Електронне "**Державне управління: удосконалення та розвиток**"
включено до переліку наукових фахових видань України з питань державного управління
(Категорія «Б», Наказ Міністерства освіти і науки України від 28.12.2019 №1643)
www.dy.nayka.com.ua | № 1 2022 р. | 27.01.2022

DOI: 10.32702/2307-2156-2022.1.38

УДК 351.862.4:340.13

О. І. Яременко,
к. держ. упр., доцент, доцент кафедри публічного управління та адміністрування,
Вінницький державний педагогічний університет імені М.Коцюбинського
ORCID ID 0000-0002-3053-2257
Я. О. Страхніцький,
аспірант кафедри публічного управління та адміністрування,
Вінницький державний педагогічний університет імені М.Коцюбинського
ORCID ID 0000-0002-3066-0961

ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

O. I. Yaremenko
PhD in Public Administration, Associate Professor of the Department of Public Administration,
Vinnytsia Mykhailo Kotsiubynsky State Pedagogical University
Y. O. Strakhnitskyi
Graduate student of the Department of Public Administration
Vinnytsia Mykhailo Kotsiubynsky State Pedagogical University

THEORETICAL AND METHODOLOGICAL BASES OF ENSURING THE SYSTEM OF PROTECTION OF CRITICAL INFRASTRUCTURE OF THE STATE

У статті визначено та обґрунтувано спектр загроз, наявність яких детермінує необхідність забезпечення дієвого захисту об'єктів критичної інфраструктури. Одним із таких напрямів розглянуто політику «експлуатаційної ефективності» – прагматизації розподілу та застосування державних безпекових ресурсів задля локалізації потенційних джерел небезпеки.

Проаналізовано підходи вітчизняних та іноземних вчених до формулювання змісту поняття «загроза об'єктам критичної інфраструктури» у результаті чого помічено спільний акцент на видах ризиків і загроз, вплив яких може викликати диферентну дестабілізацію на різних ієрархічних рівнях, найвищий із яких – національна безпека.

Розглянуто зміст окремих нормативно-правових актів, що дало підстави деталізувати перелік загроз критичній інфраструктурі та підтвердити приналежність критичної інфраструктури до складових забезпечення національної безпеки України. На основі критичного аналізу узагальнено розподіл загроз критичній інфраструктурі на три основні категорії: природного походження, техногенного характеру і зловмисні дії. Запропоновано доповнити даний перелік комбінованими загрозами, які здатні викликати «каскадний ефект дестабілізації критичної інфраструктури».

Акцентовано увагу на складності ідентифікації критичних об'єктів на національному, регіональному або локальному рівнях інфраструктури. Досліджено методику віднесення об'єктів національної інфраструктури до сфери критичної відповідно до важливості їх

функцій та послуг які вони виконують. Описано перелік життєво важливих функцій та послуг, представники з надання яких потребують захисту, як об'єкти критичної інфраструктури.
Проаналізовано теоретичні підходи до обґрунтування поняття «захист критичної інфраструктури» у вітчизняних та закордонних дослідженнях і на основі їх узагальнення запропоновано удосконалене авторське формулювання даної дефініції.

The article identifies and substantiates the range of threats to critical infrastructure, the presence of which determines the need to ensure effective protection of critical infrastructure. One of such areas is the policy of «operational efficiency» – pragmatization of the allocation and use of state security resources to localize potential sources of danger.
The approaches of domestic and foreign scientists to the wording of the concept of "threats to critical infrastructure" are analyzed, resulting in a common emphasis on the types of risks and threats, the impact of which can cause differential destabilization at different hierarchical levels, the highest of which is national security.
The content of certain normative legal acts is considered, which gave grounds to detail the list of threats to critical infrastructure and to confirm the affiliation of critical infrastructure to the components of ensuring the national security of Ukraine. Based on the analysis, the division of threats to critical infrastructure into three main categories is generalized: critical situations of natural nature, emergencies of man-made nature and malicious actions. It is proposed to supplement this list with combined threats that can cause a "cascade effect of destabilizing critical infrastructure."
Emphasis is placed on the difficulty of identifying critical objects at the national, regional or local levels of infrastructure. The method of classifying national infrastructure facilities as critical according to the importance of their functions and the services they perform has been studied. The list of vital functions and services that need to be protected as critical infrastructure is described.
Theoretical approaches to substantiation of the concept of "critical infrastructure protection" in domestic and foreign studies on the basis of their generalization are analyzed, the author's improved formulation of this definition is offered.
The key priorities in the direction of ensuring the security of critical infrastructure are outlined, in particular: comprehensive modernization of the legal field in the direction of institutional support for the protection of critical infrastructure, updating the paradigm of public administration in this sector; expansion of the subject structure of critical infrastructure protection, development of public-private partnership; monitoring of operational information on threats to critical infrastructure; development of international cooperation in this field.

Ключові слова: *критична інфраструктура; загрози; безпека; захист критичної інфраструктури; критично важливі об'єкти; державна парадигма безпеки.*

Keywords: *critical infrastructure; threats; security; critical infrastructure protection; critical facilities; state security paradigm.*

Постановка проблеми. Сучасна епоха розвитку людства відзначалася безліччю серйозних катастроф починаючи від природних явищ, таких як землетруси, повені, цунамі, вулканічні виверження до техногенних аварій, терористичних актів, кібератак та військової агресії. В таких умовах на новий рівень виходить потреба сучасного суспільства бути захищеним та готовим протистояти таким несподіваним несприятливим подіям і відновлюватися після них. Щоб гарантувати підготовку та відновлення суспільства, особливу увагу варто спрямувати на зниження вразливості важливих систем, які підтримують економічну, екологічну та соціальну життєдіяльність сучасного суспільства, тобто – сферу критичної інфраструктури. Це обумовлює актуальність питання наукового обгрунтування основ забезпечення системи захисту критичної інфраструктури держави.

Аналіз останніх досліджень і публікацій. Серед вітчизняних учених, які присвятили свої наукові дослідження проблематиці, пов'язаній із загрозами критичній інфраструктурі варто відзначити праці Д. Г. Бобро [1] О. М. Суходолі [3], вивченню державної системи захисту критичної інфраструктури в Україні присвячені доробки Я. Я. Пушак [2], М. І. Флейчук [2], В. І. Франчук [2], С. С. Теленик [13] та аналіз

кордонного досвіду описують Євсєєв В. О. [4], Єрменчук О. П. [5-6], Теленик С. С. [12] та ін. Разом із тим, потребує накового удосконалення теоретичне наповнення поняття «захист критичної інфраструктури», обґрунтування спектру загроз критичній інфраструктурі відповідно до сучасних умов, а також аналізу та удосконалення інституційного забезпечення системи захисту критичної інфраструктури держави.

Цілі статті полягають у дослідженні наукових підходів та удосконаленні підходів до питання загроз критичній інфраструктурі, предмету та складових забезпечення системи її захисту.

Виклад основного матеріалу. Вивичаючи проблематику захисту критичної інфраструктури держави, варто визначити спектр небезпек, наявність яких детермінує таку необхідність. Так, у Європейській програмі захисту критичної інфраструктури [15] члени Комісії європейських спільнот акцентують увагу на тому, що об'єкти критичної інфраструктури можуть бути пошкоджені, знищені або порушені в результаті навмисних терористичних актів, стихійних лих, недбалості, нещасних випадків, хакерської атаки, злочинної діяльності або зловмисної поведінки. Отже, можемо стверджувати, що з метою захисту життя, здоров'я та майна свого народу, державне управління має бути сконцентовано на забезпеченні захисту критичної інфраструктури від загроз порушення її функціонування. У цьому контексті розглядаємо забезпечення безпеки об'єктів критичної інфраструктури як невід'ємну парадигму державного управління, в рамках якої можливості інфраструктурної адаптативної керованості будуть пріоритетними. Вважаємо, що для цього потрібна політика «експлуатаційної ефективності» – прагматизації розподілу та застосування державних безпекових ресурсів задля локалізації потенційних джерел небезпеки. Тут варто акцентувати увагу не стільки на продуктивності окремих їх елементів, а скоріше на стратегії пов'язаній із міжсистемними комунікаціями.

Акцентуємо увагу на обґрунтуванні спектру загроз для критичної інфраструктури. Ще з початку 1990-х років дослідники з Європи та Америки в різних галузях науки, працюючи над проблематикою захисту критичної інфраструктури. Визначення поняття «захист критичної інфраструктури» зустрічаються у нормативних актах різних держав та наукових доробках учених. Дефінітив «загроза» можемо віднайти у діючому Законі України «Про національну безпеки України» [8] як «явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України». Під «загрозою» в контексті захисту критичної інфраструктури Бобро Д. Г. пропонує розуміти «наявні та потенційно можливі явища та чинники, що створюють небезпеку сталому функціонуванню об'єктів критичної інфраструктури та можуть призвести до негативних наслідків» [1]. Вважаємо дане визначення цілком об'єктивним, що можна підтвердити майже ідентичним його формулюванням у Зеленій книзі захисту критичної інфраструктури ЄС, де під цим терміном розуміються «будь-які обставини або події, що можуть порушити стале функціонування або знищити критичну інфраструктуру чи будь-який її елемент а також будь-які спроби та наміри завдання шкоди критичним активам» [15]. Даного змістовного наповнення притримується і Єременчук О. П., який під загрозами об'єктам критичної інфраструктури пропонує розуміти «наявні або потенційно можливі явища і чинники, що можуть нанести шкоду такому об'єкту (фізичному або у кіберпросторі), вивести його з ладу або порушити функціонування відповідно до призначення, чим створюють небезпеку життєво важливим національним інтересам України» [6].

У нормативних документах США спектр загроз критичній інфраструктурі конкретизують у межах сфер їх походження як «природні або техногенні явища, фізичних осіб, суб'єктів чи дії, що містять або несуть потенційну шкоду для життя, інформації, операцій, навколишнього середовища та/або власності» [5].

Отже, аналізуючи приведені визначення можемо прослідкувати акцент на видах ризиків і загроз, вплив яких може викликати різного роду дестабілізацію на різних ієрархічних рівнях, найвищий із яких – загрози національній безпеці. Деталізований перелік таких загроз у нашій державі можемо віднайти у тексті Стратегії національної безпеки України 2020 року [12]. Варто відзначити, що новий Закон «Про критичну інфраструктуру» регламентує захист критичної інфраструктури складовою частиною забезпечення національної безпеки України. Цілком погоджуємось із даним формулюванням, мотивуючись ще одним аргументом, закріпленим Стратегією внутрішньої безпеки США [17], якою визначено шість основних напрямів забезпечення національної безпеки, серед яких і захист критичної інфраструктури (рис. 1).

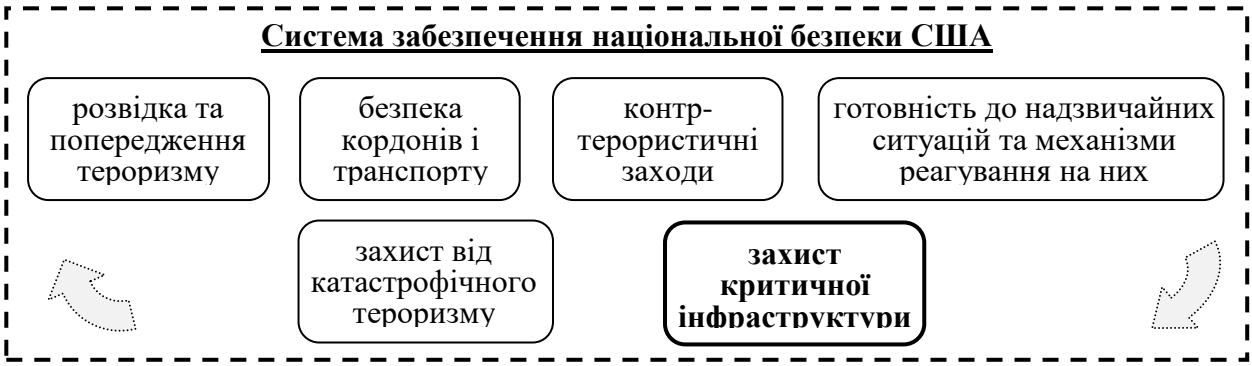

Рис.1. Структура системи забезпечення національної безпеки США

Джерело: сформовано авторами за даними [17],[3]

Враховуючи вищезазначене, перелік загроз національній безпеці, який визначено Стратегію національної безпеки України [11], варто враховувати і при формуванні системи захисту критичної інфраструктури:

1. Зміни клімату та ризик надзвичайних ситуацій природного і техногенного характеру, виникнення і поширення інфекційних хвороб.
2. Чергова гонка озброєнь на основі нових фізичних принципів.
3. Поширення міжнародного тероризму та злочинності у кіберпросторі, наркоторгівлі, торгівлі людьми, сепаратизму, розповсюдження зброї та ін.
4. Поширення коронавірусної хвороби (COVID-19) що детермінує каскад негативних наслідків таких як: криза охорони здоров'я та соціального захисту, зростання безробіття, зниження продовольчої безпеки, обмеження руху, товарів та робочої сили, розвиток глобальної фінансово-економічної кризи.
5. Посилення міжнародної конкуренції із демонстрацією «національної сили», у тому числі збройна експансія проти України Російської Федерації.
6. Дефіцит фінансування на модернізацію систем озброєння радянського виробництва, які вичерпали свій ресурс.
7. Недостатня ефективність і корумпованість державних органів влади.
8. Низький рівень добробуту населення.
9. Недостатній рівень конкуренції, низька правова захищеність у ключових сферах (зокрема в енергетиці) та значна доля державного сектору в економіці, що гальмує її інвестиційну діяльність.
10. Погіршення середовища життєдіяльності громадян (якість повітря, води, продуктів харчування, нераціональне використання природних ресурсів).
11. Погіршення демографічної ситуації та прогресуюча еміграція кадрів.

Варто також відзначити посилення ролі загроз для критичної інфраструктури, які законотворці виділили як окремий пункт та пов'язали із погіршенням її технічного стану, відсутністю інвестицій в її розвиток та модернізацію, несанкціоновані фізичні- або кібер- втручання, пролонговані бойові дії на Сході країни, а також тимчасову окупацію частини території.

Аналізуючи окремі приклади у законодавчій базі іноземних держав [15], [17], зазначимо що спільною рисою є розподіл загроз критичній інфраструктурі на три основні категорії:

1. Надзвичайні ситуації природного характеру;
2. Надзвичайні ситуації техногенного характеру;
3. Зловмисні дії.

Бобро Д. Г. [1] пропонує додати до цього переліку ще комбіновані загрози, які учений вважає особливо небезпечними, оскільки вони можуть спричинити «ефект доміно» у вигляді різноманітних каскадних ефектів внаслідок синергії елементів критичної інфраструктури між собою. Вважаємо, що симантичний опис даного явища краще розкриє дефінітив «каскадний ефект дестабілізації критичної інфраструктури» – причинно-наслідкове явище, яке виникає від дестабілізації у функціонуванні одного інфраструктурного елементу, що детермінує збій у інших взаємопов'язаних системах. Наприклад, водопостачання залежить від енергозабезпечення насосних станцій, фінансовий сектор корелює з безпекою інформаційно-компютерних систем, пожежні служби залежать від водопостачання і т.п.

Акцентуємо увагу ще на одному важливому питанні – віднесенні об'єктів національної інфраструктури до критичної відповідно до важливості функцій та послуги які вони виконують. Аналіз вітчизняних нормативно-правових актів дає підстави всі потенційні об'єкти критичної інфраструктури, які потребують захисту, узагальнити у квадро-комплекс:

1. Великі об'єкти критичної інфраструктури загальнодержавного значення.
2. Життєво важливі об'єкти критичної інфраструктури.
3. Важливі об'єкти критичної інфраструктури.
4. Необхідні об'єкти критичної інфраструктури.

Проблемою у реалізації державної політики у сфері захисту критичної інфраструктури учені вбачають складність ідентифікації об'єктів критичними на національному, регіональному або локальному рівнях

інфраструктури [10]. Ключ до відповіді на дане питання вітчизняні законотворці надали у Законі України «Про критичну інфраструктуру» [7] де зазначили перелік життєво важливих функцій та послуг, представники з надання яких потребують захисту, як об'єкти критичної інфраструктури. До таких послуг належить: енергозабезпечення; водопостачання та водовідведення; продовольче забезпечення; охорона здоров'я; фармацевтична промисловість; виготовлення вакцин, стале функціонування біолабораторій; інформаційні послуги; електронні комунікації; фінансові послуги; транспортне забезпечення; оборона, державна безпека; правопорядок, здійснення правосуддя, тримання під вартою; цивільний захист населення та територій, служби порятунку; космічна діяльність, космічні технології та послуги; хімічна промисловість; дослідницька діяльність. Вважаємо, що даний перелік є не є вичерпним та достатньо деталізованим, він здатний варіювати залежно від розміру країни та може досягати декількох тисяч пунктів. Наприклад, у США до списку критичних об'єктів включено більше 1,7 тис на національному рівні та близько 33 тис на регіональному і місцевому рівнях [17]. Наше твердження також можна підтвердити словами В. О. Євсєєва [4], який наголошує, що згідно із світовою практикою, до об'єктів критичної інфраструктури, для яких встановлюються особливі умови забезпечення захисту та функціонування в Україні, також необхідно віднести підприємства стратегічного значення для економіки та безпеки; важливі державні об'єкти, у тому числі пункти управління органів державної влади та органів місцевого самоврядування; об'єкти можливих терористичних посягань; об'єкти, які підлягають охороні і обороні в умовах надзвичайних ситуацій і в особливий період; об'єкти, що підлягають обов'язковій охороні підрозділами Державної служби охорони за договорами; об'єкти підвищеної небезпеки; об'єкти, які включені до Державного реєстру потенційно небезпечних об'єктів; радіаційно небезпечні об'єкти; чергово-диспетчерська система екстреної допомоги; аварійно-рятувальні служби; Національна система конфіденційного зв'язку; платіжні системи; нерухомі об'єкти культурної спадщини.

Фідбеком до загроз визначеним об'єктам має стати гарантія їх безпеки. Погодимося із переконанням вітчизняних учених [2], які поняття «безпека» аналізуть у спектрі філософської категорії, пояснюючи це тим, що дане поняття охоплює всі належні аспекти життєдіяльності громадян, суспільства і держави. Як правило, при дослідженні сутності «безпеки» акцентується увага на трьох аспектах: концептуальному (онтологічні і епістемологічні базиси безпеки); практичному (безпека визначається у контексті базових потреб індивіда); ціннісному (гносеологічний підхід та культура безпеки). При визначенні поняття «безпека» сучасні дослідники спираються на розуміння її як стану, ступеню захищеності; відсутності загроз; комплексу безпекових заходів [2].

Вітчизняні учені захист критичної інфраструктури визначають як «комплекс заходів, реалізований у нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури [9]. Цю позицію відстоює у своїх працях і С. С. Теленик [13]. Вважаємо більш змістовна трансформація у розумінні даного поняття викладена в аналітичній доповіді «Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки» [3], де авторський колектив під захистом критичної інфраструктури вбачає «усі види діяльності, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз об'єктам критичної інфраструктури; мінімізацію та ліквідацію наслідків у випадку реалізації загроз; швидке відновлення функціонування критичної інфраструктури».

У директиві Президента США з питань національної безпеки забезпечення безпеки критичної інфраструктури визначено, як «зменшення ризику критичної інфраструктури від втручання, атак або ефектів, спричинених природними катастрофами або людською діяльністю, за рахунок реалізації заходів із фізичного захисту або кіберзахисту» [17].

Єременчук О. П. у захист критичної інфраструктури включає «систему скоординованих організаційних, нормативно-правових, адміністративних, пошукових, охоронних, режимних інженерно-технічних, наукових та інших заходів, матеріальних та нематеріальних засобів, спрямованих на забезпечення стійкості та безпеки критичної інфраструктури» [5].

Згідно нового Закону «Про критичну інфраструктуру» аналізований термін законотворці трактують як «усі види діяльності, що виконуються перед або під час створення, функціонування, відновлення і реорганізації об'єкта критичної інфраструктури, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об'єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації [7]. Дане трактування вважаємо вірним, однак не досить вичерпним. Помітно, що у всіх проаналізованих формулюваннях провідну роль у захисті критичних об'єктів надано державі в особі уповноважених нею органів. Однак, варто зауважити, що значна, а подекуди й основна частина об'єктів критичної інфраструктури знаходиться у приватній власності. У такому випадку, її захист пов'язаний із забезпеченням міжвідомчої координації, що обумовлює необхідність розширити коло відповідальних за межі державних інститутів. Аргументуємо свою позицію текстом Національної стратегії безпеки критичної інфраструктури Канади у якій підкреслюється, що «головна відповідальність за підвищення стійкості та швидкості регенерації критичної інфраструктури залишається за її власниками та операторами» [16]. Отже, на основі приведеної гіпотези, пропонуємо авторське формулювання дефініції «захист критичної інфраструктури» – цілеспрямована взаємоузгоджена спільна діяльність державних інститутів, власників та операторів об'єктів критичної інфраструктури, із застосування комплексу заходів, спрямованих на профілактику, запобігання і своєчасне виявлення потенційних та припинення або нейтралізацію реальних загроз; мінімізацію та ліквідацію наслідків та швидке відновлення функціонування критичної інфраструктури у разі її пошкодження, що реалізовуються з метою уникнення людських жертв, значних матеріальних та екологічних збитків, або інших драматичних

наслідків які можуть призвести до порушення національної безпеки й оборони. Фактично дане тлумачення змінює кут уваги із процесу захисту критичної інфраструктури на профілактику та попередження кризових ситуацій, а також диференціює відповідальність між державою, власниками та безпосереднім працівниками критичних об'єктів.

Варто зазначити, що у вітчизняному законодавстві в лиці держави, досі не передбачено єдиного інституту, відповідального за захист критичної інфраструктури. Частково протецією критичних об'єктів займається Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України та ін.. Окремі функції також притаманні системам цивільного захисту, боротьби з тероризмом, кібербезпеки, правоохоронних органів, регулювання енергетики та енергоринку та ін. У США, наприклад, за захист відповідних критичних секторів відповідають спеціальні галузеві органи: департаменти сільського господарства, продовольства, внутрішньої безпеки, енергетики, охорони здоров'я, управління безпеки транспорту, берегова охорона та ін.[13]. Отже, серед першочергових завдань забезпечення захисту критичної інфраструктури варто визначити необхідність розробки, удосконалення та затвердження нормативно-правових актів з питань модернізації державної системи захисту критичних об'єктів інфраструктури, зокрема, створити орган, відповідальний за координацію діяльності із захисту критичної інфраструктури в мирний час та в умовах особливого періоду.

Висновки. Аналізуючи поняття «критична інфраструктура» варто дійти висновку, що воно узагальнює найважливіші об'єкти порушення функціонування яких може спричинити невідворотні негативні процеси у державі та завдати суттєвих збитків життю, здоров'ю та благополуччю громадян, а також полісекторальні порушення ситуації в країні. Відповідно, від стабільності критичної інфраструктури залежить національна безпека. Отже, запровадження системи захисту критичної інфраструктури є одним із пріоритетів національної безпеки. Доцільно окреслити ключові пріоритети у напрямку гарантування безпеки критичної інфраструктури, зокрема: комплексна модернізація правового поля у напрямку інституційного забезпечення захисту критичної інфраструктури, актуалізація парадигми державного управління у даному секторі; розширення суб'єктного складу захисту критичної інфраструктури, розвиток державно-приватного партнерства; моніторинг оперативної інформації стосовно загроз критичній інфраструктурі; розвиток міжнародного співробітництва в цій сфері.

Список використаної літератури.

1. Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. Стратегічні пріоритети. Серія: Економіка. 2015. № 4. С. 83-93.
2. Державна політика забезпечення національної безпеки України: основні напрямки та особливості здійснення: монографія/ Криштанович М.Ф., Пушак Я.Я., Флейчук М.І., Франчук В.І. Львів: Сполом, 2020. 418 с
3. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналіт. доп. / за ред. О. М. Суходолі. Київ: НІСД, 2020. 28 с
4. Євсєєв В. О. Можливі шляхи удосконалення захисту критичної інфраструктури України з урахуванням світового досвіду. Збірник наукових праць ХНУПС. 2016. № 4. С. 168-172
5. Єрменчук О.П. Нормативно-правове регулювання діяльності у сфері захисту національної критичної інфраструктури: аналіз та узагальнення нормотворчої практики США. Науковий вісник ДДУВС. 2017. № 3. С. 135-140.
6. Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монографія. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.
7. Закон України «Про національну безпеки України». URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
8. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. мат-лів міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С.І. Конд ратов; за заг. ред. О. М. Суходолі. Київ: НІСД, 2015. 176 с.
9. Лойко В. В., Храпкіна В. В., Маляр С. А., Руденко М. В. (2020) Economic and legal principles of ensuring the protection of critical infrastructure. Фінансово-кредитна діяльність: проблеми теорії та практики 4 (35). С. 426-238
10. Постанова КМУ «Деякі питання об'єктів критичної інфраструктури» № 1109 від 09.10.2020 р. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text
11. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14.09.2020 р. «Про Стратегію національної безпеки України» № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020
12. Теленик С. С. Досвід правового регулювання системи захисту критичної інфраструктури в США. Науковий вісник НАВС. 2018. № 2 (107). С. 358–370.
13. Теленик С. С. Критична інфраструктура як об`єкт адміністративно-правового регулювання. Юридичний часопис Національної академії внутрішніх справ. 2018. № 1 (15). С. 179–189.
14. Communication from the Commission (2006), European Programme for Critical Infrastructure Protection. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF
15. Commission of the European Communities (2005), Green Paper on a European programme for critical infrastructure protection. URL: https://www.ab.gov.tr/files/ardb/evt/1_avrupa_birligi/1_6_raporlar/1_2_green_papers/com2005_green_paper_on_critical_infrastructure.pdf.
16. Her Majesty the Queen in Right of Canada (2009) National Strategy for Critical Infrastructure. URL:

https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf

17. Department of Homeland Security (2013), Presidential Policy Directive. Critical Infrastructure Security and Resilience. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

18. Senate and House of Representatives of the United States of America. USA Patriot Act of 2001. URL: https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

References.

1. Bobro, D. H. (2015), "Definition of criteria for assessment and threat to critical infrastructure", *Stratehichni priorytety. Seriia:Ekonomika*, vol 4, pp.83-93.

2. Kryshtanovych, M. F., Pushak, Y. Y., Flejchuk, M. I., Franchuk, V. I. (2020), *Derzhavna polityka zabezpechennia natsional'noi bezpeky Ukrainy: osnovni napriamky ta osoblyvosti zdijsnennia* [State policy of national security of Ukraine: main directions and features of implementation], Spolom, L'viv, 418 p.

3. Sukhodoli, O. M. (2020), *Derzhavna systema zakhystu krytychnoi infrastruktury v systemi zabezpechennia natsional'noi bezpeky* [State system of critical infrastructure protection in the system of national security], NISD, Kyiv, Ukraine, 28 p.

4. Yevsieiev, V. O. (2016), "Possible ways to improve the protection of critical infrastructure of Ukraine, taking into account world experience". Scientific Works of Kharkiv National Air Force University. vol 4. pp. 168-172.

5. Yermenchuk, O. P. (2017), "Normative legal regulation of activity in the protection of national critical infrastructure: analysis and coordination of US normative practice" Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs. vol 3, pp. 135-140.

6. Yermenchuk, O. P. (2018), *Osnovni pidkhody do orhanizatsii zakhystu krytychnoi infrastruktury v krainakh Yevropy: dosvid dlia Ukrainy* [Basic approaches to the organization of critical infrastructure protection in European countries: experience for Ukraine], Dniprop. derzh. un-t vnutr. sprav, Dnipro, Ukraine, 180 p.

7. The Verkhovna Rada of Ukraine (2018), The Law of Ukraine "On National Security of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/2469-19#Text (Accessed 19 January 2022).

8. Biriukov, D. S., Kondratov, S. I., Sukhodoli, O. M. (2015), *Zelena knyha z pytan' zakhystu krytychnoi infrastruktury v Ukraini.* [Green Paper on Critical Infrastructure Protection in Ukraine], NISD, Kyiv, Ukraine, 176 p.

9. Lojko V. V., Khrapkina V. V., Maliar S. A., Rudenko M. V. (2020), "Economic and legal principles of ensuring the protection of critical infrastructure", *Financial and credit activities: problems of theory and practice,* vol.4 (35), pp. 426-238

10. Cabinet of Ministers of Ukraine (2020), "Resolution "Some issues of critical infrastructure"", available at: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text (Accessed 15 January 2022).

11. President of Ukraine (2020), "Decree of the President of Ukraine "On the decision of the National Security and Defense Council of Ukraine "On the National Security Strategy of Ukraine"", available at: https://zakon.rada.gov.ua/laws/show/392/2020 (Accessed 15 January 2022).

12. Telenyk S. S. (2018), "Experience of legal regulation of critical infrastructure protection in the US", Scientific Herald of National Academy of Internal Affairs, vol. 2 (107), pp. 358–370.

13. Telenyk S. S. (2018), "The critical infrastructure as an object of administrative and legal regulation", Law Magazine of the National Academy of Internal Affairs, vol. 1 (15), pp. 179–189.

14. Communication from the Commission (2006), "European Programme for Critical Infrastructure Protection", available at: https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF (Accessed 15 January 2022).

15. Commission of the European Communities (2005), "Green Paper on a European programme for critical infrastructure protection", available at: https://www.ab.gov.tr/files/ardb/evt/1_avrupa_birligi/1_6_raporlar/1_2_green_papers/com2005_green_paper_on_critical_infrastructure.pdf. (Accessed 10 January 2022).

16. Her Majesty the Queen in Right of Canada (2009) "National Strategy for Critical Infrastructure", available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf (Accessed 10 January 2022).

17. Department of Homeland Security (2013), Presidential Policy Directive "Critical Infrastructure Security and Resilience", available at: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (Accessed 10 January 2022).

18. Senate and House of Representatives of the United States of America (2001), "USA Patriot Act of 2001", available at: https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf (Accessed 10 January 2022).

Стаття надійшла до редакції 20.01.2022 р.