Правове регулювання захисту критичної інфраструктури в авіаційній галузі відповідно до законодавства Європейського Союзу

Андрій Кузнік[1]

Опубліковано	Секція	УДК
24.12.2023	Право	338.583+657.471

DOI: https://doi.org/10.5281/zenodo.15119692

Анотація. У статті здійснено ґрунтовний аналіз стану правового регулювання захисту критичної інфраструктури в авіаційній галузі відповідно до законодавства Європейського Союзу. Розкрито еволюцію нормативно-правових підходів ЄС до ідентифікації, захисту та підвищення стійкості об'єктів критичної інфраструктури, зокрема в межах енергетичного та транспортного секторів. Окрему увагу приділено імплементації загальноєвропейських стандартів авіаційної безпеки, забезпеченню координації між державами-членами, застосуванню єдиного підходу до оцінки ризиків і кризового реагування. Здійснено порівняльний аналіз положень Регламенту (ЄС) № 300/2008, Директив NIS2 та CER, в яких висвітлено тенденції до уніфікації норм, розширення сфери кібербезпеки, запровадження паспортів безпеки об'єктів та процедур внутрішнього контролю. Підкреслено зростаюче значення проактивної стратегії стійкості критичних об'єктів, з урахуванням викликів гібридного впливу, терористичних загроз та природних катастроф. Визначено інституційні основи міждержавної співпраці та державно-приватного партнерства у сфері захисту критичної інфраструктури, зокрема в контексті посилення взаємодії ЄС з НАТО. Аргументовано потребу адаптації національного законодавства України до відповідних норм ЄС, що є актуальним у межах євроінтеграційного курсу та загальноєвропейського безпекового простору. Запропоновано напрями подальших досліджень, зосереджених на імплементації стандартів ЄС в українське нормативне поле у сфері безпеки авіаційної критичної інфраструктури.

Ключові слова: критична інфраструктура, об'єкти критичної інфраструктури, захист об'єктів, безпека, авіаційна галузь, нормативно-правове регулювання, незаконне втручання, тероризм, інциденти, ризики, співробітництво, Європейський Союз.

Legal regulation of critical infrastructure protection in the aviation industry in accordance with European Union legislation

Abstract. The article provides a thorough analysis of the state of legal regulation of critical infrastructure protection in the aviation sector in accordance with the legislation of the

[1] аспірант НА СБ України

European Union. It explores the evolution of EU regulatory approaches to the identification, protection, and resilience of critical infrastructure objects, particularly within the energy and transport sectors. Special attention is devoted to the implementation of pan-European aviation security standards, the coordination between Member States, and the adoption of a unified approach to risk assessment and crisis response. A comparative analysis of the provisions of Regulation (EC) No. 300/2008, the NIS2 Directive, and the CER Directive is carried out, highlighting the trends toward harmonization of norms, expansion of cybersecurity scope, introduction of infrastructure safety passports, and internal control procedures. The article emphasizes the growing importance of a proactive strategy for the resilience of critical entities, considering hybrid threats, terrorism, and natural disasters. The institutional foundations of interstate cooperation and public-private partnerships in the sphere of critical infrastructure protection are defined, particularly in the context of strengthening EU–NATO cooperation. The need to adapt Ukraine's national legislation to the relevant EU standards is substantiated, which is of particular relevance in the framework of the country's European integration course and the formation of a common European security space. Prospects for further research are proposed, focusing on the implementation of EU standards in Ukraine's regulatory field regarding aviation critical infrastructure security.

Keywords: critical infrastructure, critical infrastructure objects, object protection, security, aviation sector, regulatory framework, unlawful interference, terrorism, incidents, risks, cooperation, European Union.

Вступ

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.Сєйлова, 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, зокрема стану регулювання захисту критичної інфраструктури в авіаційній галузі у законодавстві Європейського Союзу, до цього часу залишаються недостатньо дослідженими.

Метою статті є аналіз сучасного стану регулювання захисту критичної інфраструктури в авіаційній галузі у законодавстві ЄС, напрацювання перспективних напрямів подальшого наукового дослідження.

Результати

Захист критичної інфраструктури є одним із елементів безпекової політики ЄС: на початку цього століття почали формуватися підходи щодо розвитку механізмів захисту критичної інфраструктури не лише на рівні окремих країн-членів, а й Союзу у цілому, із

урахуванням моделей, напрацьованих у США, де захист критичної інфраструктури від терористичних загроз визначався як одне з основних завдань системи захисту національної безпеки.

Критична інфраструктура відіграє незамінну роль у підтримці соціальних функцій та економічної діяльності внутрішнього ринку ЄС, що має тенденцію до підвищення взаємозалежності. Це обумовлює потребу у формуванні регуляційних механізмів ЄС, націлених на забезпечення стійкості критичної інфраструктури на внутрішньому ринку та мінімальних правил, що мають забезпечувати впровадження таких механізмів шляхом надання узгодженої та сфокусованої підтримки та нагляду.

В ЄС формування організаційно-парових механізмів захисту критичної інфраструктури ініційовано у зверненні Європейської Ради до Європейської Комісії у 2004 році, де останній доручалося підготувати стратегію захисту цієї інфраструктури. В тому ж році Єврокомісія видала офіційне повідомлення [1] щодо стану захисту критичної інфраструктури в ЄС, а також пропозиції із удосконалення цієї системи, націлені, передусім, на запобігання терористичним атакам. Дотримуючись принципу субсидіарності, загальноєвропейським інституціям потрібно сконцентрувати зусилля на захисті тих об’єктів, порушення функціонування яких буде мати транскордонний вплив, залишивши за країнами ЄС відповідальність за решту об’єктів. Підхід до захисту критичної інфраструктури у всіх країнах ЄС повинен бути методологічно близьким. В повідомленні №786 за 2006р. [2] Єврокомісія рекомендувала всім країнам ЄС вжити таких заходів: розробити національну програму захисту критичної інфраструктури; забезпечувати рівень охорони здоров’я, технологічної безпеки, соціально-економічного благополуччя, який би гарантував «стійкість» нації до загроз; уніфікувати зусилля, спрямовані на захист критичної інфраструктури, надавши єдиному державному органу, що звітує з цього питання, функції координації дій державних органів влади, що відповідають за окремі галузі промисловості, до яких належать об’єкти критичної інфраструктури; визначити органи державної влади, відповідальні за сектори критичної інфраструктури, та відповідні приватні компанії; створити умови для ефективної взаємодії та обміну інформацією, даними і досвідом між країнами-членами ЄС, урядовими структурами та приватним сектором; створити гармонізовану методологію аналізу ризиків.

Європейська Директива щодо критичної інфраструктури (ECI) [3] 2008 року є основною складовою європейської політики захисту критичної інфраструктури і визначає встановлює процедуру ідентифікації та позначення об'єктів критичної інфраструктури та загальний підхід до оцінки необхідності покращення їх захисту.

Директива стосується лише енергетичного та транспортного секторів. Серед іншого, Директива вимагає від власників та операторів призначених об'єктів підготувати плани безпеки оператора та призначити офіцерів зв’язку, таким чином зв’язавши власника та оператора з національним органом, відповідальним за захист критичної інфраструктури

Директива Ради ЄС 2008/114/ЕС надала процедуру визначення критичної інфраструктури ЄС в енергетичному та транспортному секторах, пошкодження чи руйнація якої може мати значний транскордонний вплив на якнайменш дві держави-члена. Оцінка цієї Директиви, проведена у 2019 році виявила, що, через посилення взаємозалежності та транскордонну природу операцій, які використовують критичну інфраструктуру, превентивні заходи, які стосуються лише самих фізичних об'єктів, є недостатніми для запобігання руйнівному впливу. Необхідним є зміщення підходів на кращу оцінку ризиків, визначення ролі та обов'язків критичних об'єктів, що надають послуги, ключові для функціонування внутрішнього ринку, а правила ЄС необхідно адаптувати для забезпечення стійкості інфраструктури. Ландшафт загроз визначається

як динамічний і такий, що включає в себе гібридні та терористичні загрози, а також зростаючу взаємозалежність між інфраструктурою та секторами економіки.

Чинником, що сприяв прийняттю Декларації, стало подальше зростання взаємозалежності між країнами ЄС у різних сферах, унаслідок чого відбувається формування загальної критичної інфраструктури Європейського Союзу, що виходить поза межі національних кордонів. Ці взаємозалежності означають, що будь-яке порушення функціонування системи надання послуг, навіть те, яке спочатку обмежується однією організацією або одним сектором, може мати каскадні наслідки в більш широкому плані, потенційно призводячи до далекосяжного та довгострокового негативного впливу на надання критично-важливих послуг у всьому світі. Таким чином, визнається потреба у встановленні узгоджених мінімальних правил для забезпечення надання основних послуг на внутрішньому ринку, підвищення стійкості критичних суб'єктів і покращення транскордонної співпраці між компетентними органами. Визначення самих об'єктів критичної інфраструктури залишається у компетенції держав-членів.

У 2008 році було прийнято Регламент Європейського Парламенту і Ради ЄС, яким встановлюються спільні правила у сфері безпеки цивільної авіації [4].

Зазначається потреба у забезпеченні авіаційної безпеки на загальноєвропейському рівні, зокрема, шляхом створення спільних правил захисту цивільної авіації, спільних основних стандартів авіаційної безпеки, а також механізму моніторингу їх дотримання.

Регламент застосовується до усіх аеропортів або частин аеропортів на території держави-члена, що не використовуються виключно для військових цілей, усіх експлуатантів, що надають послуги в аеропортах, усіх суб'єктів авіаційної діяльності, що застосовують стандарти авіаційної безпеки та працюють у службових приміщеннях всередині або за межами службових приміщень аеропорту, а також надають товари та/або послуги для або через аеропорти.

Кожна держава-член має призначити єдиний орган, що відповідатиме за координацію та моніторинг імплементації стандартів безпеки, розробити національну програму авіаційної безпеки цивільної авіації. Крім того, кожен експлуатант аеропорту, авіаперевізник та суб'єкт авіаційної діяльності, що бере участь у реалізації стандартів авіаційної безпеки, повинен скласти, застосовувати та регулярно оновлювати програми безпеки для забезпечення відповідності Регламенту та національній програмі авіаційної безпеки цивільної авіації. Моніторинг дотримання Регламенту здійснюється Єврокомісією шляхом інспектування, у тому числі і негласного.

Для усіх рейсів на території Європейського Союзу запроваджується «єдиний пункт контролю безпеки».

З метою уніфікації підходів, Єврокомісія має укладати угоди між ЄС та третіми країнами якими визнається, що стандарти безпеки, запроваджені на території третьої країни, є еквівалентними спільним стандартам, оскільки такі угоди сприяють поширенню практики запровадження єдиного пункту контролю безпеки.

Регламент зобов'язує держави-члени забезпечити розробку програм безпеки в аеропорту, що мають складатися його експлуатантом (ст. 12). Така програма повинна визначати методи і процедури, яких повинен дотримуватися експлуатант аеропорту для забезпечення відповідності Регламенту та національній програмі авіаційної безпеки цивільної авіації держави-члена, на території якої розташований аеропорт. Також вона має містити положення про внутрішній контроль якості та описувати процес моніторингу дотримання таких методів і процедур експлуатантом аеропорту.

У додатках до Регламенту надаються спільні основні стандарти захисту цивільної авіації від актів незаконного втручання, що містять положення щодо безпеки в аеропорту. Визначається наявність в аеропортах таких зон: неконтрольована зона;

контрольована зона; зони обмеженого доступу, що охороняються; та критичні ділянки зон обмеженого доступу, що охороняються.

Заходи безпеки забезпечуються, зокрема, шляхом набору та підготовки персоналу, використання спеціального обладнання для забезпечення безпеки.

Усі аеропорти, експлуатанти та інші суб'єкти авіаційної діяльності, що виконують обов'язки із забезпечення авіаційної безпеки, необхідно регулярно перевіряти, щоб забезпечити швидке виявлення та виправлення виявлених недоліків. Заходи моніторингу дотримання встановлених вимог повинні включати аудити безпеки, інспектування та випробування. Також має здійснюватися аудит безпеки, що охоплює всі заходи безпеки в аеропорту або окрему частину національної програми авіаційної безпеки цивільної авіації. Аеропорти з річним обсягом повітряних перевезень понад 10 мільйонів пасажирів повинні проходити аудит безпеки щодо всіх стандартів авіаційної безпеки щонайменше один раз на чотири роки.

Також мають здійснюватися негласні інспектування, що охоплюють принаймні один комплекс безпосередньо пов'язаних заходів безпеки.

Для верифікації заходів безпеки проводяться випробування, що стосуються контролю доступу до зони обмеженого доступу, що охороняється; захисту повітряного судна; догляду пасажирів та ручної поклажі; догляду персоналу та предметів, які вони проносять; захисту зареєстрованого багажу; догляду вантажу або пошти; захисту вантажів та пошти.

Директива (ЄС) 2022/2555 [5], відома як NIS2, стосується захисту критичної інфраструктури від кіберзагроз та замінила Директиву (ЄС) 2016/1148, відому як просто NIS. Однією з головних відмінностей Директиви NIS2 у порівнянні з попередньою, є розширення сфери її дії на нові сектори економіки та типи підприємств. Директива спрямована на покращення існуючого стану кібербезпеки в Європейському Союзі завдяки таким факторам, як: створення міждержавної структури управління кіберкризою (EU-CyCLONe); підвищення рівня гармонізації щодо вимог безпеки та зобов'язань щодо звітності; заохочення держав-членів до впровадження нових сфер інтересів, таких як безпека ланцюгів постачання, управління вразливістю, Інтернет і кібергігієна, до їхніх національних стратегій кібербезпеки; залучення нових ідей, таких як експертні оцінки для удосконалення співпраці та обміну знаннями між державами-членами; охоплення більшої частки економіки та суспільства шляхом включення більшої кількості секторів, що означає, що більше суб'єктів зобов'язані вживати заходів для підвищення рівня кібербезпеки.

Прийняття Директиви обумовлено посиленням залежності критичної інфраструктури та суспільства у цілому від розвитку інформаційних технологій, активним використанням цієї сфери кримінальними структурами та терористичними угрупуваннями. Держава-агресор рф також активно використовує кібератаки не лише проти України, а й проти країн ЄС.

NIS2 застосовується як до компаній, визначених як ключові («essential»), так і до тих, що визначені як важливі («important»). Уряди держав-членів можуть визначити невеликі компанії з високим ризиком безпеки, які також повинні почати відповідати вимогам. Різниця між операторами критичних чи важливих послуг і постачальниками цифрових послуг усувається.

NIS2 містить перелік заходів, які повинні вжити всі важливі та важливі суб'єкти, щоб керувати ризиками кібербезпеки під час надання своїх послуг. До них належать, наприклад, політики щодо аналізу ризиків та безпеки інформаційних систем; врегулювання інцидентів; управління резервним копіюванням та антикризовий менеджмент; практики кібергігієни; політики та процедури щодо використання криптографії та шифрування; і використання багатофакторної аутентифікації.

Про будь-який суттєвий інцидент необхідно повідомити групі реагування на інциденти комп'ютерної безпеки країни-члена (CSIRT) або відповідному наглядовому органу. Організації також мають повідомляти одержувачів їхніх послуг про значні інциденти, які можуть негативно вплинути на надання цих послуг.

Директива посилює вимоги щодо здійснення нагляду та забезпечення належних повноважень правоохоронних органів. Наглядові органи повинні мати повноваження проводити інспекції на місцях і цільові аудити безпеки, а також запитувати інформацію, отримувати доступ до даних або вимагати докази виконання політики кібербезпеки.

Слід зазначити, що низка дослідників визначає, що положення цієї Директиви суттєво відрізняються від вимог законодавства України, що обумовлює потребу суттєвого доопрацювання останнього [6].

У Директиві ЄС щодо стійкості критично важливих об'єктів (Директива CER) [7] визнається збільшення деструктивних чинників сучасного полікризового світу, що обумовлює потребу у посиленні стійкості критично важливих об'єктів проти широкого спектру загроз і небезпек, включаючи стихійні лиха, терористичні та кібератаки та диверсії. ЄС пропонує у ньому підхід, що ґрунтується на оцінці ризику, для визначення критично важливих суб'єктів: організацій, які мають найбільше значення для життєво важливих економічних або соціальних функцій. Відзначається, що підходи до захисту критичної інфраструктури часто залишаються реактивними, тобто націленими на усунення негативних наслідків, а не проактивними, націленими на запобігання та формування стійкості шляхом розробки та застосування заходів превенції. Забезпечення стійкості критичної інфраструктури є безперервними процесом, що вимагає ресурсів, співпраці, адаптивності та постійного удосконалення.

Стійкість дозволяє організаціям протистояти ризикам або поглинати їх чи належними чином на них реагувати, аби мінімізувати їх вплив та залишатися у межах заздалегідь визначених допусків. Кожен критично важливий компонент, система, послуга, процес або діяльність повинні бути стійкими, відновлюваними або мати плани безперервності [8].

У тому разі, якщо негативний вплив перевищує прийнятний рівень впливу для організації, має місце криза. Під час кризи плани стійкості можуть бути перевантажені, а допустимі рівні впливу можуть бути порушені. Можливості управління кризою повинні забезпечувати гнучкий і динамічний підхід, щоб дозволити організації керувати непередбаченими збоями, продовжувати досягати своїх стратегічних цілей і повертатися до життєздатного робочого стану в цих умовах надзвичайної невизначеності.

Таким чином, стійкість характеризує здатність організації адаптуватися та досягати цілей своєї діяльності за умов постійного негативного впливу. За умов перманентної кризи стійкість є стратегічним імперативом організації. Слід також зазначити, що стійкість є передумовою забезпечення довіри між організацією та споживачами її послуг, що є критичним для функціонування як цієї організації, так і суспільства у цілому [9].

У той час, коли Директива NIS 2 стосувалася передусім кіберзагроз, Директива CER визнає, що типи загроз і небезпек, з якими ми стикаємося, є більш різноманітними, частими та складними, ніж будь-коли раніше. Це створює зобов'язання для бізнесу, промисловості та суспільства розвивати здатність реагувати та адаптуватися в умовах збоїв. Директива CER характеризується широтою охоплення секторів економіки та розмірів організацій (одинадцять секторів, у тому числі і транспортний).

Цей нормативний акт є демонстрацією стратегічного підходу, пропонуючи організаціям формувати стратегії із забезпечення стійкості. Такий підхід дозволить організаціям не лише захистити себе, а й підвищити власну ефективність, у т.ч. за

несприятливих обставин. Це, окрім іншого, має сприяти підвищенню конкурентоздатності європейської економіки.

На рівні ЄС захист критичної інфраструктури та стійкість критично важливих суб'єктів, які керують цією інфраструктурою, визнаються життєво важливими для сучасного суспільства. З цієї причини Європейська комісія постійно забезпечує підтримку захисту критичної інфраструктури та стійкості критично важливих об'єктів проти природних і антропогенних ризиків.

На виконання цієї Директиви держави-члени зобов'язуються прийняти національну стратегію до січня 2026 року та проводити регулярні оцінки ризиків для виявлення суб'єктів, які вважаються критично важливими або життєво важливими для суспільства та економіки. Єврокомісія ухвалила перелік основних послуг у всіх секторах, на які поширюється дія Директиви. Оцінка ризиків буде проведена щодо цих основних послуг, щоб можна було ідентифікувати критичні суб'єкти в кожній державі-члені.

У свою чергу, критично важливі об'єкти повинні будуть провести власну оцінку ризиків і вжити технічних, безпекових і організаційних заходів для підвищення своєї стійкості та сповіщення про інциденти.

Держави-члени повинні будуть надавати підтримку критично важливим суб'єктам для підвищення їх стійкості. Комісія надаватиме додаткову підтримку державам-членам і критично важливим суб'єктам, розробляючи на рівні Союзу огляд транскордонних і міжгалузевих ризиків, найкращі практики, керівні матеріали, методології, транскордонні навчальні заходи та навчання для перевірки стійкості критичні об'єкти, серед інших.

Цим документом започатковано діяльність Групи стійкості критичних об'єктів (CERG), яка покликана сприяти співпраці між державами-членами та Єврокомісією (зокрема, обмін інформацією та передовою практикою з питань, що стосуються стійкості критичної інфраструктури та об'єктів).

З огляду на те, що сфера національної безпеки відноситься до виключної компетенції держав-членів, виключення із сфери регулювання цієї Директиви застосовується щодо суб'єктів, чия діяльність здійснюється у сфері національної безпеки та оборони, громадської безпеки та правоохоронної діяльності.

Задля забезпечення комплексного підходу до стійкості критично важливих суб'єктів, кожна держава-член повинна мати національну стратегію підвищення стійкості критично важливих суб'єктів. Така стратегія повинна визначати стратегічні цілі та політичні заходи, які мають бути реалізовані і виступати політичною основою для удосконалення координації між компетентними органами держав-членів ЄС. Розробляючи свої стратегії, держави-члени повинні належним чином враховувати гібридний характер загроз критично важливим об'єктам та проінформувати Європейську Комісію щодо національних стратегій.

Дії на національному рівні мають ґрунтуватися на оцінці ризиків - природних і антропогенних, у тому числі тих, що мають міжгалузевий або транскордонний характер, які можуть вплинути на надання основних послуг, включаючи аварії, стихійні лиха, надзвичайні ситуації у сфері охорони здоров'я, а також гібридні загрози, терористичні акти, вплив організованої злочинності та диверсії. Послуги, економіка, вільне пересування та безпека громадян ЄС залежать від належного функціонування критичної інфраструктури, що робить забезпечення її безпеки наднаціональним завданням.

Відповідно до вимог Директиви, держави-члени повинні призначити або заснувати органи, компетентні контролювати застосування та забезпечити дотримання правил Директиви та забезпечити, щоб ці органи мали належні повноваження і ресурси. Держави-члени повинні чітко визначити завдання відповідних органів і забезпечити безперебійну та ефективну співпрацю між ними. Усі відповідні компетентні органи також повинні більш широко співпрацювати як на рівні Союзу, так і на національному

рівні. З метою забезпечення співробітництва на рівні ЄС, кожна держава-член повинна призначити одну контактну точку, відповідальну за координацію питань, пов'язаних з стійкість критично важливих суб'єктів і транскордонне співробітництво («єдина контактна точка»).

Держави-члени повинні підтримувати об'єкти критичної інфраструктури у зміцненні їхньої стійкості. Така підтримка, зокрема, має включати організацію навчань для перевірки їх стійкості, надання порад та навчання їх персоналу. Якщо це необхідно та виправдано цілями суспільного інтересу, держави-члени можуть надавати фінансові ресурси та повинні сприяти добровільному обміну інформацією та передовим досвідом між об'єктами критичної інфраструктури.

Уповноважені органи держав-членів мають здійснювати співробітництво, у т.ч. задля забезпечення узгодженого та послідовного застосування цієї Директиви. У першу чергу це співробітництво є доречним у тому випадку, коли мова йде про об'єкти критичної інфраструктури, що стосуються двох чи більше держав-членів ЄС, надають послуги іншим державам-членам тощо.

Від операторів об'єктів критичної інфраструктури очікується повне розуміння ризиків, яким вони піддаються та здійснення аналізу таких ризиків, їх оцінки. Оцінка ризиків має проводитися, якнайменш, кожні чотири роки.

Оператори мають вживати технічних, безпекових та організаційних заходів, відповідних та пропорційних ризикам, з якими вони стикаються, щоб запобігти інциденту, забезпечити захист від нього, відповідним чином відреагувати на його настання, протистояти його впливу, пом'якшити його наслідки, поглинути їх, забезпечуючи функціонування об'єкта, пристосувати цей об'єкт до нових умов та відновити його функціонування після інциденту.

Деталі та обсяг таких заходів повинні відображати ризики, які кожен оператор об'єкта критичної інфраструктури визначив у рамках оцінки ризиків цього об'єкта, а також його особливості. Єврокомісія має ухвалити керівні принципи для подальшого визначення цих технічних, безпекових та організаційних заходів, що матимуть рекомендаційний характер.

Оператори об'єктів критичної інфраструктури мають надати у плані із забезпечення стійкості опис заходів, що мають ними вживатися задля гарантування ефективності та підзвітності, беручи до уваги виявлені ризики.

У контексті забезпечення авіаційної безпеки ця Директива виступає розширенням Регламенту (ЄС) № 300/2008 (15) Європейського Парламенту та Ради у контексті запобігання інцидентам, викликаним незаконними діями та для мінімізації наслідків інцидентів, забезпечення стійкості відповідних об'єктів критичної інфраструктури.

Увага звертається також на перевірку працівників об'єктів критичної інфраструктури, оскільки випадки зловживань викликають все більше занепокоєння в ЄС. Держави-члени мають визначити умови, за яких оператори суб'єктів критичної інфраструктури можуть подавати запити на перевірку щодо осіб, які належать до певних категорій персоналу. Зазначена перевірка має здійснюватися на рівні ЄС, може включати перевірку судимості особи, використання Шенгенської інформаційної системи, оперативно-розшукові дані та іншу доступну інформацію, яка може бути необхідною для визначення придатності відповідної особи для роботи на посаді, щодо якої об'єкт критичної інфраструктури подав запит на перевірку даних.

Також необхідним є започаткування механізму повідомлення щодо певних інцидентів, який має дозволити компетентним органам швидко та адекватно реагувати на інциденти та мати повну інформацію щодо характеру, причин і можливих наслідків інцидентів. Об'єкти критичної інфраструктури мають повідомляти компетентні органи про інциденти, які суттєво порушують надання послуг, критичних для життєдіяльності суспільства та держави. Початкове повідомлення має бути надіслано не пізніше 24 годин

після отримання інформації про інцидент. Таке повідомлення має містити інформацію про причину інциденту і воно може виступати підставою для подальшого звернення по допомогу. У разі потреби, детальний звіт про інцидент може бути направлено не пізніше ніж через місяць після інциденту.

Виділяються об'єкти критичної інфраструктури, що мають особливе значення для ЄС (об'єкт критичної інфраструктури особливого європейського значення) та його внутрішнього ринку. Це такі об'єкти, що надають критично важливі послуги до шести чи більше держав-членів ЄС і можуть отримати додаткову підтримку на рівні Євросоюзу.

Держава-член ЄС, що визначила об'єкт критичної інфраструктури особливого європейського значення, повинна надати Єврокомісії повну інформацію щодо нього. Єврокомісія повинна мати змогу організувати консультативну місію для оцінки заходів, що вживаються на цьому об'єкті.

Держави-члени мають забезпечити наявність в уповноважених компетентних органів належних ресурсів та можливостей, зокрема, повноваження проводити інспектування та аудит, нагляд, витребування у операторів об'єктів критичної інфраструктури інформації та підтвердження того, що заходи, що вживаються ними, відповідають їх зобов'язанням, а також право вимагати усунути певні невідповідності. Це право має бути обмеженим та підконтрольним, відповідно до норм європейського законодавства.

Директива покладає зобов'язання на держави-члени розробити та прийняти стратегію підвищення стійкості об'єктів критичної інфраструктури, що має повинна встановлювати стратегічні цілі та політичні заходи, спираючись на відповідні існуючі національні та галузеві стратегії, плани чи подібні документи, з метою досягнення та підтримки високого рівня стійкості таких об'єктів та мінімально визначеного набору секторів. Стратегія має містити стратегічні цілі та пріоритети для цілей підвищення загальної стійкості об'єктів, беручи до уваги транскордонні та міжгалузеві залежності та взаємозалежності; структуру управління для досягнення стратегічних цілей і пріоритетів, включаючи опис ролей і відповідальності різних органів влади, об'єктів критичної інфраструктури та інших сторін, залучених до реалізації стратегії; опис заходів, необхідних для підвищення загальної стійкості таких об’єктів, включаючи опис оцінки ризику; опис процесу, за допомогою якого ідентифікуються об'єкти критичної інфраструктури; опис процесу підтримки таких об'єктів, включаючи заходи для посилення співпраці між державним та приватним сектором; перелік основних органів влади та відповідних зацікавлених сторін, залучених до реалізації стратегії; політичну основу для координації між компетентними органами; опис уже діючих заходів, спрямованих на сприяння виконанню зобов’язань об'єктами критичної інфраструктури.

Директива визначає перелік заходів із забезпечення стійкості об’єктів критичної інфраструктури. До них відноситься, зокрема: запобігання виникненню інцидентів, належним чином враховуючи заходи щодо зменшення ризику лиха; забезпечення належного фізичного захисту приміщень та інфраструктури, що включає, наприклад, огорожі, бар’єри, інструменти та процедури моніторингу периметра, обладнання виявлення та контроль доступу; реагувати на інциденти, протистояння їм і мінімізацію їх наслідків, включаючи впровадження процедур і протоколів управління ризиками та кризовими ситуаціями, а також процедур оповіщення; відновлення після інцидентів, включаючи заходи забезпечення безперервності бізнесу та визначення альтернативних ланцюгів постачання, що мають забезпечити відновлення надання основних послуг; забезпечення адекватного управління безпекою співробітників, що включає такі заходи, як визначення категорій персоналу, який виконує критично важливі функції, встановлення прав доступу до приміщень, інфраструктури та конфіденційної інформації, встановлення процедур для перевірки даних та визначення категорій осіб, від яких вимагається проходження таких перевірок, а також встановлення відповідних

вимог до підготовки та кваліфікації; підвищення обізнаності щодо зазначених вище заходів.

Кожен об'єкт критичної інфраструктури має призначити співробітника, відповідального за взаємодію із компетентними органами (офіцера зв'язку).

Рекомендація Ради щодо загальносоюзного скоординованого підходу до посилення стійкості критичної інфраструктури [10], ухвалена 08.12.2022, стала реакцією на заклики вжити додаткових заходів після диверсійних актів проти критичної інфраструктури ЄС. Рекомендація Ради пропонує дії для підвищення готовності та реагування на поточні загрози як шляхом прогнозування , так і шляхом використання інструментів, розроблених для забезпечення стійкості.

Рекомендація охоплює три пріоритетні сфери: готовність, реагування та міжнародне співробітництво .

Зокрема, для підвищення готовності державам-членам пропонується оновити свої оцінки ризиків, щоб відобразити поточні загрози, і провести стрес-тести на основі загальних принципів і спільних сценаріїв на рівні ЄС, починаючи з енергетичного сектору. Стрес-тест було завершено до кінця 2023 року і за його результатами розроблено подальші кроки із удосконалення співпраці з підвищення стійкості на рівні ЄС.

25 червня 2024 року Рада прийняла Рекомендацію щодо плану критичної інфраструктури [11], націлену на більш скоординоване реагування на значні транскордонні інциденти, що стосуються об'єктів критичної інфраструктури і можуть порушити основні послуги на внутрішньому ринку. План критичної інфраструктури містить дорожню карту із заходами, які можна застосувати, коли країни ЄС стикаються зі значними критичними інцидентами.

Іншим напрямом є посилення співпраці з НАТО, націленої на подолання ризиків та інцидентів значного транскордонного значення. Цільова група ЄС-НАТО з питань стійкості критичної інфраструктури була започаткована у 2023 році та опублікувала оціночний звіт із рекомендаціями у цій сфері. Крім того, посилюється співпраця з міжнародними партнерами. Пріоритетом є сусідство ЄС із Західними Балканами та Східною Європою, з особливим акцентом на підтримку України.

Висновки

Узагальнюючи викладене, зазначимо, що нормативно-правове регулювання захисту критичної інфраструктури в авіаційній галузі відповідно до законодавства Європейського Союзу характеризується системністю та спрямоване на уніфікацію підходів щодо визначення об’єктів критичної інфраструктури і їх значення для ЄС в цілому, запровадження стандартизованих процедур щодо оцінки ризиків, загроз, процедур реагування на інциденти, запровадження проактивних підходів у реалізації заходів, спрямованих на забезпечення стійкості об’єктів критичної інфраструктури. Окремо слід виділити посилення координації та співробітництва з країнами-членами ЄС та НАТО, зокрема ретельне дослідження іноземного досвіду та впровадження ефективних механізмів та моделей.

З урахуванням викладеного, перспективним напрямом подальшого дослідження, на нашу думку, є дослідження нормативно-правового забезпечення захисту об’єктів критичної інфраструктури в авіаційній галузі у національному законодавстві України.

Список використаних джерел

1. Communication from the Commission to the Council and the European Parliament of 20 October 2004 – Critical infrastructure protection in the fight against terrorism (COM/2004/702 final). http://eur-lex.europa.eu/.

2. Communication from the Commission on a European Programme for Critical Infrastructure Protection (COM/2006/786 final). http://eur-lex.europa.eu/.
3. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. 23.12.2008 Official Journal of the European Union. L 345/75 https://eur-lex.europa.eu/eli/dir/2008/114/oj.
4. Регламент Європейського Парламенту і Ради (ЄС) № 300/2008 від 11.03.2008 про спільні правила у сфері безпеки цивільної авіації та про скасування Регламенту (ЄС) № 2320/2002.
5. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive). O.J. L 333, 27.12.2022, p. 80–152.
6. Зубок В.Ю, Давидюк А.В., Клименко Т.М. Кібербезпека критичної інфраструктури в законодавстві України та в директиві (ЄС) 2022/2555. Electronic Modeling. 2023. V. 45. № 5, с. 54-66.
7. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance) PE/51/2022/REV/1 ELI: http://data.europa.eu/eli/dir/2022/2557/oj Official Journal of the European Union L 333, 27.12.2022, p. 164-198.
8. Business resilience and crisis management services. PwC's Global Centre for Crisis and Resilience Providing business resilience and crisis management services https://www.pwc.com/gx/en/issues/crisis-solutions.html.
9. Four ways organisations can evolve for disruption. Rethink resilience. https://www.pwc.co.uk/services/risk/rethink-risk/rethink-resilience.html).
10. Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure. 20.1.2023. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023H0120%2801%29.
11. Council Recommendation of 25 June 2024 on a blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance. Official Journal of the European Union. C series. C/2024/4371. 5.7.2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C_202404371.