РОЗДІЛ III

АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС. ФІНАНСОВЕ ПРАВО. ІНФОРМАЦІЙНЕ ПРАВО

УДК: 323.28

DOI: <https://doi.org/10.32366/2523-4269-2020-71-2-97-102>

Діхтяр Дмитро Юрійович,
здобувач

*(Донецький юридичний інститут МВС України,
м. Кривий Пир)*

ORCID: <https://orcid.org/0000-0002-5952-6563>

СУТНІСТЬ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ПРИЗНАЧЕННЯ ОРГАНІВ, ЯКІ ЗАБЕЗПЕЧУЮТЬ ОХОРОНУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У статті наголошено на тому, що захист об'єктів критичної інфраструктури є одним із пріоритетних напрямів діяльності держави. Проаналізовано законодавство у сфері захисту об'єктів критичної інфраструктури. Досліджено поняття критичної інфраструктури та види об'єктів критичної інфраструктури. Визначено моделі захисту критичної інфраструктури та зроблено висновок щодо доцільності їхнього запровадження в Україні в межах заходів із розбудови сектору безпеки й оборони.

Ключові слова: критична інфраструктура; об'єкти критичної інфраструктури; тероризм; диверсії; посягання на об'єкти критичної інфраструктури.

Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Останні події у світі наочно показують зростання терористичних атак, а згодом і військових конфліктів, що ґрунтуються на процесах глобалізації. Реалії сучасних політичних течій в Україні, наявність сепаратистських рухів, поглиблення розшарування населення за політичними суперечностями, збройний конфлікт на сході України, анексія Криму тощо створюють усередині держави багато загроз терористичного характеру.

Аналіз останніх досліджень і публікацій, у яких започатковано розв'язання окресленої проблеми й на які спирається автор. Дослідженню питань протидії тероризму було приділено значну увагу в працях вітчизняних та зарубіжних учених. Праці І. М. Ригова, В. В. Крутова, М. П. Стрельбицького, О. А. Шевченка, С. О. Кузнichenка, О. С. Шаптали, Д. В. Талалая, В. В. Мацюка, І. В. Євтушенка, С. С. Кудінова, І. І. Мусієнка та інших учених були присвячені питанню запобігання виникненню терористичних актів та мінімізації їхніх наслідків. Проблеми розповсюдження міжнародного тероризму розглядалися в працях Одрі Курт Кроніна, Кіта Л. Шимко, Фатхалі М. Могаддама, Лоуренса Тіо.

Безпосередньо питання посягання на об'єкти критичної інфраструктури були предметом дослідження таких сучасних авторів, як С. С. Теленик (щодо моделі адміністративно-правового регулювання захисту критичної інфраструктури), О. П. Єрменчук (стосовно

побудови системи захисту критичної інфраструктури в Україні з використанням досвіду сектору безпеки іноземних держав), С. Єсімов (про функціонування системи забезпечення безпеки критично важливої інформаційної інфраструктури) та інші вітчизняні й закордонні фахівці.

Формування цілей статті (постановка завдання). Головною метою дослідження є визначення місця та ролі органів, які забезпечують охорону та захист об'єктів критичної інфраструктури в секторі безпеки й оборони країни.

Виклад основного матеріалу. Сучасні глобалізаційні економічні процеси підсилюють появу та загострення терористичних актів. «Глобалізація» є терміном, за допомогою якого, зокрема, описують безперервний процес інтеграції об'єктів регіональних економік, суспільства та культури, формування мереж зв'язку й торгівлі загальносвітового рівня. Безпосередньо термін «глобалізація» стосується економічних процесів: інтеграції національних економік у світову економіку через торгівлю, прямі іноземні інвестиції, ринок капіталу, міграцію та поширення технологій [1].

Проведеними дослідженнями встановлено різні точки зору стосовно системних наслідків глобалізації щодо окремих об'єктів. Наприклад, у підході Р. Робертсона [2, с. 557] до опису глобалізації застосовано «об'єктові» характеристики: індустріалізацію і технічні зміни на окремих об'єктах; появу «європейських» об'єктів в Азії і Атлантиці; створення глобального світового порядку під американською гегемонією. Розвиваючи в певному сенсі вказані положення, М. Хана вважав, що глобалізація сприяла лібералізації трансміжнародних угод про передачу державного суверенітету щодо окремих об'єктів на суверенній території [3].

Після терактів 11 вересня виникла активна дискусія з приводу доцільності глобалізації з огляду на безпеку об'єктів, що є критично важливими для державного управління, національної та світової економіки, яка, відповідно, трансформувала наявні до цього часу погляди. Розглядаючи причини нападів на об'єкти критичної інфраструктури, Ф. М. Могхаддам указував, що роздроблена глобалізація мала побічним наслідком радикалізацію, конфлікти, терор і зіткнення ідеологій [4].

Із цієї причини, а також через терористичні атаки 13–14 листопада 2015 року в Парижі питання глобалізації, критичної інфраструктури та терористичної загрози почали поєднуватися в одну систему боротьби з тероризмом і міграційною кризою, яка безпосередньо почала формуватися під час економічного саміту G20 15 листопада 2015 року в Анкарі.

Відтоді дедалі ширше використовується інтегрований підхід до забезпечення безпеки систем, об'єктів і ресурсів, які є критично важливими від злочинних посягань та терористичних загроз, а також загроз іншої природи – природних, техногенних, соціальних, військових.

Здійснений С. Ф. Гончаром, Г. П. Леоненком, О. Ю. Юдіним аналіз методик (послідовностей) проведення робіт із формування складових частин систем захисту об'єктів критичної інфраструктури, таких як організаційно-технічні та режимні заходи й методи, програмно-технічні методи й засоби захисту надає змогу виділити основні етапи їхнього створення:

- визначення ресурсів, а також об'єктів, які підлягають захисту, – об'єктів захисту;
- формування переліку потенційно можливих загроз і каналів витоку інформації на об'єктах критичної інфраструктури;
- оцінку ризиків завдання збитків компонентам системи за наявності вразливостей, загроз, сприятливих умов для реалізації цих загроз;
- визначення вимог до системи захисту;
- здійснення вибору засобів захисту та їхніх характеристик;
- упровадження і організацію використання вибраних заходів, способів і засобів захисту;
- здійснення контролю цілісності та керування системою захисту [5].

Не минула ця тенденція і Україну. Як зазначав С. С. Теленик, об'єднання в концепції критичної інфраструктури систем, об'єктів і ресурсів, які є вкрай важливими для суспільства й держави, засвідчує значущість забезпечення їхнього захисту, що передбачає формування

самостійного напряму адміністративно-правового регулювання [6]. І хоча термін «критична інфраструктура» ще не отримав свого законодавчого визначення, він де-факто вже використовується в таких основоположних документах, як Закон України «Про національну безпеку України».

Слід погодитися з позицією Д. С. Бірюкова, який ще у 2012 році вказував на низку категорій об'єктів, що виокремлюються із загалу на підставі їхньої вагомості для економіки, техногенної безпеки, терористичної загрози тощо. У контексті міжнародної практики, на його думку, такі об'єкти (або певну частину таких об'єктів) слід позначати «критичною інфраструктурою» [7, с. 75].

Також, згідно з позицією згаданого вище автора, загальну проблему складають відсутність взаємозв'язку між ними (об'єктами), відомствами, до сфери управління яких вони належать, брак загального оцінювання на рівні держави ризиків цих об'єктів, спільного підходу до захисту від усіх груп загроз (техногенного, природного та соціально-політичного спрямування) [7, с. 76].

Відповідно до сучасного Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави [8], критична інфраструктура – сукупність об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або руйнування яких може мати вплив на національну безпеку та оборону, природне середовище, призвести до значних фінансових збитків та людських жертв; об'єкти критичної інфраструктури – підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки й безпеки держави, суспільства та населення.

Директива Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їхньої охорони та захисту № 2008/114/ЄС [9] визначає критичну інфраструктуру як об'єкт, систему, або її частину, розташовану в державах-членах, що є суттєвою для підтримки життєво важливих громадських функцій, здоров'я, безпеки, захищеності, економічного або соціального добробуту населення, пошкодження або знищення якої матиме істотний вплив у державі-члені через неспроможність такої інфраструктури підтримувати згадані функції.

Під критичною інфраструктурою у США розуміють «системи та ресурси, фізичні чи віртуальні, настільки життєво важливі для Сполучених Штатів, що недієздатність або знищення таких систем або ресурсів підриває національну безпеку, національну економіку, здоров'я або безпеку населення, або має своїм результатом будь-яку комбінацію з переліченого».

Станом на жовтень 2019 року лише формується законодавча база захисту об'єктів критичної інфраструктури та залишається не визначеним на загальнодержавному рівні орган, який буде здійснювати формування державної політики захисту об'єктів критичної інфраструктури, а також орган (військове формування), на який буде покладена реалізація завдань захисту об'єктів критичної інфраструктури від різного роду загроз. Так, базовий законопроект № 10328 «Про критичну інфраструктуру та її захист» було відкликано 29.08.2019. Згідно з останнім, об'єкт критичної інфраструктури мав визначатись у встановленому законодавством порядку як складовий елемент критичної інфраструктури, функціональність, безперервність, цілісність і стійкість якого забезпечують реалізацію життєво важливих національних інтересів.

Відмова від запропонованого підходу вимагає повернутися до питання розробки національної моделі функціонування суб'єктів захисту об'єктів критичної інфраструктури або запровадження дієвого досвіду інших країн у цій сфері. Так, щодо останнього напрямку О. П. Єрменчук стверджує, що загальні підходи до захисту критичної інфраструктури можна поділити на дві основні групи (моделі функціонування):

— «американську», де значні повноваження надані органам державної безпеки та розвідувальним органам, при них організовані та діють органи із захисту критичної інфраструктури, функціонують досить потужні аналітичні центри, державним органам доводиться актуальна аналітична інформація для прийняття управлінського рішення, уживаються заходи з виявлення та локалізації загроз;

— «урядову», за якої при національному уряді створюються спеціально уповноважені органи для захисту критичної інфраструктури, однак дещо вужчі повноваження спецслужб, які в основному залучаються до відпрацювання окремих завдань органів із захисту критичної інфраструктури, участі у визначенні критично-важливих об'єктів, припинення загроз у сфері тероризму тощо [10]. Ученим зазначено, що прикладом «урядової» моделі залучення спецслужб у процес захисту критичної інфраструктури є чинні системи в Польщі та Литві. Також слід звернути увагу, що забезпечення безпеки об'єкта в тексті проекту Закону № 10328 «Про критичну інфраструктуру та її захист» мало бути покладено на «оператора об'єкта» та уповноважений орган у сфері захисту критичної інфраструктури України.

Висновки з наданого дослідження і **перспективи подальших розвідок** в окресленому напрямі. Суб'єкти захисту об'єктів критичної інфраструктури мають здійснювати відповідну діяльність щодо протидії загрозам терористичного характеру:

– терористичним актам – застосуванню зброї, учиненню вибуху, підпалу чи інших дій, які створюють небезпеку для життя чи здоров'я людини або заподіяння значної майнової шкоди чи настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення, або з метою впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами, або привернення уваги громадськості до певних політичних, релігійних чи інших поглядів винного (терориста), а також погрози вчинення зазначених дій із тією самою метою.

У разі, коли терористична діяльність супроводжується вчиненням злочинів, передбачених статтями 112, 147, 258–260, 443, 444, а також іншими статтями Кримінального кодексу України, відповідальність за їхнє вчинення настає відповідно до Кримінального кодексу України;

– диверсіям – учиненню з метою ослаблення держави вибухів, підпалів або інших дій, спрямованих на масове знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їхньому здоров'ю, на зруйнування або пошкодження об'єктів, які мають важливе народногосподарське чи оборонне значення, а також учиненню з тією самою метою дій, спрямованих на радіоактивне забруднення, масове отруєння, поширення епідемій, епізоотій чи епіфітотій (стаття 113 Кримінального кодексу України);

– іншим злочинам загальнокримінального характеру, що скоюються з мотивів очевидної неповаги до держави, суспільства та супроводжуються особливою зухвалістю чи винятковим цинізмом.

Відповідні подальші наукові розвідки мають спрямовуватися на обґрунтування запровадження в Україні «урядової» моделі захисту об'єктів критичної інфраструктури та напрацювання параметрів контрдиверсійної діяльності уповноваженого органу.

Список використаних джерел

1. Foundationfor Tolerance International. URL : <http://www.fti.org.kg/eng/welcome.php> (дата звернення: 11.03.2020).
2. Robertson, Robbie (2004) «The Historical Context and Significance of Globalization», Development and Change 35 (3).
3. Muqtedar Khan. Teaching Globalization in the Era of Terrorism. URL : <http://www.ijtihad.org/globalterror.htm> (дата звернення: 21.03.2020).
4. Fathali M. Moghaddam. HOW GLOBALIZATION SPURS TERRORISM. The lopsided Benefits of «One World» and Why That Fuels Violence. Part one The global context of terrorism, 2008.

5. Гончар С. Ф., Леоненко Г. П., Юдін О. Ю. Теоретико-методологічний аспект забезпечення інформаційної безпеки об'єктів критичної інфраструктури. *Вісник Національного університету "Львівська політехніка". Комп'ютерні системи та мережі*. 2014. № 806. С. 34–39. URL : http://nbuv.gov.ua/UJRN/VNULPKSM_2014_806_8 (дата звернення: 07.03.2020).
6. Теленик С. С. Критична інфраструктура як об'єкт адміністративно-правового регулювання. *Юридичний часопис Національної академії внутрішніх справ*. 2018. № 1. С. 179–189. URL : http://nbuv.gov.ua/UJRN/aymvs_2018_1_17 (дата звернення: 20.03.2020).
7. Бірюков Д. С., Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Київ : НІСД, 2012. 96 с.
8. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави : Постанова Кабінету Міністрів України від 23.08.2016 р. № 563. URL : <http://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF> (дата звернення: 15.03.2020).
9. Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту № 2008/114/ЄС : Директива Ради 2008/114/ЄС від 08.12.2008 р. URL : http://zakon.rada.gov.ua/laws/show/984_002-08 (дата звернення: 02.04.2020).
10. Єрменчук О. П. Побудова системи захисту критичної інфраструктури в Україні з використанням досвіду сектору безпеки іноземних держав. Актуальні проблеми вдосконалення чинного законодавства України. Івано-Франківськ, 2017. № XLIV. С. 224–235.

References

1. Foundationfor Tolerance International. URL : <http://www.fti.org/kg/eng/welcome.php>.
2. Robertson, Robbie (2004). «The Historical Context and Significance of Globalization», *Development and Change* 35 (3).
3. Muqtedar Khan. Teaching Globalization in the Era of Terrorism. URL : <http://www.ijtiihad.org/globalterror.htm>.
4. Fathali M. Moghaddam. HOW GLOBALIZATION SPURS TERRORISM. The lopsided Benefits of «One World» and Why That Fuels Violence. Part one The global context of terrorism, 2008.
5. Honchar, S. F., Leonenko, H. P., Yudin, O. Yu. (2014). Teoretyko-metodolohichniy aspekt zabezpechennia informatsiinoi bezpeky ob'ektiv krytychnoi infrastruktury. *Visnyk Natsionalnoho universytetu Lvivska politehnika. Kompiuterni systemy ta merezhi* [Theoretical and methodological aspect of ensuring information security of critical infrastructure facilities. Bulletin of the National University Lviv Polytechnic. Computer systems and networks]. № 806. S. 34–39 [in Ukrainian].
6. Telenyk, S. S. (2018). Krytychna infrastruktura yak ob'ekt administratyvno-pravovoho rehuliuвання. *Yurydychnyi chasopys Natsionalnoi akademii vnutrishnikh sprav* [Critical infrastructure as an object of administrative regulation. Law Journal of the National Academy of the Interior]. № 1. S. 179–189 [in Ukrainian].
7. Biriukov, D. S., Kondratov S. I. (2012). Zakhyst krytychnoi infrastruktury: problemy ta perspektyvy vprovadzhennia v Ukraini [Critical infrastructure protection: challenges and prospects for implementation in Ukraine]. Kyiv : NISD. 96 s. [in Ukrainian].
8. Pro zatverdzhennia Poriadku formuvannia pereliku informatsiino-telekomunikatsiinykh system ob'ektiv krytychnoi infrastruktury derzhavy. Postanova Kabinetu Ministriv Ukrainy vid 23.08.2016 [On approval of the Procedure for forming a list of information and telecommunication systems of critical infrastructure objects of the state. Resolution of the Cabinet of Ministers of Ukraine dated 23.08.2016]. № 563 [in Ukrainian].
9. Pro identyfikatsiiu i vyznachennia yevropeiskyykh krytychnyykh infrastruktur ta otsiniuvannia neobkhdnosti pokrashchennia yikh okhorony ta zakhystu. Dyrektyva Rady 2008/114/IeS vid 08.12.2008 [On the identification and identification of European critical infrastructures and the assessment of the need to improve their guard and defence. Council Directive 2008/114 / EU dated 08.12.2008] [in Ukrainian].
10. Yermenchuk, O. P. (2017). Pobudova systemy zakhystu krytychnoi infrastruktury v Ukraini z vykorystanniam dosvidu sektoru bezpeky inozemnykh derzhav. Aktualni problemy vdoshkonalennia chynnoho zakonodavstva Ukrainy. [Construction of critical infrastructure protection system in Ukraine using the experience of foreign sector sector. Current issues of improving the current legislation of Ukraine]. Ivano-Frankivsk. № 44. S. 224–235 [in Ukrainian].

Dikhtiar Dmytro,

Applicant

(Donetsk Law Institute, MIA of Ukraine, Kryvyi Rih)

ORCID: <https://orcid.org/0000-0002-5952-6563>

THE ESSENCE OF CRITICAL INFRASTRUCTURE PROTECTION AND THE APPOINTMENT OF BODIES WHICH PROVIDE THE PROTECTION OF CRITICAL INFRASTRUCTURE OBJECTS

The article emphasizes that the protection of facilities of critical infrastructure is one of priority directions of state activities. The connection between modern globalization economic processes with the emergence and aggravation of terrorist threat has been investigated. The carried out studies have shown different perspectives on the systemic effects of globalization concerning individual facilities. Legislation in the area of critical infrastructure protection has been analyzed. The article also emphasizes on the widespread use of an integrated approach to the assurance of the security of systems, facilities and resources that are critically important of criminal threats and terrorist threats, as well as natural, man-made, social, military threats, as threats of a different nature. The concepts of critical infrastructure and types of facilities of critical infrastructure have been explored. On the basis of studying the methods (sequences) of carrying out the works on the formation of components of systems for protection of critical infrastructure facilities, the main stages of their creation are identified. The system of threats to facilities of critical infrastructure has been developed, which, by means of encroachment, includes terrorist acts, sabotage, and other crimes of general criminal nature, which are committed on the grounds of clear disrespect for the state, society and are accompanied by special boldness or exceptional cynicism. The models of critical infrastructure protection have been identified and the conclusion regarding the feasibility of implementing them in Ukraine within the activities of security and defence sector development has been drawn.

Key words: critical infrastructure; facilities of critical infrastructure; terrorism; sabotage; encroachment on critical infrastructure.

Надійшла до редколегії 17.03.2020