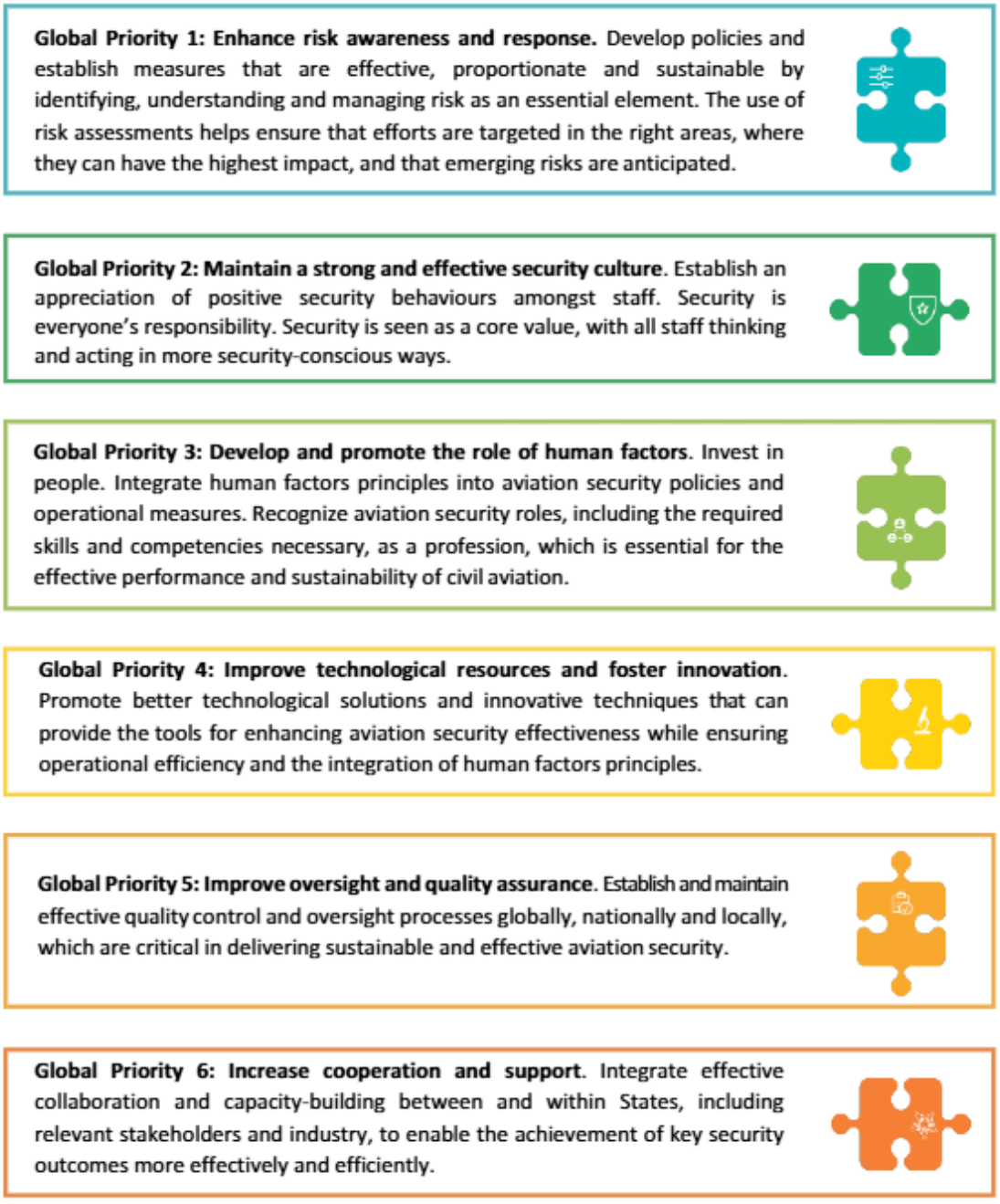

Рисунок 2. Сутність глобальних пріоритетних областей Глобального плану ICAO з авіаційної безпеки

Таким чином, GASP є системоутворюючим документом, що слугує базисом для стратегічного планування, нормативного регулювання та

оперативного управління у сфері забезпечення авіаційної безпеки на національному рівні.

Окрему увагу в GASP приділено необхідності розробки національних стратегій безпеки, які враховують взаємодію цивільної та державної (військової) авіації — що прямо корелює із завданням інтеграції стандартів НАТО у безпекову політику держав-членів Альянсу. Принципи GASP також зосереджені на забезпеченні стійкості інфраструктури, запровадженні кібергігієни, а також на підтримці кадрової спроможності органів авіаційної безпеки [22].

Особливе місце в системі забезпечення безпеки авіації держав-членів НАТО, які є членами Європейського союзу, належить діяльності Європейського агентства з авіаційної безпеки (EASA). Цей орган функціонує відповідно до законодавства Європейського Союзу та виконує ключову роль у встановленні єдиних технічних вимог, процедур сертифікації, систем управління безпекою польотів, а також забезпеченні ефективного нагляду за їх дотриманням у цивільній авіації. Водночас практики EASA безпосередньо інтегруються у стандарти національних військових структур країн-членів НАТО, які забезпечують експлуатацію державної авіації з урахуванням як вимог національної безпеки, так і міжнародних стандартів.

До основних принципів діяльності EASA, які стали фундаментом для інтегрованих підходів до забезпечення авіаційної безпеки в НАТО, належать:

- ризик-орієнтоване управління безпекою (risk-based safety management), що передбачає аналіз і ранжування загроз, їх системну оцінку та пріоритезацію ресурсів відповідно до рівня небезпеки;
- застосування систем управління безпекою польотів (Safety Management System (SMS) у всіх авіаційних суб’єктів, включаючи операторів, аеродроми, органи обслуговування повітряного руху;
- перехід до проактивного та прогностичного підходу, де профілактика інцидентів є пріоритетнішою за реагування на вже скоєні порушення;
- інтеграція аналізу безпеки з кіберзахистом, що є особливо актуальним у військово-авіаційних структурах [23].

З точки зору забезпечення авіаційної безпеки, що регламентується документами НАТО важливу роль відіграють STANAGs, які регламентують стандартизацію процесів у військовій авіації, а також доктринальні документи НАТО, які регулюють забезпечення контррозвідувального режиму на всіх стадіях військової операції та під час повсякденного функціонування, такі як AJP-2 – загальна доктрина з розвідки, контррозвідки та безпеки, яка містить положення щодо забезпечення інформаційної та фізичної безпеки операцій, включаючи авіаційний компонент (місце доктрини розвідки в архітектурі об'єднаної доктрини НАТО представлена на Рисунку 3) [24]; AJP-2.2 – доктрина НАТО щодо контррозвідки та безпеки, яка встановлює принципи захисту від загроз, пов'язаних зі шпигунством, саботажем та кіберзагрозами, що безпосередньо впливає на авіаційну сферу; AJP-3.3 – доктрина НАТО щодо проведення повітряних операцій, яка регулює механізми застосування військової авіації у бойових діях, миротворчих місіях та реагуванні на кризові ситуації; AJP-3.14 – доктрина з управління ризиками та забезпечення захисту критично важливої інфраструктури, що визначає принципи безпеки військових та цивільних аеродромів, контроль доступу та протидію потенційним загрозам.

Варто звернути увагу, на доктрину НАТО AJP-3.14 "Allied Joint Doctrine for Force Protection", яка є ключовим документом, що визначає принципи захисту сил та критично важливої інфраструктури в умовах сучасних загроз. Вона спрямована на забезпечення безпеки персоналу, об'єктів, матеріальних засобів, операцій та діяльності від різноманітних загроз і небезпек, з метою збереження свободи дій та ефективності операцій, що сприяє успішному виконанню місії.

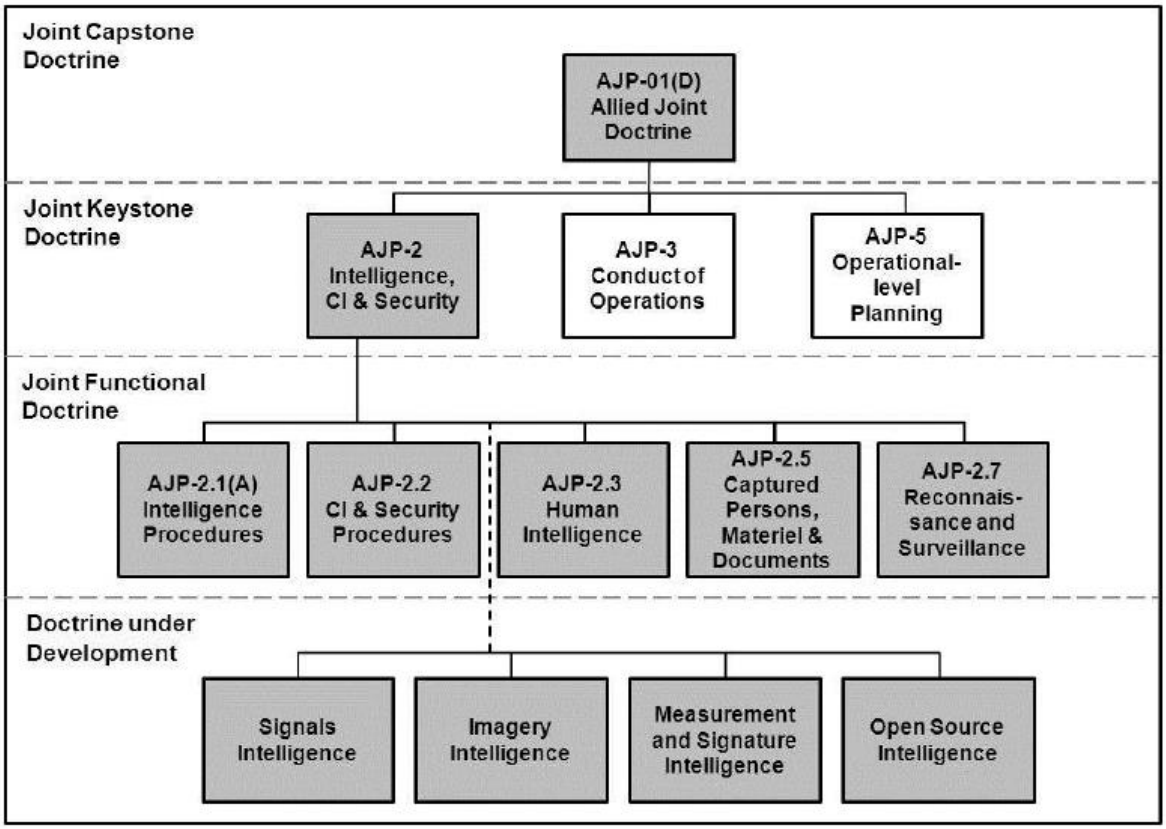

Рисунок 3. Місце доктрини розвідки в архітектурі об'єднаної доктрини НАТО

Фундаментальними елементами захисту сил (Рисунок 4) відповідно до цієї доктрини є:

- ✓ Протиповітряна оборона (Air Defence) - захист від загроз із повітря (ракет, авіаційних ударів, БпЛА тощо);
- ✓ Контроль тактичної зони відповідальності (Tactical Area of Responsibility Control) - управління простором навколо об'єкта або підрозділу, включаючи зони наближення та охорону периметра;
- ✓ Медичний захист та охорона здоров'я особового складу (Medical FP and Force Health Protection) - забезпечення медичної підтримки, санітарного захисту та профілактики захворювань серед військових;
- ✓ Захист від зброї масового ураження (CBRN Defence)- захист від хімічної, біологічної, радіаційної та ядерної загрози;
- ✓ Стійкість (Resilience) - здатність підрозділів та об'єктів продовжувати функціонування попри негативні впливи та атаки;

- ✓ Управління наслідками (Consequence Management) - планування та реагування на надзвичайні події після їх настання, мінімізація шкоди та відновлення функцій;
- ✓ Безпека (Security) - організація фізичної охорони, контролю доступу, охоронних процедур та технічних засобів захисту;
- ✓ Інженерна підтримка захисту сил (MILENG Support to Force Protection) - використання військових інженерних підрозділів для створення укріплень, загороджень, пунктів спостереження тощо.

Основою та підтримкою захисту сил є:

- ✓ Командування, управління, комунікація, координація та інтеграція захисту сил (Force Protection Command, Control, Communication, Coordination, and Integration) - забезпечення системного управління усіма елементами захисту сил;
- ✓ Розвідувальна підтримка захисту сил (Intelligence Support to Force Protection) - аналітична підтримка, оцінка загроз, контррозвідувальна інформація;
- ✓ Навчання і тренування (Training and Exercises) - підготовка персоналу, регулярні тренування для відпрацювання стандартних процедур та готовності до загроз.

Узагальнюючи представлені елементи захисту сил, можна стверджувати, що ефективне забезпечення безпеки авіаційних об’єктів у контексті стандартів НАТО неможливе без системної інтеграції розвідувального та контррозвідувального компонентів. Саме розвідка і контррозвідка виступають основою для формування актуального уявлення про загрози та небезпеки, що, згідно зі схемою доктрини AJP-3.14, є центральною ланкою всієї архітектури захисту сил [25].

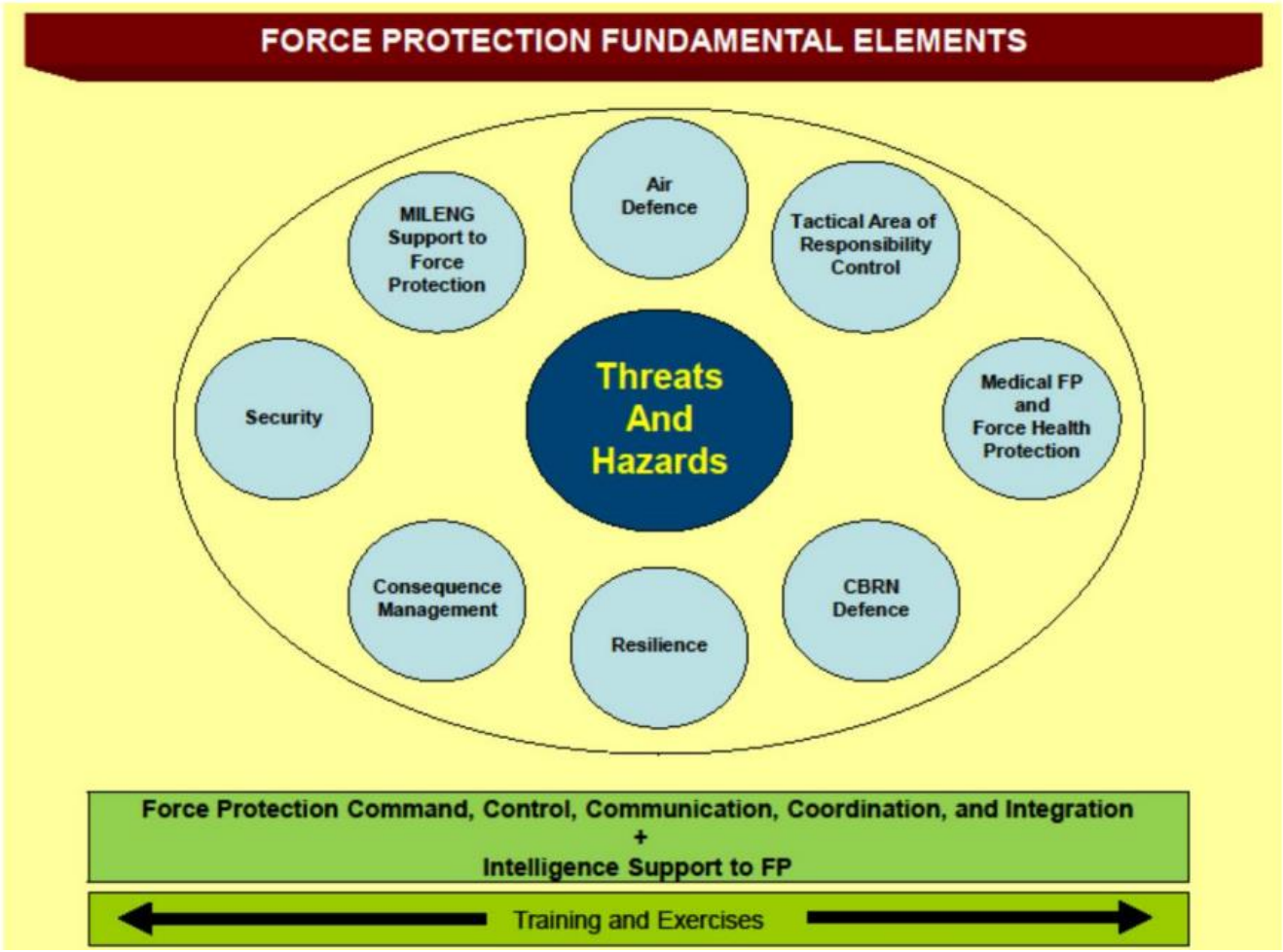

Рисунок 4. Фундаментальні елементи захисту сил

На практиці це означає, що розвідувальні підрозділи мають не лише своєчасно виявляти потенційні джерела загроз, а й оперативно передавати дані до системи управління захистом. У свою чергу, контррозвідка забезпечує проактивне виявлення диверсійної, шпигунської та інформаційно-підривної діяльності, яка може мати як зовнішнє, так і внутрішнє походження. Роль цих елементів суттєво зростає в умовах гібридних загроз, де класичні засоби нападу поєднуються з кібернетичними, інформаційними та інсайдерськими атаками.

Виходячи з зазначеного, можна стверджувати що розвідувальна та контррозвідувальна діяльність не є периферійними складовими, а мають статус функціонального ядра системи захисту сил, яке забезпечує її адаптивність, превентивність та стійкість до новітніх загроз яку використовують країни-слени Альянсу.

Таким чином, симбіоз військових нормативних документів НАТО (STANAG, AJP), принципів ICAO, практик EASA та стратегічних орієнтирів GASP створює основу для побудови ефективної системи забезпечення авіаційної безпеки як у мирний, так і в особливий період. Для України, яка прагне інтеграції у євроатлантичні структури, адаптація цих стандартів до потреб державної авіації є одним із ключових напрямів реформування сектору національної безпеки.

3.2. Практичні підходи країн-членів НАТО до організації контррозвідувального режиму (базуючись на досвіді Сполучених Штатів Америки)

Кравченко Р.М. у своїй статті “Щодо деяких підходів до вдосконалення контррозвідувального пошуку органів військової контррозвідки сб України з урахуванням аналізу законодавства США” зазначає що організація контррозвідувального режиму в країнах-членах НАТО, зокрема у Сполучених Штатах Америки, ґрунтується на багаторівневому, системному підході, що охоплює як правове регулювання, так і функціональну інтеграцію контррозвідувальних заходів у повсякденну діяльність збройних сил. Досвід США у цій сфері демонструє високу ступінь інституціалізації контррозвідувального компоненту в усіх аспектах військової безпеки, що робить його взірцем для наслідування в умовах адаптації національного законодавства до стандартів НАТО.

Ключовим елементом практичної моделі, як зазначає автор, є “Програма контррозвідувальної обізнаності та інструктажу”, впроваджена Інструкцією Міністерства оборони США № 5240.6, яка запровадила поняття *Counterintelligence Awareness*. В її основі лежить щорічне обов’язкове проходження особовим складом Армії США інструктажів щодо виявлення ознак шпигунської, терористичної та підривної діяльності, а також зобов’язання негайного повідомлення про відповідні інциденти органам військової

контррозвідки. Аналогічні вимоги поширюються і на цивільних працівників, а також на суб'єктів господарювання, які виконують оборонні контракти.

Законодавство США, зокрема Директиви № 5240.06 і № 5240.02, чітко встановлюють процедури і форми надання контррозвідувальних повідомлень, включаючи категоризацію загроз за рівнем імовірності їхнього зв'язку з іноземними розвідувальними структурами. Це дозволяє формувати базу емпіричних даних для стратегічного аналізу загроз та ефективного планування заходів нейтралізації.

Особливу увагу приділено обов'язкам командирів усіх рівнів, які зобов'язані контролювати реалізацію контррозвідувальних інструктажів, сприяти оперативному наданню інформації до відповідних підрозділів та запроваджувати систему регулярного моніторингу якості навчання

Окремим напрямом є реалізація положень Інструкції Армії США № 381-12 "Диверсія та шпигунство, спрямовані проти Армії США", яка передбачає проведення спеціалізованих контррозвідувальних тренувань, що охоплюють не лише загальні знання, але й приклади з практики, юридичні аспекти відповідальності за порушення вимог безпеки, а також методи виявлення ознак ворожого впливу.

Усі повідомлення та інциденти, що надходять до військової контррозвідки, підлягають щорічному узагальненню в спеціальному звіті, який включає статистику інформування, кількість розслідувань, результати розкритих фактів шпигунства, тероризму чи витоку інформації, а також аналіз ефективності реалізації програми обізнаності для забезпечення контролю та оцінки ефективності реалізації Програми контррозвідувальної обізнаності та інструктажу, в тому числі проведених на підставі неї контррозвідувальних розслідувань та операцій. Результати аналізу та узагальнення річних підсумків реалізації програми повинні доповідатися керівництву Контррозвідки Армії США. Всі дані які використовуються під час контррозвідувальних заходів обов'язково мають бути оцінені з точки зору управління ризиками. Згідно якого кожен процес опрацьовується в декілька етапів: Establishing the context —

Встановлення контексту; Risk assessment — Оцінка ризику; Risk identification — Ідентифікація ризику; Risk analysis — Аналіз ризику; Risk evaluation — Оцінювання ризику; Risk treatment — Обробка (зниження) ризику. Оцінка ризиків з точки зору контррозвідки є ключовим інструментом у запобіганні, виявленні та нейтралізації загроз, що походять від іноземних розвідувальних служб, терористичних організацій, внутрішніх агентів або деструктивних впливів.

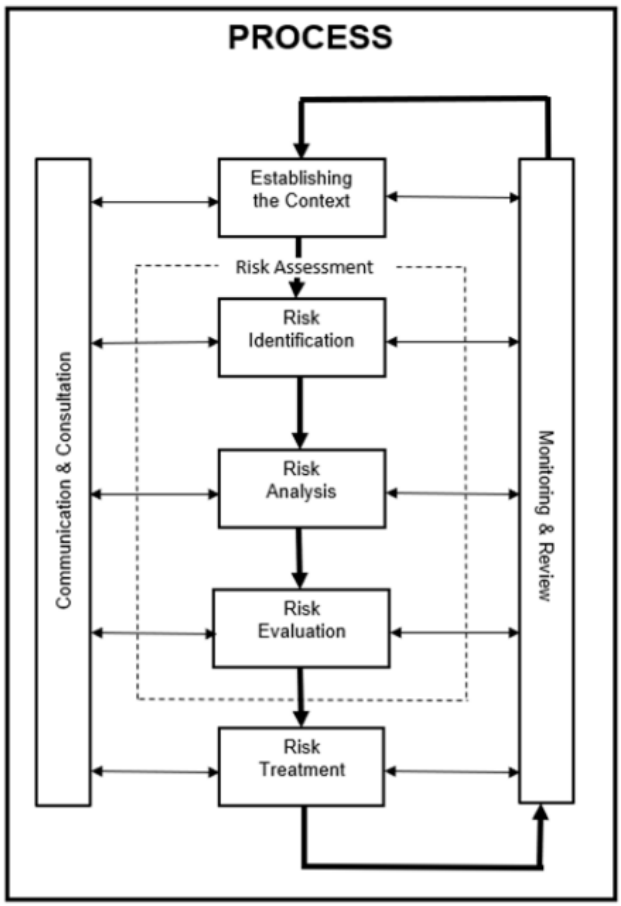

Рисунок 5. Процес управління ризиками

Автор в своїй статті наголошує що практичний досвід США у сфері організації контррозвідувального режиму у військових формуваннях базується на принципах:

- обов’язковості участі всього особового складу у заходах контррозвідувального характеру;
- прозорості процедур інформування про загрози;

- системного аналізу інформації та оцінці ризиків з метою її подальшої реалізації;
- уніфікації відповідальності за порушення безпекових вимог;
- постійного оновлення стандартів підготовки та навчання.

Імплементація подібних механізмів в Україні, з урахуванням специфіки законодавчого поля та потреб сектору безпеки й оборони, зокрема у сфері державної авіації, сприятиме посиленню контррозвідувального режиму, зниженню ризиків інфільтрації та підвищенню оперативної чутливості до гібридних загроз [21].

3.3. Оцінка потенціалу впровадження міжнародних авіаційних стандартів в українські реалії

Впровадження міжнародних авіаційних стандартів у систему забезпечення безпеки об'єктів державної авіації України становить важливу складову інтеграції у євроатлантичний безпековий простір. Цей процес не обмежується суто технічним або нормативним адаптуванням — він передбачає глибоку трансформацію підходів до управління ризиками, контррозвідувального забезпечення та взаємодії між державними структурами, об'єктами інфраструктури та суспільством.

Як зазначалось в підрозділі 3.1 розділу 3 міжнародні стандарти, зокрема документи Міжнародної організації цивільної авіації (ICAO), Європейського агентства з авіаційної безпеки (EASA), а також доктрини НАТО, визначають багаторівневий підхід до забезпечення безпеки. Він включає фізичний захист об’єктів, інформаційну безпеку, кіберзахист, протидію внутрішнім загрозам, а також створення системи превентивного виявлення та нейтралізації ризиків. Такий підхід є особливо актуальним в умовах гібридної агресії, коли диверсії, атаки на критичну інфраструктуру, проникнення агентурних мереж та використання технічних засобів розвідки набувають системного характеру.

Потенціал впровадження зазначених стандартів в українські умови є достатнім, проте значною мірою залежить від здатності національних інституцій

адаптувати принципи захисту, що ґрунтуються на цілісному управлінні ризиками. Основними викликами на цьому шляху є:

- інституційна фрагментованість відповідальних органів (відповідальність за забезпечення безпеки об’єктів державної авіації розподілена між кількома державними структурами та не існує чіткої єдиної системи координації, вертикалі управління або спільної політики);
- відсутність єдиної нормативної бази, гармонізованої зі стандартами НАТО та ІСАО;
- недостатнє кадрове забезпечення фахівцями у сфері авіаційної безпеки та контррозвідки;
- обмежене впровадження сучасних технічних рішень, зокрема систем відеоспостереження, захисту периметру, контролю доступу, засобів протидії БпЛА;
- низький рівень міжвідомчої координації у питаннях захисту об’єктів авіаційної інфраструктури.

Одним із ключових елементів адаптації міжнародного досвіду є запровадження механізмів безперервного оцінювання загроз та вразливостей. Практика країн-членів НАТО демонструє, що ефективна система авіаційної безпеки спирається на регулярний моніторинг оперативного середовища, аналіз ризиків та побудову моделі реагування, яка включає як технічні, так і організаційно-правові інструменти.

Крім цього, важливим елементом, який варто запозичити в країн-членів НАТО (зокрема США) – це формування культури безпеки серед персоналу, що передбачає обов’язкове навчання, регулярні інструктажі, ідентифікацію ознак підозрілої поведінки, а також створення каналів повідомлення про потенційні загрози. Особлива роль у цьому процесі відводиться органам контррозвідки, які мають бути інтегрованими в систему управління об’єктами державної авіації на всіх рівнях — від стратегічного до тактичного.

Також слід враховувати, що стандарти безпеки не можуть бути впроваджені ізольовано — вони потребують функціональної адаптації до

національного правового поля. Це включає необхідність оновлення внутрішніх положень, відомчих інструкцій та узгодження процедур між Збройними Силами України, Службою безпеки України, Головним управлінням державної авіації та іншими військовими формуваннями, що утворені відповідно до Законів України та що забезпечують безпеку і оборону.

Крім інституційної складової, необхідно враховувати суспільний аспект трансформації безпекового середовища. Як слушно зазначає в своєму дослідженні І.В. Слюсарчук, під час формування нової правової бази доцільно було у якості уніфікованого документу розробити контррозвідувальна стратегію, яка визначала б основні напрями протидії спецслужб дружніх країн європейської та світової спільнот спецслужбам та іншим структурам держав-агресорів та держав-терористів. Створення цієї стратегії може бути важливим елементом, який сформував би основні напрями діяльності спецслужб, інших силових структур, державних органів, громадських організацій, приватного сектору, включаючи і авіаційну специфіку. Також, реалізація принципу взаємодії контррозвідки з усіма елементами суспільства — від органів державної влади до приватного сектору — є фундаментальною умовою ефективного застосування міжнародного досвіду [26]. Практика країн НАТО, зокрема США, засвідчує, що однією з передумов успішної реалізації стандартів безпеки є глибока інтеграція розвідувально-контррозвідувальної діяльності в середовище об’єктів захисту, а також залучення цивільних структур до превентивного виявлення загроз. У цьому контексті положення пункт 11 статті 25 Закону України “Про Службу безпеки України” відкриває перспективу для закріплення штатних посад Служби безпеки України в організаціях, пов’язаних з авіаційною діяльністю, що відповідатиме найкращим практикам союзників. А можливо навіть утворюючи вертикаль аналогу служби авіаційної безпеки з цивільної авіації у держану (військову) авіацію.

Важливою пропозицією щодо вдосконалення системи забезпечення безпеки, яку обґрунтовує у своєму дослідженні Хміль Я.І., є створення єдиного інформаційно-аналітичного центру з накопичення, обробки, аналізу та

прогнозування інформації, що функціонував би під координацією Служби безпеки України. Автор акцентує увагу на тому, що наразі однією з ключових проблем є не лише відсутність такого інтегрованого центру, але й загальна недостатність ресурсного забезпечення, розпорошеність функцій між суб'єктами безпеки, а також неефективне використання наявних сил і засобів у секторі безпеки та оборони. В умовах війни, коли ризики реалізуються у високій динаміці, такий розрив між органами стратегічного аналізу та виконавчими структурами створює передумови для втрати контрольованості над критично важливими об'єктами, зокрема об'єктами державної авіації. Пропозиція автора щодо створення єдиного інформаційно-аналітичного центру при СБУ, який би забезпечував міжвідомчу координацію дій у сфері контррозвідки, становить важливу передумову для якісного впровадження міжнародних стандартів, орієнтованих на проактивне реагування на загрози, а не лише їх наслідки [27]. Створення подібного центру, дозволить реалізовувати кращі практики країн-членів НАТО, які описані в підрозділі 3.2 цього розділу.

У підсумку, потенціал імплементації міжнародних стандартів у сфері авіаційної безпеки в Україні залишається високим за умови системної роботи у трьох ключових напрямках:

1. Нормативне забезпечення — гармонізація національного законодавства з вимогами стандартів ICAO, EASA та НАТО.
2. Інституційна інтеграція — створення спільних структур для аналізу загроз, розробки стандартів і реагування на інциденти.
3. Операційна реалізація — впровадження стандартів на рівні об'єктів авіаційної інфраструктури, підготовка персоналу, технічне оснащення та інструктивно-методичне супроводження.

Реалізація цих завдань дозволить не лише зміцнити захищеність авіаційної інфраструктури в умовах воєнного стану, а й наблизити національну систему авіаційної безпеки до моделей, що функціонують у країнах НАТО.

ВИСНОВКИ ДО РОЗДІЛУ 3

У третьому розділі магістерської роботи було здійснено комплексний аналіз міжнародного досвіду та стандартів у сфері контррозвідувального забезпечення авіаційної безпеки, що застосовуються в країнах-членах НАТО, з особливим акцентом на доктрини Альянсу, рекомендації Міжнародної організації цивільної авіації (ICAO), Європейського агентства з авіаційної безпеки (EASA), а також на практику, що склалася у Сполучених Штатах Америки як одного з провідних центрів вироблення контррозвідувальної політики в авіаційному секторі.

Насамперед варто відзначити, що міжнародні стандарти авіаційної безпеки, які діють у межах системи ICAO, ЄС та НАТО, ґрунтуються на інтегральному підході до ризик-менеджменту та системної протидії загрозам у широкому спектрі — від фізичного вторгнення до кіберзагроз і диверсійної діяльності. Їх ключова особливість полягає у синергетичному поєднанні технічних, організаційних, кадрових та інформаційно-аналітичних заходів, що реалізуються на основі доктринального планування, стандартизації процедур, а також через формування сталої культури безпеки.

Проаналізовані доктрини НАТО (зокрема AJP-2, AJP-2.2, AJP-3.14, AJP-3.3) фокусуються на тому, що забезпечення безпеки авіаційних об’єктів не може розглядатися як виключно технічна функція — навпаки, воно повинно розглядатися в контексті загальної доктрини захисту сил, у межах якої контррозвідувальний компонент відіграє роль центрального ядра превентивного реагування на загрози. На відміну від цивільних підходів, стандарти Альянсу передбачають посилений контроль за інформаційними потоками, протидію ворожим розвідувальним структурам, боротьбу з інсайдерськими загрозами та формування оперативно-чутливого середовища.

Особливо важливими є висновки, отримані в результаті аналізу американської моделі організації контррозвідувального режиму у військовому секторі. Практика США засвідчує високий рівень інституційної деталізації

процедур, в тому числі обов'язковість проходження контррозвідувальних інструктажів усім особовим складом, обов'язок негайного повідомлення про підозрілі дії, категоризацію загроз за ступенем імовірності, систематизацію зібраної інформації у централізованих базах даних, а також щорічне звітування щодо ефективності заходів контррозвідки. Така модель доводить доцільність і дієвість побудови системи, в якій кожен військовослужбовець чи цивільний фахівець розглядається як активний учасник безпекового процесу.

У свою чергу, здійснена в підрозділі 3.3 оцінка потенціалу впровадження міжнародних стандартів у національні реалії України дозволяє дійти висновку, що адаптація зазначених практик є не лише актуальною, але й об'єктивно необхідною умовою забезпечення національної безпеки у сфері державної авіації. Разом з тим, цей процес стикається з низкою структурних, інституційних і нормативно-правових бар'єрів.

По-перше, системна інституційна фрагментація органів, відповідальних за безпекове забезпечення, перешкоджає створенню єдиного контррозвідувального середовища у державній авіації. Відсутність централізованого координаційного механізму між Службою безпеки України, Міністерством оборони України, Головним управлінням державної авіації України та іншими суб'єктами сектору безпеки ускладнює формування цілісної політики безпеки, заснованої на спільних ризик-орієнтованих підходах.

По-друге, відсутність уніфікованої нормативної бази, яка б регламентувала контррозвідувальні заходи на об'єктах державної авіації відповідно до стандартів ICAO, EASA і НАТО, суттєво знижує ефективність інтеграції міжнародного досвіду. Хоча у цивільному авіаційному секторі вже існують документи, які відповідають вимогам додатку 17 до Чиказької конвенції, державна авіація досі позбавлена нормативного інструментарію, що дозволив би імплементувати подібні практики.

По-третє, кадрова, ресурсна та технічна незабезпеченість також є стримувальним чинником. На багатьох об'єктах державної авіації не функціонують повноцінні системи фізичного захисту, відеоспостереження,

протидії дронам тощо. При цьому фахівці, відповідальні за реалізацію заходів авіаційної безпеки, не завжди проходять спеціалізовану підготовку, що враховує принципи контррозвідувальної обізнаності, оцінки ризиків і протидії сучасним гібридним загрозам.

Четвертим ключовим блоком висновків є необхідність створення єдиного інформаційно-аналітичного центру при СБУ, який би забезпечував системну обробку даних про загрози, їх класифікацію, прогнозування сценаріїв та координацію заходів реагування. Ідея, викладена у роботах Я.І. Хміля та І.В. Слюсарчука, є не лише науково обґрунтованою, але й має стратегічне значення в контексті формування державної контррозвідувальної політики.

П’ятий важливий аспект полягає у доцільності імплементації моделі функціональної інтеграції представників СБУ безпосередньо в організації, що експлуатують об’єкти державної авіації, на зразок практики цивільної авіаційної безпеки. Такий підхід дозволить не лише посилити горизонтальні зв’язки між секторами, але й підвищити якість реагування на загрози за рахунок постійної присутності уповноважених осіб у структурі суб’єкта авіаційної діяльності.

Узагальнюючи викладене, можна констатувати, що потенціал впровадження міжнародних стандартів авіаційної безпеки в Україні є високим, однак його реалізація потребує системного підходу, що включає:

- нормативну гармонізацію законодавства України із вимогами стандартів ICAO, EASA та НАТО;
- інституційну інтеграцію на рівні створення міжвідомчих структур аналізу ризиків і управління безпекою;
- кадрову трансформацію, зокрема запровадження безперервного навчання, інструктажів і підвищення контррозвідувальної обізнаності;
- впровадження технічних рішень, що забезпечують захист від широкого спектру сучасних загроз;
- посилення культури безпеки як загальносуспільного явища, що охоплює всі рівні – від державного до інституційного.

Таким чином, результативне впровадження міжнародних стандартів є не лише технічним або нормативним процесом, а глибокою структурною реформою, що охоплює всі рівні функціонування системи національної безпеки України у сфері державної авіації.

РОЗДІЛ 4. НАПРЯМИ УДОСКОНАЛЕННЯ ПРАВОВИХ ТА ОРГАНІЗАЦІЙНИХ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ КОНТРРОЗВІДУВАЛЬНОГО РЕЖИМУ НА ОБ'ЄКТАХ ДЕРЖАВНОЇ АВІАЦІЇ

4.1. Інституційна модель контррозвідувального режиму в державній авіації: необхідність побудови вертикалі управління

Організація контррозвідувального режиму на об'єктах державної авіації України нині характеризується високим ступенем інституційної фрагментованості, що унеможливлює ефективну координацію заходів з виявлення, запобігання та нейтралізації загроз розвідувально-підривного характеру. Аналіз чинної моделі показує, що відповідальність за реалізацію контррозвідувального режиму розподілена між Службою безпеки України, Міністерством оборони України, Головним управлінням державної авіації України, окремими авіаційними формуваннями, військовими частинами, підрозділами Військової служби правопорядку, що створює правовий та організаційний дисбаланс.

На відміну від цивільної авіації, де реалізація політики безпеки здійснюється через централізовану вертикаль, очолювану Державною авіаційною службою України відповідно до статті 9 Повітряного кодексу України та Закону України "Про Державну програму авіаційної безпеки цивільної авіації" [1], у державній авіації відсутній уповноважений орган, відповідальний за інтегровану реалізацію контррозвідувального компоненту безпеки.

Як зазначається у статті 5 Закону України "Про контррозвідувальну діяльність", саме Служба безпеки України уповноважена на здійснення контррозвідувального забезпечення [16]. Проте в авіаційній сфері ця діяльність здійснюється переважно через загальну систему Департаменту військової контррозвідки без урахування галузевої специфіки об'єктів державної авіації, їхнього інженерного, інформаційного та операційного устрою. Водночас,

статтею 7 Повітряного кодексу України визначає, що Головне управління державної авіації України не здійснює координації заходів безпеки чи контррозвідки, на відміну від свого цивільного аналогу – Державної авіаційної служби України [1].

У контексті цього правового вакууму необхідним видається формування централізованої інституційної вертикалі управління контррозвідувальним режимом на об’єктах державної авіації за моделлю, схожою на цивільну. Йдеться не про створення дублюючого органу, а про інституціалізацію окремого структурного підрозділу в межах Служби безпеки України чи Міністерства оборони України (зокрема при Головному управлінні державної авіації України), уповноваженого на:

– координацію контррозвідувального забезпечення на об’єктах державної авіації,

– розробку типових інструкцій, методик і ризик-орієнтованих сценаріїв реагування,

– здійснення моніторингу загроз та зв’язку з авіаційними підрозділами сил безпеки та оборони,

– погодження режимних карт об’єктів у військово-авіаційній сфері.

Досвід країн-членів НАТО свідчить, що ключовим елементом ефективного захисту критичної інфраструктури є створення спеціалізованих координуючих центрів, що інтегрують зусилля розвідки, військового управління та охорони об’єктів (наприклад, Joint Intelligence Centers в США чи Joint Force Protection Units у Великобританії) [20; 25].

В умовах гібридної війни проти України, де аеродроми, командно-диспетчерські пункти, пункти бойового управління та інші об’єкти державної авіації є пріоритетними цілями для засобів радіоелектронної розвідки, агентурно-диверсійних груп, а також ударних безпілотників, питання побудови вертикалі управління контррозвідкою набуває не лише організаційного, а й стратегічного значення. У цьому зв’язку доцільним є також запровадження національного стандарту з організації контррозвідувального режиму, який би

слугував міжвідомчим нормативним фундаментом для синхронізації процедур доступу, охорони, взаємодії та обміну даними.

Таким чином, побудова інституційної вертикалі контррозвідувального режиму в державній авіації є необхідною умовою підвищення стійкості, керованості та уніфікації системи безпеки. Її реалізація має ґрунтуватися на принципах централізованого управління, ризик-орієнтованості, міжвідомчої взаємодії та інтеграції в євроатлантичну безпекову архітектуру.

4.2. Нормативне закріплення та гармонізація контррозвідувального режиму із міжнародними стандартами

У результаті проведеного аналізу, викладеного у попередніх розділах цієї роботи, стало очевидним, що національна система забезпечення контррозвідувального режиму на об’єктах державної авіації України не лише фрагментарна, але й концептуально не оформлена у вигляді чіткої нормативної моделі. Відсутність законодавчо закріпленого поняття “контррозвідувальний режим”, а також інституційно оформленої вертикалі управління у цій сфері створює загрозливі диспропорції у загальній архітектурі національної безпеки, особливо в умовах дії правового режиму воєнного стану та гібридних загроз.

Вважаю, що першочерговим завданням у цьому контексті має стати нормативне впорядкування сфери контррозвідувального забезпечення державної авіації через внесення змін до Повітряного кодексу України. Зокрема, потребує розширення повноважень уповноважених органів у сфері державної авіації. На сьогоднішній день Головне управління державної авіації України виконує, по суті, координаційну роль у межах Міністерства оборони України, однак позбавлене правового інструментарію, аналогічного тому, що має Державна авіаційна служба України у цивільному секторі. З метою подолання цієї асиметрії вбачаю за доцільне надати Міністерству оборони України або Головному управлінню державної авіації України (уповноваженому органу у сфері державної авіації) повноваження, співмірні із функціями Державної авіаційної служби України, у частині сертифікації безпекових служб,

затвердження інструкцій з охорони, погодження об’єктових планів безпеки, моніторингу рівня загроз, а також затвердження вимог до організації пропускного режиму та технічного забезпечення охорони об’єктів державної авіації.

Не менш важливим, на мій погляд, є законодавче закріплення поняття “контррозвідувальний режим”. У чинному законодавстві воно трапляється лише на рівні стратегічних документів та не має ні визначення, ні правового механізму реалізації (з відкритих джерел інформації). Пропоную законодавчо визначити цей режим як сукупність правових, організаційних, інформаційних та технічних заходів, що спрямовані на виявлення, попередження та нейтралізацію розвідувально-підривної, шпигунської, агентурної, диверсійної та інформаційної діяльності.

Окрім цього, в контексті державної авіації та заходів забезпечення безпеки державної авіації, пропоную сформулювати поняття “контррозвідувальний режим на об’єктах державної авіації” як спеціальний режим безпеки, що передбачає комплекс організаційно-правових, оперативно-розшукових, інформаційно-аналітичних, технічних та режимних заходів, спрямованих на:

1. виявлення, попередження, нейтралізацію та припинення розвідувально-підривної, диверсійної, терористичної, агентурної, кібернетичної та іншої діяльності, що здійснюється на шкоду національній безпеці України в сфері державної авіації;
2. забезпечення охорони критичних об’єктів державної авіації, захисту персоналу, інформаційних систем, озброєння, інженерної інфраструктури та повітряних суден;
3. функціонування скоординованої системи заходів контррозвідувального характеру, що реалізується уповноваженими органами сектору безпеки і оборони України за участі експлуатантів, органів військового управління, військових формувань, центральних органів виконавчої влади та відповідно до принципів багаторівневого управління ризиками.

Подальшим кроком у побудові системного підходу має стати розробка і ухвалення окремого Закону України “Про державну програму забезпечення безпеки державної авіації”, яка, на кшталт чинної Державної програми авіаційної безпеки цивільної авіації, визначатиме інституційний ланцюг взаємодії всіх суб’єктів — від Служби безпеки України і Міністерства оборони України до органів охорони, технічного забезпечення, військової поліції, а також охоплюватиме інтеграцію контррозвідувальних заходів у повсякденну експлуатацію об’єктів державної авіації. Вказана програма має ґрунтуватися не лише на внутрішніх правових положеннях, але й на міжнародних стандартах, рекомендованих практиках ICAO (Annex 17, Doc 8973), положеннях регламентів ЄС (зокрема, Regulation (EC) № 300/2008), а також доктринах НАТО.

У цьому контексті вважаю за необхідне ініціювати імплементацію положень AJP-2.2 “Allied Joint Doctrine for Counterintelligence” та AJP-3.14 “Allied Joint Doctrine for Force Protection” у нормативне поле України. Ці документи містять не лише визначення завдань контррозвідки у воєнній сфері, але й надають структурну модель дій з управління загрозами, координації заходів безпеки, а також планування контррозвідувального супроводу в умовах багатонаціональних операцій. Як показує досвід країн НАТО, контррозвідка є невід’ємним елементом force protection — захисту сил, інфраструктури та безперервності операцій.

Зважаючи на викладене, вважаю логічним і доцільним розробити “Національну доктрину охорони об’єктів державної авіації” — документ, який би об’єднав елементи фізичної, інженерної, кібернетичної, інформаційної безпеки та контррозвідки в уніфіковану систему із чітко прописаними вимогами щодо персоналу, процедур допуску, технічного оснащення та порядку взаємодії із суб’єктами Службою безпеки України. Така доктрина стане не лише логічним завершенням імплементації стандартів НАТО, але й дозволить Україні побудувати стійку модель забезпечення захисту стратегічних об’єктів у повітряному просторі.

У межах реалізації вищенаведених ініціатив, вважаю за необхідне створити систему підзаконного регулювання, яка включатиме спільні накази Міністерства оборони України, Служби безпеки України, Міністерства внутрішніх справ та інших уповноважених органів, спрямовані на:

- уніфікацію підходів до пропускного режиму та режимних заходів на об’єктах державної авіації;
- регламентацію процедур доступу до охоронюваних зон і повітряних суден;
- створення міжвідомчих центрів координації безпеки на авіаційних аеродромах;
- періодичне оновлення карт загроз та проведення спільних навчань.

Таким чином, запропонована модель нормативного забезпечення має на меті не лише усунути диспропорцію між цивільною та державною авіацією, а й підвищити інституційну стійкість України до сучасних загроз, забезпечити відповідність міжнародним стандартам, а також закласти правову основу для майбутньої інтеграції у євроатлантичний безпековий простір.

4.3. Упровадження системи управління ризиками та цифрових технологій моніторингу

Окрім запропонованих змін, варто приділити увагу запровадженні системі управління ризиками, яка на мою думку є дієвим інструментом при забезпеченні безпеки авіації. Формування ефективної системи контррозвідувального режиму на об'єктах державної авіації неможливе без впровадження системного управління ризиками, яке є одним із фундаментальних принципів сучасної авіаційної безпеки. Згідно з міжнародною практикою, управління ризиками не лише доповнює класичні заходи охорони, а й формує проактивний, гнучкий і адаптивний механізм реагування на сучасні багатовимірні загрози. Зокрема, у доктрині НАТО AJP-3.14 визначено, що управління ризиками є ключовим компонентом у захисті сил та інфраструктури, включаючи аеродроми, командні пункти, бази зберігання та логістичні вузли [15].

У державній авіації України на сьогоднішній день ризик-орієнтований підхід не є системно реалізованим. Наявна модель безпеки, переважно, залишається реактивною, акцентуючи увагу на фізичній охороні та ізольованих елементах протидії загрозам. Такий підхід є недостатнім в умовах гібридної війни, де загрози швидко змінюються, поєднують традиційні та нетрадиційні методи (кіберрозвідка, диверсії, психологічні операції), мають як зовнішнє, так і внутрішнє походження.

Запровадження системи управління ризиками (risk management system) повинно здійснюватися на основі міжнародних стандартів:

- ISO 31000: Risk Management – Guidelines;
- ICAO SSeMS (Security Systems for Safety Management);
- EASA Risk-Based Oversight Model;
- а також NATO Risk Management Doctrine, яка включає циклічну структуру:

  Визначення контексту (Establishing context) — формування розуміння зовнішнього та внутрішнього середовища, в якому функціонує об'єкт, визначення цілей, завдань, критеріїв прийнятності ризику, меж і зацікавлених сторін.

  Ідентифікація ризиків (Risk identification) — виявлення потенційних загроз, вразливостей та джерел небезпек, які можуть негативно вплинути на об'єкт або процес.

  Аналіз ризиків (Risk analysis) — визначення вірогідності реалізації ризику, масштабу можливих наслідків, побудова моделей впливу.

  Оцінювання ризиків (Risk evaluation) — порівняння рівнів ризиків із допустимими критеріями, визначення пріоритетів для подальшого реагування.

  Обробка ризиків (Risk treatment) — розробка та впровадження заходів щодо зниження, уникнення, передавання або прийняття ризику.

  Моніторинг та перегляд (Monitoring and review) — постійне спостереження за змінами у середовищі, ефективністю заходів та оновлення ризик-менеджменту відповідно до нових даних або подій.

Принципи побудови системи управління ризиками на об’єктах державної авіації мають включати:

1. Визначення контексту безпеки: ідентифікація місця об’єкта у стратегічній структурі оборони держави, його інфраструктурна значимість, критичні функції, рівень залежності від зовнішніх систем.
2. Аналіз та класифікація загроз: побудова профілю загроз, що включатиме диверсійні, технічні, агентурні, інформаційно-психологічні та кіберзагрози. На цьому етапі також оцінюється ймовірність їх реалізації та потенційна шкода.
3. Ідентифікація вразливостей: перевірка процедур охорони, фізичного стану периметра, стану систем зв'язку, функціоналу контррозвідувального супроводу, навченості персоналу.
4. Оцінка ризику та його пріоритезація: на основі методів матриці ризику (risk matrix), аналізу сценаріїв (scenario analysis), дерева несправностей (fault tree analysis), тощо.
5. Визначення заходів пом'якшення ризику (risk treatment): планування контррозвідувальних, інженерно-технічних, адміністративних, навчальних заходів.
6. Безперервний моніторинг, аудит та оновлення: цифрові платформи повинні забезпечувати постійне оновлення даних, аналіз інцидентів та адаптацію системи до нових умов [28].

Інтеграція цифрових рішень до управління ризиками має стати однією з ключових опор удосконалення контррозвідувального режиму. Серед пріоритетних напрямів:

- Розгортання об’єктових систем ситуаційного моніторингу: включаючи багаторівневу відеоаналітику, сенсорні системи вторгнення, контролери доступу з біометрією, автоматизовані пости охорони.
- Використання аналітичних платформ на основі штучного інтелекту для виявлення аномалій у поведінці персоналу, зміни в комунікаційних шаблонах, виявлення потенційної агентурної активності.

- Створення єдиної цифрової бази інцидентів, яка буде оновлюватись у режимі реального часу із залученням Служби безпеки України, Міністерства оборони України, Головним управлінням державної авіації України, частин та авіаційних баз.
- Впровадження цифрових risk maps – карт ризиків кожного авіаоб'єкта, що поєднують технічні, організаційні, територіальні та персональні вразливості.
- Геоінформаційні системи (ГІС) для відстеження переміщення персоналу, транспорту, вантажів на території об'єкта [29].

На стратегічному рівні необхідно створити Національний центр авіаційного ризик-менеджменту (можливо об'єднаний – цивільно-військовий), до повноважень якого увійде:

- методичне забезпечення всіх об'єктів державної авіації;
- координація моніторингу загроз;
- розробка стандартів оцінки;
- навчання персоналу;
- ведення статистики інцидентів;
- узагальнення та аналіз контррозвідувальної інформації.

Також важливо впровадити обов'язкову практику формування "профілю ризику" для кожного об'єкта державної авіації із щорічною актуалізацією, що має бути закріплено на нормативному рівні.

Для ефективного запровадження зазначених механізмів необхідна розробка та ухвалення змін до Повітряного кодексу України щодо делегування повноважень у сфері моніторингу ризиків у державній авіації, підзаконних актів Міністерства оборони України та Служби безпеки України, які регулюватимуть збір, зберігання та обробку даних ризиків, спільного порядку взаємодії суб'єктів сектору безпеки і оборони в частині цифрового аналізу загроз, інструкцій для авіаційних частин щодо організації об'єктових центрів ситуаційної обізнаності.

Упровадження системи управління ризиками та цифрових технологій моніторингу становить одну з ключових передумов формування ефективного,

адаптивного та взаємосумісного контррозвідувального режиму в авіаційній сфері. Без такої реформи неможливо забезпечити ні стійкість державної авіації до гібридних загроз, ні інтеграцію у євроатлантичні структури. Орієнтація на стандарти ICAO, EASA та НАТО, доповнена цифровою трансформацією процедур безпеки, здатна радикально підвищити рівень захищеності критичної інфраструктури та зміцнити потенціал обороноздатності держави.

4.4. Кадровий потенціал та формування культури контррозвідувальної обізнаності

Ефективне функціонування контррозвідувального режиму на об'єктах державної авіації потребує не лише належного нормативного, інституційного чи технічного забезпечення, а й наявності підготовленого кадрового ресурсу. Людський чинник відіграє визначальну роль у реалізації всіх безпекових заходів, починаючи від ідентифікації потенційних ризиків і закінчуючи оперативною взаємодією з контррозвідувальними органами. У зв'язку з цим, ключового значення набуває формування професійного кадрового потенціалу, здатного діяти в умовах складної та динамічної загрозової ситуації.

Станом на сьогодні в Україні відсутня цілісна система професійної підготовки фахівців саме у сфері контррозвідувального забезпечення державної авіації. У переважній більшості випадків залучення персоналу до контррозвідувальних заходів здійснюється фрагментарно: у межах загальних безпекових інструктажів, планових занять чи заходів державної таємниці. Такий підхід не забезпечує достатнього рівня стійкості до складних гібридних загроз, які поєднують фізичний, інформаційний, технічний, психологічний та кіберкомпоненти.

Найбільш актуальними кадровими проблемами в авіаційній сфері державного призначення є:

- дефіцит кваліфікованих фахівців з досвідом роботи у сфері авіаційної безпеки та контррозвідки;

- відсутність спеціалізованих навчальних програм, орієнтованих на поєднання авіаційної специфіки з контррозвідувальною діяльністю;
- недостатній рівень мотивації та ротації персоналу на об’єктах з підвищеним рівнем загроз;
- нерівномірність рівня підготовки між різними відомствами, які забезпечують охорону та функціонування об’єктів державної авіації.

У цьому контексті доцільним є запровадження багаторівневої системи кадрового забезпечення, яка включала б:

1. Формування цільового освітнього компоненту. Розробка програм підготовки та перепідготовки кадрів у профільних вищих військових навчальних закладах та інститутах сектору безпеки і оборони з фокусом на авіаційну специфіку контррозвідувальної діяльності.
2. Створення міжвідомчого навчального центру з підготовки персоналу для об’єктів державної авіації, в якому реалізовувалися б модулі з виявлення розвідувально-підривної діяльності, оцінки ризиків, реагування на інциденти, взаємодії з контррозвідувальними органами.
3. Систематичне впровадження контррозвідувальних інструктажів для всього особового складу, залученого до діяльності на об’єктах державної авіації, із щорічною атестацією рівня знань, у тому числі з прикладних кейсів.
4. Впровадження єдиних міжвідомчих стандартів компетенцій, які б визначали обсяг знань, навичок і поведінкових індикаторів фахівців з безпеки на всіх рівнях — стратегічному, оперативному, тактичному.
5. Підготовка інструкторів і тренерів з числа представників військової контррозвідки, які б забезпечували фаховий супровід на об’єктах, адаптований до конкретних умов дислокації, ризиків і функціональних завдань.

Паралельно з розвитком кадрового потенціалу має відбуватися формування культури контррозвідувальної обізнаності — тобто сталої системи

цінностей, переконань і поведінкових моделей, орієнтованих на превентивне мислення, пильність, відповідальність і готовність до дій у разі загроз.

Контррозвідувальна культура включає такі ключові складові:

- психологічну готовність персоналу до усвідомлення важливості безпекових процедур;
- знання ознак розвідувально-підривної діяльності та методів прихованого спостереження;
- готовність інформувати уповноважені органи про підозрілі дії або ситуації;
- відкритість до міжвідомчої взаємодії та дотримання процедур реагування;
- вміння діяти в умовах кібер-, інформаційної та психологічної дестабілізації.

Важливою частиною культури є інституційна підтримка зворотного зв'язку: створення механізмів анонімного інформування, захист викривачів, аналіз уроків інцидентів та їх узагальнення у внутрішньовідомчих рекомендаціях.

Формування такої культури має супроводжуватися інтеграцією стандартів НАТО, зокрема вимог AJP-3.14 щодо підготовки персоналу у сфері захисту сил (Force Protection), а також доктрини AJP-2.2, яка встановлює принципи контррозвідувальної діяльності, включаючи персональну відповідальність за інформування про потенційні загрози.

Показовим прикладом у цій сфері є досвід Сполучених Штатів Америки, зокрема практика впровадження Програми контррозвідувальної обізнаності та інструктажу, визначеної Інструкцією Міністерства оборони США № 5240.6. В її основі — вимога щорічного обов'язкового інструктажу всього особового складу, як військового, так і цивільного, щодо ознак шпигунства, диверсійної чи терористичної діяльності, а також негайного повідомлення про такі випадки до органів військової контррозвідки.

Крім цього, американський підхід передбачає чітке нормативне закріплення обов'язків командирів щодо реалізації контррозвідувальної обізнаності, зокрема моніторингу виконання інструктажів, перевірки знань,

аналізу інцидентів та звітування. Відповідні дані узагальнюються в річних звітах, що дозволяє формувати емпіричну базу для стратегічного аналізу загроз та визначення найбільш ефективних форм реагування.

Цей досвід доцільно адаптувати в українських реаліях, сформувавши багаторівневу модель кадрового забезпечення контррозвідувального режиму, яка передбачала б:

- Обов’язкове впровадження системи регулярних контррозвідувальних інструктажів на всіх об’єктах державної авіації, з урахуванням специфіки авіаційної діяльності, елементів гібридної загрози та процедур фіксації підозрілої активності;
- Запровадження внутрішніх тренінгових програм, що охоплюють прикладні сценарії, юридичні наслідки порушень, профілактику витоку інформації, методи виявлення ознак зовнішнього впливу;
- Формалізацію зобов’язання командирів та керівників об’єктів державної авіації щодо організації навчального процесу, контролю участі персоналу та оперативної передачі повідомлень до контррозвідувальних органів;
- Імплементацію системи оцінювання ефективності програми через створення внутрішньої звітності, збору статистичних даних про рівень загроз, кількість виявлених інцидентів, рівень обізнаності персоналу тощо.

Кадрова політика в системі контррозвідувального режиму має бути переорієнтована з реагування на інциденти на превентивне моделювання загроз через професіоналізацію персоналу, стандартизацію знань і поведінкових практик. Культура контррозвідувальної обізнаності повинна стати інструментом підвищення резистентності авіаційної інфраструктури державного призначення до гібридних та асиметричних загроз, а сам персонал — ключовим суб’єктом у моделі стійкості держави.

4.5. Етапи впровадження, контроль та індикатори ефективності нової моделі

Реалізація модернізованої моделі забезпечення контррозвідувального режиму на об’єктах державної авіації потребує чіткої поетапної імплементації, яка враховує як інституційні можливості України, так і стратегічну динаміку безпекового середовища. Створення нової вертикалі управління, нормативне оновлення та інтеграція цифрових і аналітичних рішень мають відбуватись поетапно, з відповідною системою моніторингу ефективності, контролю реалізації та зовнішньої оцінки результатів.

Короткострокова перспектива:

- Внесення змін до Повітряного кодексу України з наданням Головним управлінням державної авіації України або іншому спеціалізованому органу повноважень, аналогічних до Державної авіаційної служби України в цивільному секторі;
- Нормативне закріплення поняття “контррозвідувальний режим на об’єктах державної авіації” та визначення його основних елементів;
- Створення міжвідомчої робочої групи з розробки Доктрини охорони сил і державної програми безпеки державної авіації;
- Запуск пілотного проекту регулярного контррозвідувального інструктажу на окремих об’єктах державної авіації.

Середньострокова перспектива:

- Прийняття Закону України “Про забезпечення безпеки державної авіації” як нормативної основи для створення єдиної системи безпеки в державному авіаційному сегменті;
- Розробка та впровадження уніфікованих стандартів взаємодії між суб’єктами (Міністерством оборони України, Службою безпеки України, Головним управлінням державної авіації України, Державної прикордонної служби тощо);

- Побудова національної системи цифрового моніторингу ризиків і розгортання інформаційно-аналітичної платформи під координацією Служби безпеки України;
- Актуалізація відомчих інструкцій, приведення їх у відповідність до AJP-2.2, AJP-3.14 та інших документів НАТО.

Довгострокова перспектива:

- Повноцінна інтеграція нової системи в архітектуру сектору безпеки та оборони, у тому числі в контексті перспектив членства в НАТО;
- Функціонування повноцінної вертикалі управління в державній авіації з чітким розподілом повноважень, процедур реагування та системою партнерського контролю;
- Підготовка незалежного аналітичного звіту (у форматі “White Paper”) щодо результатів реалізації нової моделі безпеки державної авіації.

Для забезпечення об'єктивного оцінювання ефективності імплементації пропонуються такі індикатори функціонального та результативного характеру:

- Операційні індикатори:
    - Кількість проведених навчань і тренувань із контррозвідувальної обізнаності;
    - Рівень охоплення особового складу програмами підготовки;
    - Час реагування на інциденти та кількість випадків оперативного інформування контррозвідувальних органів.
- Системні індикатори:
    - Ступінь уніфікації нормативних документів;
    - Частка об’єктів, охоплених інтегрованою системою цифрового моніторингу;
    - Частота оновлення протоколів реагування відповідно до оцінки ризиків.
- Стратегічні індикатори:
    - Зменшення кількості підтверджених інцидентів шпигунства, диверсій або витоку інформації;

- Рівень узгодженості українських підходів до авіаційної безпеки з вимогами AJP-3.14 та ICAO Doc 8973;
- Позитивна оцінка з боку партнерських структур (наприклад, НАТО, EUAM, EASA тощо) щодо інтеграції контррозвідувального компоненту [30].

Оцінка ефективності нової моделі має здійснюватися через поєднання внутрішнього аудиту, зовнішнього моніторингу та партнерського контролю. Передбачається:

- Запровадження щорічного відомчого аудиту реалізації програми, що охоплюватиме аналіз ефективності заходів, дотримання стандартів та ступінь реагування на інциденти;
- Формування експертної наглядової ради за участі представників органів державної влади, наукової спільноти, міжнародних партнерів;
- Проведення експертних оцінок та інституційного peer-review за участі міжнародних аудиторських структур (на кшталт EASA або TAIEX), що дозволить забезпечити транспарентність і відповідність міжнародним стандартам;
- Запровадження інструментів внутрішньої аналітики з виведенням інтегрального індикатора безпеки, що дозволятиме керівникам об'єктів та органам управління щомісячно отримувати зведену інформацію про рівень ризиків, динаміку інцидентів і ступінь відповідності стандартам.

Визначення чітких етапів впровадження, запровадження індикаторів ефективності та створення незалежного механізму моніторингу дозволить не лише забезпечити контроль над реалізацією нової моделі безпеки, а й посилити стратегічну прозорість і підзвітність у сфері авіаційної безпеки державного сектору. Такий підхід є передумовою для уніфікації із євроатлантичними підходами, підвищення довіри з боку партнерів і забезпечення стійкості до сучасних гібридних загроз.

ВИСНОВКИ ДО РОЗДІЛУ 4

Розділ 4 було присвячено формулюванню стратегічних та операційних підходів до вдосконалення правових і організаційних механізмів забезпечення контррозвідувального режиму на об’єктах державної авіації України. Комплексна оцінка чинної ситуації, проведена в попередніх розділах, засвідчила: наявна модель охоплення контррозвідувальними заходами авіаційної інфраструктури військового призначення є фрагментованою, нормативно неуніфікованою та інституційно нефокусованою. Це, своєю чергою, формує розрив між рівнем загроз, які продукує сучасне безпекове середовище, і спроможністю системи державного управління адекватно на них реагувати.

У межах цього розділу обґрунтовано п’ять ключових векторів реформування, які, в комплексі, утворюють оновлену модель контррозвідувального режиму на об’єктах державної авіації — модель, яка має відповідати стандартам євроатлантичної спільноти, водночас враховуючи специфіку українського сектору безпеки в умовах воєнного стану.

По-перше, аргументовано необхідність створення централізованої інституційної вертикалі управління, яка забезпечуватиме безперервну координацію, аналітику та методичне керівництво у сфері контррозвідувального супроводу об’єктів державної авіації. Відсутність єдиного уповноваженого органу, що має повноваження, аналогічні тим, які здійснює Державна авіаційна служба України в цивільному сегменті, призводить до дублювання функцій, відомчої ізольованості та фрагментарності у прийнятті рішень. Передбачено можливість створення такого органу як у межах Служби безпеки України (через спеціалізований центр або управління), так і в рамках Міністерства оборони України — зокрема через трансформацію функцій Головне управління державної авіації України з координаційних у регуляторно-керівні.

По-друге, обґрунтовано необхідність нормативного оновлення — від зміни Повітряного кодексу України до формулювання та закріплення поняття “контррозвідувальний режим” на законодавчому рівні. У поточній правовій

архітектурі України відсутнє як визначення самого терміну, так і інституціональний контекст його реалізації. Запропоновано модель контррозвідувального режиму як правового механізму, що поєднує елементи фізичного, інженерного, кібернетичного, інформаційного та оперативно-розшукового захисту. Водночас пропонується розробити Закон України "Про державну програму забезпечення безпеки державної авіації", аналогічний до вже чинної державної програми у сфері цивільної авіації.

По-третє, акцент зроблено на запровадженні системи управління ризиками, як фундаментального елементу сучасної моделі безпеки, що дозволяє не лише фіксувати загрози постфактум, але й прогнозувати їх, моделювати сценарії розвитку інцидентів, формувати профілі вразливостей об'єктів. У запропонованій моделі інтегруються міжнародні стандарти (ISO 31000, ICAO SSeMS, AJP-3.14), створюється система цифрового моніторингу загроз, автоматизовані ситуаційні центри та єдина база даних інцидентів. На макрорівні передбачено формування Національного центру авіаційного ризик-менеджменту з повноваженнями методичного забезпечення та координації.

По-четверте, окрему увагу приділено кадровому забезпеченню та формуванню контррозвідувальної культури. Оскільки навіть найсучасніші системи безпеки залишаються неефективними без підготовленого персоналу, запропоновано концепт багаторівневої моделі професіоналізації кадрів: від створення освітніх програм до стандартизації інструктажів, атестації та впровадження повноцінної культури превентивної контррозвідувальної обізнаності. До розробки цієї моделі було адаптовано досвід США, де діє обов'язкова програма контррозвідувального інструктажу для всього персоналу, а також сформовано нормативні вимоги до командирів і системи моніторингу ефективності навчання.

П'ятий і фінальний компонент — це етапи імплементації та система моніторингу ефективності. У структурі цього підпункту запропоновано поетапну карту реалізації (коротко-, середньо- та довгострокову), визначено ключові індикатори функціональної ефективності (реакція на загрози, частота навчань,

ступінь уніфікації протоколів), індикатори безпеки (динаміка інцидентів, охоплення цифровим моніторингом), а також систему внутрішнього й зовнішнього аудиту. Передбачено формування експертної наглядової ради за участі міжнародних партнерів (NATO, EUAM, EASA), яка б здійснювала регулярне інституційне peer-review.

Узагальнюючи викладене, можна стверджувати, що реалізація запропонованої моделі дозволить не лише подолати правову та інституційну асиметрію між цивільною та державною авіацією, але й створити нову архітектоніку національного авіаційного захисту, яка відповідатиме стандартам НАТО та ІСАО, буде адаптована до гібридного характеру загроз та спроможна забезпечити стійкість ключових об’єктів державної авіації в умовах як війни, так і стратегічного партнерства. Такий підхід є не лише відповіддю на актуальні безпекові виклики, але й передумовою для формування модернізованої парадигми контррозвідувальної діяльності у воєнно-авіаційному секторі України.

ВИСНОВКИ

Магістерське дослідження на тему “Правові та організаційні засади контррозвідувального режиму на об’єктах державної авіації” було присвячене комплексному аналізу чинного нормативно-правового забезпечення, інституційної структури, наявних викликів і перспективних шляхів удосконалення системи контррозвідувального забезпечення стратегічно важливих об’єктів державної авіації в Україні в умовах воєнного стану, гібридних загроз і поступової інтеграції до євроатлантичного безпекового простору.

Узагальнення результатів дослідження дозволяє зробити такі системні висновки:

1. Систематизація результатів дослідження

По-перше, виявлено фундаментальну проблему відсутності системного визначення та нормативної конкретизації поняття “контррозвідувальний режим” як правової категорії. У чинному законодавстві це поняття наявне переважно в стратегічних або міжвідомчих документах, не має чіткого змістовного наповнення, не конкретизується у законодавчих або підзаконних актах, і відповідно — не супроводжується механізмами реалізації.

По-друге, встановлено, що нормативно-правова архітектура авіаційної безпеки в Україні є асиметричною: у той час як цивільна авіація має законодавчо оформлену вертикаль (на основі Повітряного кодексу України, Державної програми авіаційної безпеки, стандартів ІСАО тощо), сектор державної авіації не має аналогічного рівня нормативного регулювання. Відсутній спеціальний закон або програма, що регулювала б уніфіковану систему безпеки державної авіації з урахуванням контррозвідувального компоненту.

По-третє, у результаті аналізу організаційної структури встановлено, що система контррозвідувального забезпечення функціонує у фрагментованому, неінтегрованому вигляді. Відповідальність розподілена між Службою безпеки України, Міністерством оборони України, Головним управлінням державної

авіації України, командуваннями видів Збройних Сил України, підрозділами військової служби правопорядку, інших військових формувань, утворених відповідно до Законів України при цьому відсутній єдиний координуючий орган, уніфіковані процедури, типові інструкції або протоколи міжвідомчої взаємодії. Цей стан речей значно ускладнює оперативність реагування на загрози та створює прогалини в зонуванні відповідальності.

По-четверте, виявлено відсутність ризик-орієнтованого підходу у плануванні та реалізації заходів безпеки на об'єктах державної авіації. Аналіз продемонстрував, що на більшості об'єктів не ведеться фіксація ризиків, не застосовуються цифрові карти вразливостей, не функціонують ситуаційні центри або об'єктові пункти управління інцидентами. Поряд із цим, інформаційно-аналітичне забезпечення контррозвідувальних заходів часто носить несистемний характер, обмежується фрагментарною оперативною роботою, що значно знижує ефективність реагування.

По-п'яте, підтверджено низький рівень кадрової підготовки, відсутність уніфікованих стандартів контррозвідувальної обізнаності, недостатній рівень міжвідомчого навчання та бракує обов'язкової інституціоналізованої моделі регулярного контррозвідувального інструктажу. У процесі аналізу було ідентифіковано суттєві диспропорції в практиках підготовки між різними об'єктами та підрозділами.

По-шосте, на основі компаративного аналізу було встановлено, що країни-члени НАТО, зокрема Сполучені Штати Америки та Великобританія, будують системи контррозвідувального забезпечення критичної інфраструктури на засадах централізованого управління, нормативного визначення обов'язків особового складу, впровадження аналітичного моніторингу та індикаторів ефективності. Цей досвід може бути адаптований до українських реалій через доктринальне та нормативне імплементування стандартів AJP-2.2, AJP-3.14, ISO 31000 тощо.

2. Практичні рекомендації для національних органів авіаційної безпеки та оборони

На підставі результатів дослідження доцільно реалізувати наступні практичні кроки:

- Нормативні ініціативи:
  - Внести зміни до Повітряного кодексу України, закріпивши повноваження Головного управління державної авіації України або іншого уповноваженого органу щодо безпеки державної авіації;
  - Законодавчо визначити поняття “контррозвідувальний режим на об’єктах державної авіації”;
  - Прийняти Закон України “Про державну програму безпеки державної авіації”;
  - Імплементувати положення AJP-2.2, AJP-3.14, ISO 31000, Doc 8973 у нормативне поле України, в частині державної авіації.
- Інституційні заходи:
  - Створити централізований підрозділ координації безпеки об’єктів державної авіації при Службі безпеки України або Міністерстві оборони України;
  - Побудувати міжвідомчу систему цифрового управління ризиками;
  - Ініціювати створення ситуаційних центрів або авіаційного командного пункту безпеки.
- Кадрова політика:
  - Впровадити обов’язкові контррозвідувальні інструктажі для всього персоналу на об’єктах державної авіації;
  - Розробити стандарти компетентності фахівців у сфері авіаційної безпеки;
  - Інституціоналізувати підготовку інструкторів з контррозвідувальної обізнаності.
- Цифрова трансформація:
  - Розгорнути електронні карти ризиків, системи ситуаційного відеоспостереження, індикатори вразливостей;

- Запровадити цифрову систему внутрішньої звітності й оцінки ефективності заходів безпеки.

3. Перспективи подальших наукових досліджень

У процесі реалізації положень магістерського дослідження виникає потреба в більш глибокому опрацюванні ряду науково-прикладних тем, зокрема:

- Розробка універсальної моделі державного управління безпекою об’єктів критичної авіаційної інфраструктури з урахуванням багатоступеневої загрозової динаміки;
- Аналіз ефективності міжвідомчої координації в рамках єдиної системи ситуаційних центрів;
- Створення системи цифрової обізнаності командирів та офіцерів безпеки в умовах гібридної війни;
- Оцінка ефективності впровадження індикаторів контррозвідувальної стійкості, зокрема в контексті адаптації інструментарію НАТО;
- Моделювання систем превентивного управління кризами у секторі державної авіації.

Результати магістерського дослідження дають підстави стверджувати, що сучасна система контррозвідувального забезпечення державної авіації України потребує глибокої трансформації. Необхідна модернізація має охоплювати не лише юридичне оформлення, а й інституційне, процедурне, кадрове, аналітичне та технологічне переосмислення. Лише за умов комплексного оновлення та орієнтації на міжнародні стандарти можливо сформувати ефективну, резилієнтну, адаптивну і сумісну з НАТО модель контррозвідувального режиму, що забезпечить захист державної авіації в умовах стратегічної нестабільності та глобальних викликів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Повітряний кодекс України : Кодекс України від 19.05.2011 № 3393-VI // Відомості Верховної Ради України. 2011. № 48-49. Ст. 536.
2. Положення про регулювання діяльності державної авіації України: наказ МОУ від 10.01.2014 № 14; зареєстровано в Мін'юсті України 23.01.2014 за № 149/24926.
3. Романов М. С. Контррозвідувальний режим в Україні: підручник. — Острог : Видавництво НУ "Острозька академія", 2024. — 512 с.
4. NATO Standardization Agreement (STANAG) 3117. Aeronautical Information Publications. – Edition 6. – Brussels : NATO Standardization Office, 2019. – 64 p.
5. NATO Standard AJP-3.3. Allied Joint Doctrine for Air and Space Operations. – Edition C, Version 1. – Brussels : NATO Standardization Office, February 2021. – 152 p.
6. Указ Президента України № 56/2022 "Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 р. 'Про Стратегію забезпечення державної безпеки'" [Електронний ресурс] — Офіц. сайт Президента України. URL: https://www.president.gov.ua/documents/562022-41377.
7. Романов М. С. Контррозвідувальний режим в Україні: функції та призначення в умовах військової агресії Російської Федерації [Електронне видання] : стаття, 11 ст. // URL: https://eprints.oa.edu.ua/.../Romanov-19.01.%2020.pdf.
8. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 13 вересня 2017 р. 'Про Концепцію забезпечення контррозвідувального режиму в Україні'" № 310/2017, [Електронний ресурс] // URL: https://zakon.rada.gov.ua/laws/show/310/2017.

9. Регламент (ЄС) № 300/2008 від 11.03.2008 “Про спільні правила у сфері авіаційної безпеки цивільної авіації…” [Електронний ресурс] // URL: https://zakon.rada.gov.ua/laws/show/984_018-08
10. Міжнародна організація цивільної авіації (ICAO). Додаток 17 до Конвенції про міжнародну цивільну авіацію. Авіаційна безпека. Захист міжнародної цивільної авіації від актів незаконного втручання (Annex 17 to the Convention on International Civil Aviation. Security – Safeguarding International Civil Aviation Against Acts of Unlawful Interference). – 11th ed. – Montréal : ICAO, 2020. – 98 p.
11. Міжнародна організація цивільної авіації (ICAO). Додаток 19 до Конвенції про міжнародну цивільну авіацію. Управління безпекою польотів (Annex 19 to the Convention on International Civil Aviation. Safety Management). – 2nd ed. – Montréal : ICAO, 2016. – 46 p.
12. Міжнародна організація цивільної авіації (ICAO). Doc 8973 – Aviation Security Manual. – 11th ed. – Montréal : ICAO, 2020. – 415 p.
13. Закон України “Про Державну програму авіаційної безпеки цивільної авіації” [Електронний ресурс] // URL: https://zakon.rada.gov.ua/laws/show/1965-19/
14. Міністерство оборони України. Наказ від 21.03.2016 № 152 “Про затвердження Порядку організації охорони об’єктів державної авіації”; зареєстровано в Мін’юсті України 08.04.2016 за № 526/28656.
15. NATO Standard AJP-3.14. Allied Joint Doctrine for Force Protection. – Edition B, Version 1. – Brussels : NATO Standardization Office, October 2024. – 112 p.
16. Про контррозвідувальну діяльність : Закон України від 26.12.2002 № 378-IV (ред. станом на 01.05.2025) [Електронний ресурс] // Верховна Рада України. – URL: https://zakon.rada.gov.ua/laws/show/378-15
17. Про Службу безпеки України : Закон України від 25.03.1992 № 2229-XII (ред. станом на 01.05.2025) [Електронний ресурс] // Верховна Рада України. – URL: https://zakon.rada.gov.ua/laws/show/2229-12.

18. Наказ Державної служби України з нагляду за забезпеченням безпеки авіації № 482 від 05.07.2006 “Про затвердження Положення про взаємодію в контрольованій зоні авіаційних суб'єктів служб авіаційної безпеки…”; зареєстровано в Мін’юсті України 27.07.2006 за № 881/12755.
19. Леус С. А., Архипов О. Є. Аналіз взаємозв’язку між загрозами, вразливостями та ризиком в автоматизованих системах управління технологічними процесами : УДК 004.056 // Нац. техн. ун-т “КПІ” [Електронний ресурс] // URL: https://ela.kpi.ua/bitstreams/558533d1-b9c9-4049-a38e-7b259981bbb1/download.
20. Department of Defense Directive No. 5240.06 [Електронний ресурс] // URL: https://fas.org/irp/doddir/dod/d5240_06.pdf.
21. Кравченко Р. М. Щодо деяких підходів до вдосконалення контррозвідувального пошуку органів військової контррозвідки СБ України з урахуванням аналізу законодавства США // Інформація і право. – 2019. – № 2(29). – С. 87–94. – [Електронний ресурс]. – Режим доступу: https://bit.ly/3VnFZjB.
22. Global Aviation Security Plan. Second edition, 2024 [Електронне видання] // ICAO. URL: https://elibrary.icao.int/reader/423587/
23. Офіційний сайт EASA [Електронний ресурс] // URL: https://www.easa.europa.eu/en/regulations#regulations-standardisation-inspections
24. NATO Standard AJP-2. Allied Joint Doctrine for Intelligence Procedures. – Brussels : NATO Standardization Office, 2016. – 154 p.
25. NATO Standard AJP-3.14 Allied Joint Doctrine for Force Protection. — [стандарт НАТО].
26. Слюсарчук І. В. Контррозвідувальна стратегія України як основа інтеграції сектору безпеки та суспільства : тези доповіді Всеукр. наук.-практ. конф. – Київ : ВПЦ «Київський Університет», 2017. – С. 105.

27. Хміль Я. І. До питання контррозвідувальної діяльності СБ України в умовах зовнішньої агресії : тези доповіді Всеукр. наук.-практ. конф. – Київ : ВПЦ «Київський Університет», 2017. – С. 119.
28. ISO 31000:2018 – Risk management — Guidelines [Електронний ресурс] // URL: https://zakon.isu.net.ua/...dstu_iso_31000_2018.pdf
29. EASA Risk Based Oversight Model : European Union Aviation Safety Agency, 2020 [Електронний ресурс] // URL: https://www.easa.europa.eu/en/domains/safety-management/safety-risk-management
30. Міністерство оборони України. Наказ 01.07.2013 № 441 “Про затвердження Інструкції з експлуатації аеродромів державної авіації України”; зареєстровано в Мін’юсті України 22.07.2013 за № 1229/23761.
31. Мошняга Л., Єрмоленко-Князєва Л. Безпека цивільної авіації як об’єкт кримінально-правового регулювання : УДК 342. // [Електронний ресурс] // URL: http://journal-app.uzhnu.edu.ua/article/...