Засади державної політики захисту об’єктів критичної інфраструктури в авіаційній галузі

Андрій Кузнік[1]

Опубліковано	Секція	УДК
28.12.2024	Право	338.583+657.471

DOI: https://doi.org/10.5281/zenodo.15120105

Анотація. У статті здійснено ґрунтовний аналіз засад державної політики захисту об’єктів критичної інфраструктури в авіаційній галузі України з урахуванням викликів сучасного безпекового середовища, спричиненого збройною агресією рф та трансформаціями глобального простору. Визначено особливості системи загроз для об’єктів авіаційної інфраструктури, зокрема комплексну природу ризиків, які виходять далеко за межі авіаційної безпеки, охоплюючи гібридні, терористичні, кібер- та воєнні загрози. Обґрунтовано важливість об'єктів авіаційного транспорту як елементів критичної інфраструктури держави, що відіграють визначальну роль не лише в забезпеченні мобільності, а й у реалізації оборонних, гуманітарних та соціально-економічних функцій. Розглянуто вплив міжгалузевих і транснаціональних залежностей критичної інфраструктури, включаючи інформаційну взаємозалежність, на формування політики її захисту.

Особливу увагу приділено кіберскладовій безпеки, зокрема викликам, пов’язаним із захистом автоматизованих систем управління, телекомунікаційних мереж та хмарних середовищ, що активно використовуються в авіаційній сфері. Визначено ключові принципи державної політики у сфері захисту ІТ-компонентів критичної інфраструктури, зокрема нормативну визначеність, міжсекторальну інтеграцію, персональну відповідальність операторів, дозвільний характер діяльності, а також пріоритет недопущення технологічної залежності від ворожих держав.

На підставі вивчення міжнародного досвіду, насамперед практик ЄС та НАТО, підкреслено необхідність упровадження проактивного підходу до формування державної політики, яка ґрунтується на системності, інтеграції функціонального розподілу повноважень між компетентними органами та ефективному державно-приватному партнерстві. Запропоновано розглядати взаємодію держави та приватного сектору як фундамент для забезпечення сталої безпеки аеропортів, де питання довіри, цінності, реалістичних очікувань і постійного діалогу між сторонами виходять на перший план. Висвітлено європейські підходи до інституціоналізації партнерств, їх нормативного забезпечення, обміну інформацією та формування спільних стратегій реагування на інциденти.

Окремо охарактеризовано нормативну основу реалізації політики авіаційної безпеки в Україні на прикладі Програми авіаційної безпеки Міжнародного аеропорту

[1] аспірант НА СБ України

«Бориспіль», із виокремленням ролі Служби безпеки України та Міністерства внутрішніх справ у системі реагування на акти незаконного втручання. Зроблено висновок про необхідність системного переосмислення принципів управління захистом об'єктів критичної інфраструктури авіаційної галузі в умовах війни, посилення ролі національних інституцій, розробки єдиної стратегії взаємодії суб'єктів у цій сфері та адаптації законодавства до сучасних викликів.

Ключові слова: критична інфраструктура, об'єкти критичної інфраструктури, захист об'єктів, безпека, авіаційна галузь, нормативно-правове регулювання, суб'єкти, СБ України, МВС України.

Principles of state policy for the protection of critical infrastructure in the aviation industry

Abstract. The article provides an in-depth analysis of the principles of state policy for the protection of critical infrastructure objects in Ukraine's aviation sector, taking into account the challenges of the current security environment caused by the armed aggression of the russian federation and global transformations. The study identifies the specific threat landscape for aviation infrastructure, highlighting the complex nature of risks that go far beyond aviation safety, encompassing hybrid, terrorist, cyber, and military threats. The importance of aviation transport facilities as elements of national critical infrastructure is substantiated, emphasizing their vital role not only in mobility but also in fulfilling defense, humanitarian, and socio-economic functions. The study explores the influence of intersectoral and transnational dependencies—particularly informational interdependence—on the development of protection policy for such infrastructure.

Special attention is paid to the cybersecurity dimension, including challenges related to the protection of automated control systems, telecommunications networks, and cloud environments extensively used in the aviation field. The article outlines key principles of state policy for securing IT components of critical infrastructure, such as legal clarity, intersectoral integration, personal responsibility of operators, permit-based activity, and the priority of minimizing technological dependence on hostile states.

Drawing on international experience, especially from the EU and NATO, the paper emphasizes the need to implement a proactive, systematic approach to state policy, based on a functional distribution of powers among competent authorities and effective public-private partnerships. The interaction between the state and private sector is proposed as a cornerstone of sustainable airport security, with particular focus on trust, value, realistic expectations, and continuous dialogue as prerequisites for successful cooperation. European approaches to institutionalizing such partnerships, regulatory support, information sharing, and joint incident response planning are discussed.

The article also examines the regulatory framework for implementing aviation security policy in Ukraine, using the Aviation Security Program of Boryspil International Airport (2020) as a case study. The roles of the Security Service of Ukraine and the Ministry of Internal Affairs in responding to unlawful interference are highlighted. The study concludes that there is a pressing need to rethink the governance model for critical infrastructure protection in aviation during wartime, strengthen the role of national institutions, develop an integrated coordination strategy among actors, and adapt legislation to contemporary threats.

Keywords: critical infrastructure, critical infrastructure objects, object protection, security, aviation sector, regulatory framework, subjects, Security Service of Ukraine, Ministry of Internal Affairs of Ukraine.

Вступ

Постановка проблеми. Критична інфраструктура підтримує життєдіяльність соціуму, сприяє забезпеченню економічного розвитку, національної безпеки, функціонуванню громад. Мережі, що об'єднують елементи критичної інфраструктури у єдину систему, є складними, взаємозалежними та взаємопов'язаними і становлять собою основу сталого розвитку. Руйнація одного елементу може мати вплив на різні ланки системи, у тому числі і на міжнародному рівні, що не обмежуються лише суто економічними втратами.

Одним із елементів критичної інфраструктури виступає транспортний комплекс та, зокрема, одна з його складових – авіаційний транспорт. Авіація є потужною галуззю національної економіки, яка має без сумніву стратегічне значення для економічної та національної безпеки. Критична інфраструктура в авіаційній галузі є невід'ємною складовою критичної інфраструктури держави.

Дослідження окремих аспектів проблематики захисту об'єктів критичної інфраструктури здійснювала низка вітчизняних та іноземних вчених, зокрема С.І.Азаров, В.Л.Сидоренко, Дж.Фулмер, П.С.Демпсі, С.А.Єременко, А.В.Пруський, А.М.Демків, С.О.Гнатюк, Н.А.Сейлова, В.М.Сидоренко, М.Б.Домарацький, Д.Г.Бобро, О.М.Суходоля, Я.О.Стахніцький, В.Ю.Зубок, А.В.Давидюк, Т.М.Клименко, Д.С.Бірюков, С.І.Кондратов та інші.

Разом із цим, комплексно питання захисту об'єктів критичної інфраструктури авіаційної галузі України, зокрема базових підходів держави у цій сфері, до цього часу залишаються недостатньо дослідженими.

Метою статті є аналіз засад державної політики захисту об'єктів критичної інфраструктури в авіаційній галузі України, напрацювання перспективних напрямів подальшого наукового дослідження.

Результати

Критичні об'єкти – це об'єкти, порушення чи припинення функціонування яких веде до втрати управління економікою на національному чи регіональному рівнях, значного зниження безпеки життєдіяльності населення. Відповідно до цих критеріїв здійснюється категоризація об'єктів, що у подальшому визначає кількісні та якісні вимоги до їх захисту. Категорія визначається відповідно до оцінки потенційних загроз для об'єкта, ймовірності та масштабів втрат [1].

Втрати, із значним ступенем умовності, можуть розподілятися на політичні, гуманітарні, фінансово-економічні, культурні, екологічні тощо. За масштабом вони можуть бути локального, регіонального, національного та міжнародного рівня [2]. В рамках кожного процесу визначається можливість настання в разі його порушення негативних наслідків соціального, політичного, економічного, екологічного характеру, а також наслідків для оборони та безпеки держави, забезпечення правопорядку. Процеси, порушення яких може призвести до такого роду наслідків, визначаються як критичні. Для кожного критичного процесу визначаються об'єкти інфраструктури, що ним використовуються, які і будуть віднесені до об'єктів критичної інфраструктури. Для кожного такого об'єкта визначаються негативні наслідки у разі втручання у його функціонування. Таким чином, об'єкт відноситься до певної категорії, чим держава здійснює вплив на суспільні відносини, пов'язані із використанням об'єктів, критично важливих для функціонування суспільства, економіки та держави. З цією метою державою формується нормативно-правовий механізм державного регулювання у сфері охорони критичної інфраструктури [3, 4].

Очевидно, що функцією об'єктів критичної інфраструктури, призначених для забезпечення транспортних цілей, є саме забезпечення транспортних перевезень. Тобто значення аеропортів як об'єктів критичної інфраструктури полягає саме у забезпеченні

функціонування системи цивільної авіації. Поза виконанням цієї функції ці об'єкти втрачають своє значення і не можуть розглядатися як такі, що мають самостійну цінність для держави, економіки та суспільства. Водночас із цим, загрози для цих об'єктів суттєво виходять поза межі лише забезпечення функціонування цивільної авіації. Так, будучи місцем скупчення великої маси людей, вони можуть розглядатися як «м'які цілі» для терористичних організацій, при цьому саме порушення діяльності цивільної авіації у цілі цих організацій може і не входити. Атаки держави-агресора на українські аеропорти були спрямовані, у т.ч., і для позбавлення України можливості використовувати їх з метою забезпечення функцій оборони. Інші загрози були пов'язані із намірами агресора використовувати такі аеропорти для висадки власних збройних сил для подальшого просування вглиб території нашої країни. Таким чином, система загроз для аеропортів як для об'єктів критичної інфраструктури суттєво виходить поза межі власне забезпечення лише авіаційної безпеки, функціонування цивільної авіації.

Як потенційні цілі атак, такі об'єкти критичної інфраструктури авіаційної галузі, як аеропорти, мають низку особливостей, серед яких відсутність розподілу на робочий та неробочий час, майже постійна наявність значного скупчення людей. можливість змови терористів чи інших осіб, що планують атаку, із персоналом аеропорту, що полегшуватиме вчинення атаки, можливість проведення атаки відносно невеликою кількістю виконавців, що можуть завдати значної шкоди, можливість досить ретельної підготовки атаки, оскілки частина споруд аеропорту знаходиться у вільному доступі, а щодо іншої частини інформація є відносно доступною, необмеженість атакуючих у часі для підготовки атаки, настання досить серйозних наслідків для суспільства навіть у результаті відносно обмеженої за масштабами атаки, можливість спрямовувати атаки на різі об'єкти – людей, техніку, психологічній стан суспільства у цілому, тощо.

Слід також враховувати такі чинники, як взаємодію аеропортів із суб'єктами підприємництва різних форм власності, потреба у забезпеченні різних рівнів безпеки для різних ділянок аеропорту, наявність в аеропорту власної служби безпеки, що вимагає погодження взаємодії між нею та компетентними органами держави, залежність функціонування аеропортів від інших об'єктів критичної інфраструктури, що забезпечують постачання електроенергії, води, теплопостачання, інших ресурсів. Надзвичайні ситуації в аеропорту, навіть відносно невисокого рівня, отримуватиме значну увагу суспільства та ЗМІ. Це, у свою чергу, може спровокувати паніку та інші надзвичайні ситуації, Таким чином наявність комунікації із суспільством, доведення правдивої інформації способом, що має довіру, може мати критичного значення. Належне функціонування загальних систем реагування на надзвичайні ситуації (ситуаційно-кризові центри, системи громадського попередження тощо) відіграє позитивну роль у забезпеченні безпеки на критично важливих об'єктах [5, 6].

Певні види атак в аеропорту, наприклад, терористичні акти, можуть здійснити навіть особи без високого рівня підготовки, або терористи-одинаки. Також можливим є використання ними досить широкого кола технічних засобів – автівок та вантажівок, зброї різного виду – від вогнепальної до переносних зенітних чи протитанкових систем, дронів, засобів кібернападу тощо.

Враховуючи глибоке залучення спецслужб РФ у діяльність терористичних угрупувань в різних регіонах світу, можна передбачити, наприклад, організацію ними теракту в країнах Європи чи в США із використанням переносних зенітних комплексів, що використовуються Збройними Силами України, у т.ч. і тих, що постачаються партнерами країн Заходу, для здійснення терористичних атак проти суден цивільної авіації поблизу аеропортів. Метою таких атак може бути дискредитація України на міжнародній арені як країни, що начебто постачає зброю терористам, припинення допомоги з боку країн Заходу, а також вплив на психологічний стан суспільства західних країн.

Слід також враховувати взаємні залежності різних об'єктів критичної інфраструктури. Так, ефективне функціонування об'єктів цивільної авіації залежить від так само ефективного функціонування низки інших секторів. Такого роду залежності є природними і дозволяють більш ефективно використовувати ресурси. З іншого боку, порушення в одному із секторів веде до каскадних порушень в інших. Сутність залежності полягає у тому, що для створення продукту чи послуги в одному із секторів необхідно вироблення продукту чи послуги у іншому. Від таких секторів, як виробництво та розподіл електроенергії, телекомунікації, постачання продуктів харчування залежить функціонування широкого кола секторів, у т.ч. і цивільна авіація [7, 8]. Залежності можуть бути, зокрема, фізичні, що полягають у поставках фізичних продуктів, інформаційними (кібер), сутність яких у тому, що функціонування певних об'єктів критичної інфраструктури залежить від інформації, що може передаватися через інформаційну інфраструктуру. На сьогодні інформаційна залежність набула універсального характеру, оскільки розповсюджується на всі сектори критичної інфраструктури без виключення. Ця залежність має виражений міжгалузевий та транснаціональний характер. Це обумовлює і універсальну вразливість від кібератак усіх таких секторів. Особливу небезпеку становитиме поєднана, комбінована кібератака на об'єкти критичної інфраструктури, що здійснюватиметься разом із атакою фізичною. Кібертероризм є чинником, що посилює вплив терористичної атаки, яка проводитиметься із використанням більш «традиційних» засобів, наприклад, бомбова атака, поєднана із кібератакою, що порушила функціонування телефонного зв'язку. Руйнація аварійного реагування в результаті такої кібератаки значно збільшить кількість жертв серед мирного населення.

Метою кібертероризму проти об'єктів критичної інфраструктури виступають автоматизовані системи управління ними, діяльність яких пов'язана із об'єктами критичної інформаційної інфраструктури взагалі [9, 10, 11]. Зазначене обумовлено низкою чинників, у тому числі універсальним впровадженням та використанням інформаційних технологій у будь-які системи управління, глобальним характером сучасного інформаційно-телекомунікаційного простору, що веде до розмиття кордонів національних складових, суттєвим збільшенням ваги розподільних автоматизованих систем управління об'єктами критичної інфраструктури та зростанням інформаційних потоків у цілому.

Підходи до формування державної політики у сфері забезпечення безпеки телекомунікацій та автоматизованих систем управління визначаються під впливом низки чинників, зокрема:

- збільшенням масштабів комплексів систем автоматизованого управління, що веде до їх ускладнення;
- постійним ускладненням програмного та апаратного забезпечення, що використовуються в автоматизованих системах;
- залученням до створення та обслуговування автоматизованих систем транснаціональних корпорацій та інших іноземних суб'єктів підприємництва, а також використанням майже виключно обладнання та програмного забезпечення, виробленого в інших країнах;
- використанням розробниками програмного забезпечення універсальних бібліотек та інших фрагментів програм, що веде до стандартизації програмних продуктів, які використовуються на різних об'єктах критичної інфраструктури і навіть у різних її секторах;
- постійним удосконаленням шкідливого програмного забезпечення та професійного рівня злочинців, їх інтеграцією до спецслужб країни-агресора, спрямуванням їх діяльності політичними інтересами кримінальної еліти Російської Федерації;

- інтеграція кримінальних структур, причетних до кіберзлочинності, до терористичних угрупувань, суттєва частка яких знаходяться під контролем або тим чи іншим чином пов'язана із спецслужбами рф;

- небажанням операторів об'єктів критичної інфраструктури розкривати факти порушень штатного функціонування автоматизованих систем, обумовлена комерційними міркуваннями;

- недостатнім рівнем професійної підготовки та освіти персоналу, на який покладено обслуговування автоматизованих систем управління об'єктами критичної інфраструктури, жорсткою конкуренцією на ринку праці серед спеціалістів ІТ-індустрії, що веде до їх перетягування до приватного сектору;

- потребою в удосконаленні нормативно-правового регулювання забезпечення безпеки автоматизованих систем об'єктів критичної інфраструктури, що має універсальний характер і є притаманною для більшості країн світу і міжнародних об'єднань і обумовленою об'єктивними процесами технологічного розвитку;

- все більш широким використанням хмарних носіїв інформації, що веде до ситуації, коли фізичне розташування даних невідомо їх власнику та користувачу.

Можна виділити наступні базові принципи побудови державної політики у сфер забезпечення безпеки автоматизованих систем управління об'єктами критичної інфраструктури:

- чітке законодавче обумовлення державної політики, що включає і виконання міжнародних договорів України, зокрема, відповідних директив ЄС;

- взаємна інтеграція інтересів та відповідальності держави, суспільства та приватного сектору, дотичних до розробки та функціонування такого роду систем;

- персональна відповідальність посадових осіб, операторів та іншого персоналу об'єктів критичної інфраструктури, до функціональних обов'язків яких віднесено розробку та експлуатацію автоматизованих систем управління;

- комплексний підхід до захисту інформаційної інфраструктури держави, що передбачає формування загальнодержавної системи раннього виявлення та попередження кібератак на об'єкти критичної інфраструктури, оцінку реального рівня захисту її складових;

- дозвільний характер діяльності у сфері забезпечення безпеки автоматизованих систем управління об'єктами критичної інфраструктури, що включає застосування механізмів ліцензування та сертифікації;

- функціональний розподіл між різними органами державної влади, уповноваженими на забезпечення кібербезпеки об'єктів критичної інфраструктури, інших аспектів безпеки таких об'єктів, забезпечення ефективної координації їх діяльності;

- визначення на законодавчому рівні прав та обов'язків власників автоматизованих систем управління об'єктами критичної інфраструктури та іншими об'єктами критичної інформаційної інфраструктури;

- мінімізація та зведення до раціонально обумовленого рівня технологічної залежності від інших держав при недопущенні залежності від держав, що використовують власні технологічні розробки для ведення шпигунської діяльності та інших неправомірних дій (РФ, Китай). Реалізацію цього напряму доцільно узгоджувати із партнерами України з країн ЄС та НАТО.

Одну із ключових ролей у захисті секторів та об'єктів критичної інфраструктури відіграє партнерство між державним та приватним секторами. Переважна частина об'єктів критичної інфраструктури перебуває у приватній власності. Ті об'єкти, що знаходяться у державній чи комунальній власності, до яких, зокрема, відносяться і аеропорти, у своїй діяльності залежать від об'єктів приватної власності, що також відносяться до критичної інфраструктури. Окрім цього, основними партнерами

аеропортів є компанії-авіаперевізники, що, як правило, належать до приватного сектору. Належна взаємодія між ними має критичне значення для обох сторін.

«Меридіанський процес», відкритий форум для обміну ідеями щодо захисту критично важливих об'єктів інфраструктури та співробітництва між високопоставленими урядовими політиками, визначив такі чинники, що лежать в основі ефективного державно-приватного партнерства: довіра, цінність, повага, кодекс поведінки, поінформованість про можливості та обмеження, реалістичні очікування.

Державно-приватні партнерства не мають фокусуватися на одному конкретному етапі циклу захисту критично важливих об'єктів інфраструктури. Однак вони мають охоплювати усі етапи, від розробки та реалізації заходів до етапів управління ризиками та кризами. Переваги об'єднання ресурсів, взаємної підтримки та спільного ухвалення рішень між державним сектором і приватними операторами КВОІ поширюються на такі сфери, як оцінка безпеки; огляд заходів безпеки; визначення критично важливих активів і процесів; розроблення планів дій у надзвичайних ситуаціях; навчання реагування на інциденти тощо.

Найбільш відповідна форма цього партнерства залежить від багатьох чинників, таких як цілі, кількість зацікавлених сторін, які будуть залучені, і від того, чи очікується, що партнерство вирішить стратегічні або операційні питання. Державно-приватні партнерства можуть приймати різні форми, від дуже неформальних форм співробітництва до більш формальних умов. Ступінь формальності нерідко пов'язано з рівнем контролю, який державні органи прагнуть здійснювати. З іншого боку, встановлено, що проєктно-орієнтовані державно-приватні партнерства зазвичай більш ефективні, ніж процесно-орієнтовані. Це пов'язано з тим, що проєктно-орієнтоване партнерство зазвичай включає чітко певні місії, терміни та бюджети [12].

Також було визначено фактори, що обумовлюють ефективність державно-приватного партнерства:

- довіра: оскільки державно-приватне партнерство часто стосується проблемних суб'єктів (комерційних питань, репутації, безпеки, перерозподілу обов'язків), важливо створити атмосферу довіри, в якій всі організації будуть усвідомлювати потребу одне одного в обачності і послідовно діяти відповідно. Чіткі керівні принципи членства в оперативних правилах можуть сприяти зміцненню довіри;

- цінність: участь у державно-приватному партнерстві повинна приносити користь, інакше інтерес до участі швидко згасне;

- повага: всі організації повинні визнавати і поважати додану вартість, яку інші організації вносять до співпраці.

- кодекс поведінки: необхідно мати чіткі, конкретні та передбачувані правила, які не надають можливості для роз'єднання і запобігають будь-якому конфлікту інтересів;

- обізнаність про можливості та обмеження один одного: це запобігає конфлікту через неправильне судження про причини негативної відповіді і дозволяє оптимально окупити зусилля альянсу. Це означає, що обидві організації повинні бути інформовані про діяльність одне одного. Надійний спосіб добитися цього – працювати разом довгий час, переважно роки;

- реалістичні очікування: всі організації повинні враховувати доступність ресурсів, бюджет розвитку тощо, щоб мати можливість формувати реалістичні очікування державно-приватного партнерства [13].

Переваги об'єднання ресурсів, взаємної підтримки та спільного прийняття рішень між державним сектором та приватними операторами об’єктів критичної інфраструктури поширюються на такі сфери, як оцінка безпеки; огляд заходів безпеки; визначення критично важливих активів і процесів; розробка планів дій у надзвичайних ситуаціях; навчання реагуванню на інциденти тощо.

Організація з безпеки та співробітництва в Європі (ОБСЄ) розробила базове 8-етапне керівництво про те, як країни мають максимізувати вигоди, які можна отримати від державно-приватного партнерства, використовуючи спільні інтереси всіх зацікавлених сторін. Незважаючи на те, що керівні принципи розроблено у рамках передової практики для критично важливої енергетичної інфраструктури, вони вважаються універсальними і загалом можуть застосовуватися у всіх секторах:

1) аналіз і визначення мотивації кожного партнера, який буде включено до партнерства захисту критичної інфраструктури, щоб уточнити взаємні очікування та внески;

2) визначення амбіцій і цілей партнерства із захисту об'єктів критичної інфраструктури на основі загальних національних цілей їх захисту;

3) перевірка існуючої нормативної бази, яка стосується кожного критично важливого сектору інфраструктури; визначення обов'язкових норм, правил і принципів; оцінювання адекватності існуючої нормативної бази з урахуванням очікуваних ризиків і рівнів готовності;

4) забезпечення механізмів захисту та правової визначеності для обміну інформацією, яку пов'язано із захистом об'єктів критичної інфраструктури, між усіма зацікавленими сторонами; забезпечення механізмів для добровільних зусиль, включаючи розробку та обмін передовим досвідом, консультації та діалог для постійного та ефективного партнерства;

5) формування інституційної структури, яка сприяє міжорганізаційному співробітництву та обміну інформацією; уточнення ролі та внеску кожного партнера (наприклад, урядових установ, власників та операторів критично важливої інфраструктури, постачальників продукції, асоціацій); встановлення керівних принципів співробітництва;

6) зосередження на одному чи двох критично важливих секторах інфраструктури;

7) визначення критично важливих етапів для розгляду, що було досягнуто та що треба надалі робити;

8) забезпечення постійного процесу перевірки для перегляду та оновлення партнерських відносин, щоб гарантувати прогрес, який співмірний із загальною картиною ризику та заходами безпеки, які необхідні для оптимального рівня захисту [14].

На виконання Державної програми авіаційної безпеки цивільної авіації відповідні документи розробляються кожним аеропортом. Розглянемо таку програму на прикладі Програми авіаційної безпеки Державного підприємства «Міжнародний аеропорт «Бориспіль», прийнятої у 2020 році. Програма містить організаційну структуру системи забезпечення її виконання із розподілом функцій суб'єктів. Також зазначаються технічні характеристики аеропорту, що визначають систему забезпечення його безпеки. Програма надає опис системи заходів безпеки аеропорту, що включає фізичні об'єкти захисту, систему контролю, заходи безпеки у неконтрольованій зоні, периметру аеропорту, його пропускної системи тощо. У програмі також зазначаються об'єкти – засоби аеронавігаційного обслуговування, що підлягають охороні, які знаходяться поза межами аеропорту.

Також Програма вказує на заходи реагування на акти незаконного втручання, що мають здійснюватися під керівництвом СБ України або МВС України відповідно до окремих планів, зокрема при загрозі вибуху, проведенні антитерористичної операції тощо.

Висновки

Загальними засадами державної політики захисту об'єктів критичної інфраструктури в авіаційній галузі є:

- необхідність забезпечення стійкості та здатності об'єктів критичної інфраструктури виконувати свої функції з огляду на наявність різноманітних загроз та взаємну залежність об'єктів критичної інфраструктури, зокрема в авіаційній галузі;
- необхідність забезпечення протидії загрозам воєнного характеру для функціонування об'єктів критичної інфраструктури авіаційної галузі України та необхідність відновлення функціональності таких об'єктів у повоєнний час;
- необхідність посилення спроможностей захисту інформаційної (IT чи кібер) складової діяльності об'єктів критичної інфраструктури авіаційної галузі;
- системний підхід до визначення критичності об'єктів авіаційної галузі (паспортизація), розробка та запровадження стандартизованих алгоритмів та протоколів діяльності таких об'єктів у визначених ситуаціях;
- запровадження передового досвіду провідних країн світу (ЄС, НАТО) у сфері захисту об'єктів критичної інфраструктури авіаційної галузі;
- ефективне державно-приватне партнерство;
- формування державного механізму (системи) захисту об'єктів критичної інфраструктури авіаційної галузі за участі різних суб'єктів з визначенням та розмежуванням їхніх повноважень.

З урахуванням викладеного, перспективним напрямом подальшого дослідження, на нашу думку, є дослідження проблематики взаємодії суб'єктів системи захисту об'єктів критичної інфраструктури в авіаційній галузі України.

Список використаних джерел

1. Домарацький М. Б. Методика державного категорування критично важливих об'єктів / М. Б. Домарацький // Держава та регіони. – 2019. – № 4(68). – С. 278 – 281. – (Серія «Державне управління»)., с. 278-280.
2. Домарацький М. Б. Особливості категоріювання об'єктів критичної інформаційної інфраструктури / М. Б. Домарацький // Фінансова система та економічна безпека: стан, проблеми, ефективність: збірник тез наукових робіт учасників міжнародної науково-практичної конференції для студентів, аспірантів та молодих учених. - К.: Аналітичний центр «Нова Економіка», 2019. – Ч. 2. – с. 91–92.
3. Бобро Д. Г. Удосконалення методології ранжування об'єктів критичної інфраструктури та їх віднесення до критичної інфраструктури : аналітична записка [Електронний ресурс] / Д. Г. Бобро. – Режим доступу : http://www.niss.gov.ua/content/articles/files/krutuchna_infra-a7636.pdf.
4. Коротич О.Б. Державне управління регіональним розвитком України : монограф. / О.Б. Коротич. – Х. : Вид-во ХарРІ НАДУ «Магістр», 2006. – 220 с.
5. Безпека людини у надзвичайних ситуаціях : навч. посіб. / За ред. В. І. Голінька. – Д. : Національний гірничий університет, 2011. – 161 с.
6. Малишева Н. Надзвичайна ситуація / Н. Малишева // Юридична наука, 2002. – С. 54–57.
7. Бірюков Д. С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні/ Аналітична доповідь / Д. С. Бірюков, С. І. Кондратов. – К. : ПП «Видавництво «ФЕНІКС», 2012. – 92 с.
8. Домарацький М. Б. Нормативне й адміністративне забезпечення державного регулювання критичної інфраструктури в Україні: аналіз і оцінка / М. Б. Домарацький // Вісник Національного університету цивільного захисту України. – 2020. – Вип. 1 (12). – С. 470–475.

9. Безопасность критических инфраструктур [Електронный ресурс]. – Режим доступу: http://www. slideshare.net/demidovov/1803201437129875.
10. Безпека як категорія і функція державного управління / Г. П. Ситнік // Вісн. Нац. академії держ. управління. – 2004. – № 1. – С. 350–357.
11. Бобро Д. Г. Удосконалення методології ранжування об'єктів критичної інфраструктури та їх віднесення до критичної інфраструктури : аналітична записка [Електронний ресурс] / Д. Г. Бобро. – Режим доступу : http://www.niss.gov.ua/content/articles/files/krutuchna_infra-a7636.pdf.
12. Трушкіна Н. В. Державно-приватне партнерство як механізм забезпечення захисту критичної інфраструктури: досвід ЄС. // Механізми протидії сучасним викликам і загрозам: досвід ЄС для України. Матеріали Міжнародної науково-практичної конференції (Суми, Сумський державний університет, 30-31 березня 2023 року). 108 с., с. 42 – 45.
13. Домарацький М.Б. Державне управління забезпеченням безпеки критичної інфраструктури в Україні. Дисерація на здобуття наукового ступеня кандидата наук з державного управління. Харків, 2020, 259 с., с. 159 – 160.
14. Public-Private Partnerships: Preventing Cyberattacks on Critical Infrastructure in the OSCE Region // Aaron Joshua Pinto, Alexandra Borgeaud dit Avocat, Elena Lulcheva, Philipp Dietrich. 2021. https://www.osce.org/files/f/documents/6/0/506930.pdf.