Соціально-правові студії. 2021. Випуск 1 (11). С. 132-139
Social & Legal Studios. 2021. Issue 1 (11). P. 132-139

UDC(УДК) 343.98:351.862.4(100)

**Гора Ірина Віталіївна,**
доктор юридичних наук, професор,
головний науковий співробітник
науково-організаційного центру
Національної академії Служби безпеки України
(Київ, Україна)
e-mail: irvitgora@ukr.net
ORCID ID: 0000-0003-2940-5338

**Батюк Олег Володимирович,**
кандидат юридичних наук, доцент,
доцент кафедри політології,
управління та державної безпеки
Волинського національного університету
імені Лесі Українки
(Луцьк, Україна)
e-mail: Batiyk.Oleg@vnu.edu.ua
ORCID ID: 0000-0002-2291-4247

# ОКРЕМІ ПИТАННЯ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ЗАРУБІЖНИЙ ДОСВІД

**Анотація.** Проаналізовано нормативно-правові акти, які регулюють питання захисту об'єктів критичної інфраструктури в таких зарубіжних країнах, як Сполучені Штати Америки, Великобританія, Німеччина, Франція, Польща, Словаччина. За результатами проведеного аналізу зроблено низку висновків, а саме: термін «критична інфраструктура» введено до нормативно-законодавчих актів багатьох держав, де його розуміння дещо відрізняється, проте такі відмінності не суттєві. Загальним є те, що терміном «критична інфраструктура» зазвичай охоплюються ті об'єкти, системи, мережі або їх частини, порушення функціонування або руйнування яких призведе до найсерйозніших наслідків для соціальної та економічної сфери держави, негативно вплине на рівень її обороноздатності та національної безпеки.

**Ключові поняття:** безпека, держава, диверсія, закон, злочин, об'єкти, інфраструктура.

**Hora Iryna,**
Doctor of Law, Professor,
Chief Researcher of Scientific and Organizational Center,
National Academy of Security Service of Ukraine
(Kyiv, Ukraine)
e-mail: irvitgora@ukr.net
ORCID ID: 0000-0003-2940-5338

**Batiuk Oleh,**
PhD (Law), Associate Professor,
Associate Professor of the Department of Political Science,
Public Administration and National Security,
Lesya Ukrainka Volyn National University
(Lutsk, Ukraine)
e-mail: Batiyk.Oleg@vnu.edu.ua
ORCID ID: 0000-0002-2291-4247

# INDIVIDUAL ISSUES OF PROTECTION OF CRITICAL INFRASTRUCTURE: FOREIGN EXPERIENCE

**Abstract.** The authors carried out a scientific analysis of normative legal acts that govern issues of the protection of critical infrastructure in such foreign countries as the United States, Great Britain, the Federal Republic of

Germany, the Republic of France, the Republic of Poland and the Republic of Slovakia in the provisions of scientific article. The authors made conclusions that were based on the results of the carried out analysis, first, that the term "critical infrastructure" had been introduced into the normative legislative acts of many states, where its understanding is somewhat different, however, such differences are not significant. The common thread is that the term "critical infrastructure" usually covers those facilities, systems, networks or their parts, the disruption of the functioning or destruction of which will lead to the most serious consequences for the social and economic sphere of the state, will negatively affect the level of its defense capabilities and national safety. Second, the functioning of critical infrastructure is associated in peacetime with the support of vital functions in society, the protection of the basic needs of its members and the formation of their inner sense of safety and protection. Third, the approaches to the understanding of the general essence of the infrastructure, which is based on the functions that are performed by it, or the composition of economic entities that perform the specified functions, are seemed to be logical. The lists of sectors that belong to critical infrastructure in different countries are mostly similar, because the development of modern society is happened almost by uniform, although not fully convergent laws, rules, schemes. The available differences that are due primarily to national specifics, geopolitical conditions, traditions and features of the safe policy of a given country or international structure. Fourth, world experience points to that the most critical facilities are those that can be attributed to the sphere of provision of electricity and foodstuffs. Society is inclined today to believe that developed European and North American countries are not able to do without electric power in the long term. Civilization has progressed so much that people have lost the ability to live without an electric power and are not ready for it from the technical side.

**Key concepts:** safety, state, sabotage, law, crime, facilities, infrastructure.

**DOI 10.32518/2617-4162-2021-1-132-139**

**Вступ**

Актуальність обраної теми обумовлена тим, що безпека є фундаментальною потребою і окремої людини, і суспільства загалом. Віддавна проблема безпеки є особливим суспільним явищем, що укріплювалося й розширювалося відповідно до зростання загроз і небезпек для громадян і з боку внутрішніх, і зовнішніх ворогів. Нині забезпечення безпеки й надалі є одним із найважливіших завдань та функцій суспільства, держави. Останніми десятиліттями у європейських країнах і в Україні зокрема питання аналізу загроз значно актуалізувалося. Питання ідентифікації загроз та організації заходів із протидії їм набуває актуальності для більшості держав ЄС і часто пов'язується із загрозами природного характеру, залишаючи людський фактор дещо осторонь, на другому плані. Водночас значення роботи з визначення та своєчасної ідентифікації загроз для вжиття адекватних заходів з кожною такою подією зростає. Водночас зростає і глобальність підходів до визначення загроз. Спершу цей процес характеризувався локальним чи державним рівнем. Донедавна базовий підхід до гарантування безпеки критичної інфраструктури був майже виключно зосереджений саме на захисті її конкретних структур, ресурсів і об'єктів від обмеженого кола небезпечних, але загалом відомих і порівняно очікуваних загроз.

Науковим дослідженням окремих питань безпеки об'єктів критичної інфраструктури присвячено роботи таких науковців, як С. О. Андреєв, Д. С. Бірюков, С. Ф. Гончар, В. О. Євсєєв, О. П. Єрменчук, С. І. Кондратов, Г. П. Леоненко, Г. П. Ситник, О. М. Суходоля, О. Ю. Юдін. Варто зауважити, що наукових досліджень, присвячених проблемам зарубіжного досвіду захисту об'єктів критичної інфраструктури, фактично немає, що зумовило підготування цієї наукової праці.

*Метою статті* є здійснення огляду нормативно-правових актів зарубіжних країн стосовно окремих питань захисту об'єктів критичної інфраструктури й відтак пропонування змін і доповнень до чинного законодавства України для вдосконалення питань захисту об'єктів критичної інфраструктури.

**1. До питання розуміння критичної інфраструктури в Україні та світі**

У країнах світу, які в рамках забезпечення національної безпеки вживають поняття «критична інфраструктура», під нею розуміють об'єкти та системи, настільки важливі для забезпечення життєдіяльності людей і держави, дестабілізація роботи яких, не мовлячи про колапс, призведе до тяжких негативних або навіть катастрофічних наслідків. Водночас особливу небезпеку становлять каскадні ефекти, коли порушення в роботі одного об'єкта критичної інфраструктури призводить до порушень у роботі інших об'єктів і систем унаслідок їх взаємозалежності («ефект доміно») [1]. До критичної інфраструктури належать й особливо небезпечні виробництва, аварії на яких викликані будь-якими причинами (природними або техногенними надзвичайними ситуаціями,

зловмисними чи необережними діями), також можуть обернутися катастрофічними для певних територій і їх населення наслідками.

Науковці стверджують, що вперше на національному рівні про критичну інфраструктуру мовили у 80-х роках XX століття в США, коли Національна Дослідницька Рада (National Research Council) визначила інфраструктуру як сукупність взаємопов'язаних елементів, що підтримують цілісність усієї структури і насамперед включила до неї автомагістралі, дороги, мости, мережі громадського транспорту, аеропорти, доставку води та водні джерела, поводження із стічними водами й небезпечними відходами, виробництво і передачу електроенергії та телекомунікації [2, с. 22–23].

Термін «критична інфраструктура» ввійшов до обігу ділового, наукового та дипломатичного спілкування із середини 1990-х рр. і спершу був пов'язаний з інформаційною інфраструктурою [3, с. 151]. Критично важливі об'єкти інфраструктури діють як система життєзабезпечення повсякденного існування людей. Співтовариства людей підтримуються доволі комплексною і складною мережею інфраструктурних систем. Громадяни очікують і покладаються на функціонування в своїх країнах установ і служб для захисту свого здоров'я, фізичної безпеки, охорони й економічного благополуччя. Виведення з ладу, серйозні збої і навіть дрібні, але постійні недоліки в роботі та функціонуванні певної інфраструктури чи її елементів можуть створювати загрозливі, а іноді й критичні для нормальної життєдіяльності ситуації.

Тому в більшості зарубіжних країн із метою систематизації потенційно небезпечних об'єктів введено до обігу термін «критична інфраструктура». Необхідно зазначити, що цілісна концепція критичної інфраструктури вперше була сформована та розроблена у США і саме цю країну вважають піонером у розробленні й запровадженні концепції критичної інфраструктури та її захисту, оскільки саме тут у 1996 р. уперше дано визначення терміна «критична інфраструктура», до якого вносилися зміни й він набув сучасного розуміння [3, с. 4]. Після серії горезвісних терористичних актів у вересні 2001 р. уряд цієї країни кардинально переглянув не тільки своє уявлення про систему безпеки держави і суспільства за нових геополітичних умов, а й вніс зміни в національне законодавство, структуру уряду, державний бюджет, визначення пріоритетів основних напрямів внутрішньої і зовнішньої політики. В США критична інфраструктура визначається як сукупність фізичних або віртуальних систем і засобів, важливих для держави такою мірою, що їх вихід із ладу або знищення можуть призвести до згубних наслідків у галузі оборони, економіки, охорони здоров'я та безпеки нації [4]. Отже, це треба розуміти так, що знищення, руйнування чи в інший спосіб виведення з ладу об'єктів критичної інфраструктури, зокрема і в результаті вчинення злочинів на них, створює загрозу національній безпеці.

## 2. Нормативне забезпечення функціонування об'єктів критичної інфраструктури

У 2002 р. в США був прийнятий відповідний документ – Акт щодо інформації з критичної інфраструктури (Critical Infrastructure Information Act («США») [5], в якому регулювалися положення стосовно обміну інформацією з питань оцінки вразливості та загроз інфраструктурі, також і пов'язаних із терористичними загрозами. Закон запровадив термін «інформація щодо критичної інфраструктури» і розуміння інформації, яка зазвичай не перебуває в полі зору суспільства та належить до безпеки функціонування критичної інфраструктури чи захищених систем. Цим Актом був визначений урядовий орган – Департамент внутрішньої безпеки, який мав відповідати за збір, аналіз і поширення інформації з метою вжиття необхідних заходів для захисту критичної інфраструктури. Одночасно законом установлювалися вимоги до використання такої інформації (запроваджується режим обмеженого доступу) для недопущення зловживань і захисту суб'єктів господарювання (операторів інфраструктури) від поширення вразливої комерційної інформації [3, с. 153]. Відтоді Сполучені Штати займають лідерські позиції у цій сфері, зокрема завдяки застосуванню апробованих на інших напрямах сучасних управлінських підходів, удосконаленню інформаційно-аналітичної підтримки процесу прийняття рішень, використанню новітніх технологій та активному поширенню різноманітних форм і форматів підготовки кадрів і населення для забезпечення захисту та стійкості критичної інфраструктури. Одним із прикладів цього є створення в 2018 р. у системі Міністерства внутрішньої безпеки США Агентства з питань кібербезпеки та безпеки інфраструктури, що функціонує як оперативна складова, яка на національному рівні керує зусиллями, спрямованими на усвідомлення та управління ризиками, сформованими загрозами критичній інфраструктурі країни [6, с. 4–5, 8].

Нині в більшості розвинених країн широко використовують досвід і напрацювання з питань захисту критичної інфраструктури, які отримали й продовжують отримувати фахівці з США. Проте в Європі термін «критична інфраструктура» вживали дещо раніше, ніж у Сполу-

чених Штатах, а саме наприкінці 1990-х, коли посилилася загроза тероризму. Першою про це заговорила Великобританія, маючи на увазі необхідність захисту системи телекомунікації, банківського та фінансового сектору, водопостачання, енергозбереження та інших важливих для економіки країни об'єктів. Доволі активно і на міждержавному рівні дослідження з безпеки почали проводитись із 2003 р. у рамках програм ЄС «European industrial potential in the field of security research» та «European Security Research Programme (ESRP)». Із 2007 р. у багатьох європейських країнах задля підготовки заходів на випадок війни чи надзвичайних подій розпочалась робота над ініціативою «Research for Secure Europe» (дослідження для безпеки Європи). Поряд із зазначеним з 2004 р. на рівні ЄС та Європейської комісії розпочали створення проєкту захисту критичної інфраструктури «European Programme for Critical Infrastructure Protection» («EPCIP»). У ньому важливу увагу приділено захисту від терористичних загроз. Тоді під критичною інфраструктурою розуміли «обладнання, служби й інформаційні системи, життєво важливі для держави, знищення чи відмова від яких призведе до послаблення суспільства, національного господарства, системи охорони здоров'я, безпеки ефективного функціонування державного устрою». 17 листопада 2005 р. Комісія прийняла «Зелену книгу» із захисту критичної інфраструктури (EPCIP). Її основним завданням було сформувати на політичному та безпосередньо на рівні виконавців загальну позицію та заходи із захисту критичної інфраструктури в країнах-членах ЄС. Насамперед зауважено, що захист критичної інфраструктури кожної країни потребує посилення взаємодії та обміну інформацією щодо загроз на загальноєвропейському рівні та між окремими країнами-учасницями [7, с. 17–18].

Водночас розуміння критичної інфраструктури та її об'єктів у окремих європейських країнах за спільних до їх визначення підходів може дещо різнитись, що зумовлене національними традиціями, розумінням національних цінностей, безпеки країни, добробуту населення тощо. Наприклад, у Німеччині розуміння критичної інфраструктури закладене у Національній стратегії захисту критичної інфраструктури, згідно з якою до критичних віднесено організаційні та фізичні структури й об'єкти, життєво важливі для суспільного та економічного існування нації настільки, що виведення їх з ладу або погіршення функціонування може призвести до тривалих недопоставок, утворення значних прогалин у системі державної безпеки або до інших тяжких наслідків [8]. Інтереси нації і безпека держави, як і в США, є ключовими поняттями для віднесення у ФРН об'єктів до критичної інфраструктури.

У Республіці Польща розуміння критичної інфраструктури наведено у Законі РП від 26 квітня 2007 р. «Про кризове управління», де в статті 3 до критичної інфраструктури віднесено системи та взаємозалежні функціональні об'єкти цих систем, зокрема й будівлі, обладнання, а також ключові для безпеки держави та її громадян послуги, які надаються для забезпечення ефективного функціонування органів державної влади, а також інших установ і підприємств [9]. Ключовим у розумінні таких об'єктів, знову ж таки, є безпека держави Польща та безпека й добробут її громадян. Невдовзі, 30 квітня 2010 р., у Польщі видано Регуляторний акт Ради Міністрів (Уряду) Польщі «Про національну програму захисту критичної інфраструктури», в якому у § 3 відповідальність за розробку критеріїв віднесення об'єктів до системи критичної інфраструктури покладено на Директора Урядового центру з безпеки [10]. Окреме значення для усвідомлення сутності та значення критичної інфраструктури в Польщі має «Стратегія національної безпеки Республіки Польща, 2014 р.». Відповідно до положень п. 86 цієї Стратегії, критична інфраструктура охоплює ключові системи та елементи, що гарантують безпеку держави та її громадян, а також ефективне функціонування органів державного управління, інститутів та бізнесу. Зокрема, зазначено, що надзвичайно важливо забезпечити умови для захисту критичної інфраструктури. Ця інфраструктура охоплює ключові системи й елементи, що забезпечують безпеку держави та її громадян, а також ефективні функціонування органів державного управління, установ та підприємців. За захист критичної інфраструктури відповідають оператори власників, яких підтримує потенціал державного управління. В Польщі впроваджується інноваційний підхід у цій галузі на основі принципів спільної відповідальності зацікавлених сторін, широкі співпраця та взаємна довіра. Дії держави полягають у можливій активізації системи антикризового управління у разі зриву функціонування критичної інфраструктури, а також підвищення обізнаності, знань та компетенції, а також сприяння співпраці у цій галузі [11].

У травні 2020 р. в Республіці Польща прийнято нову «Стратегію національної безпеки Республіки Польща, 2020», де, як і в багатьох інших країнах, враховано нові загрози, пов'язані із пандемією COVID-19. В зв'язку із значущістю своєчасного і правдивого інформування населення про загрози, профілактику, заходи з недопущення захворювань, важливим елементом

польської національної критичної інфраструктури названо окремі об'єкти, якими є комунікаційні системи. Загалом така Стратегія має чотири розділи. Вступ до неї складається з двох підрозділів: безпечне середовище; цінності, національні інтереси та стратегічні цілі в сфері національної безпеки. У Розділі І. Безпека держави і громадян визначено: Управління національною безпекою; Імунітет держави та загальний захист; Збройні сили Республіки Польща; Кібербезпека; Інформаційний простір. Розділ ІІ має назву «Польща в міжнародній системі безпеки». Розділ ІІІ – «Ідентичності і національна спадщина». Розділ ІV – «Соціально-економічний розвиток. Охорона навколишнього середовища», в якому визначено підрозділи, в яких йдеться і про окремі об'єкти критичної інфраструктури, зокрема: здоров'я та захист сім'ї; міграційну політику; економічну безпеку; енергетичну безпеку; збереження природного середовища; науково-технічний потенціал [12].

У Федеративній Республіці Німеччина головним координатором захисту критичної інфраструктури є Федеральне міністерство внутрішніх справ. Також створено інституцію Захисту критичної інфраструктури в Німеччині (Schutz Kritischer Infrastrukturen in Deutschland), яка досліджує уразливість інфраструктури і пропонує стратегії її захисту та політику співробітництва і кооперації громадського управління з приватними суб'єктами.

В 1999 р. у Великобританії створено Координаційний центр з безпеки національної інфраструктури (National Infrastructure Security Coordination Centre NISCC), який входив спершу до Міністерства внутрішніх справ, а згодом до Ради національного центру з безпеки (National Security Advice Centre – NSAC). Із 2007 р. ці організації замінив Центр по захисту національної критичної інфраструктури (National Security Advice Centre – NSAC). Великобританія за прикладом США в захисті критичної інфраструктури орієнтується насамперед на тероризм і порушення кіберпростору [2, с. 39–40].

У Франції за координацію діяльності галузі критичної інфраструктури відповідає прем'єр-міністр, а в організаційній складовій ці функції виконує Генеральний секретар з оборони і національної безпеки (Secrétariat Général de la Défense et de la Sécurité Nationale – SGDSN), який безпосередньо підпорядкований прем'єр-міністру. З погляду правового забезпечення основним документом є закон про захист основних економічних секторів від 2014 р. № 6600/SGDSN/PSE/PSN (Secteurs d'Activités d'Importance Vitale), згідно з яким критичними вважаються всі сектори, що слугують для забезпечення основних соціальних і економічних процесів, зокрема громадське управління, судочинство, збройні сили, сільське господарство, електронні комунікаційні системи, енергетика, космос і дослідна діяльність, вода, промисловість, громадське здоров'я, транспорт.

У Словацькій Республіці до 2011 р. критична інфраструктура розглядалась у межах оборонної інфраструктури, а у 2011 р. видано Закон № 45/2011 «Про критичну інфраструктуру», згідно з яким кураторство над окремими секторами здійснюють відповідні міністерства, а головним органом із захисту критичної інфраструктури є Міністерство внутрішніх справ [2, с. 45–46, 50].

У зазначених країнах створено державні структури або визначено урядових осіб, які відповідають за захист критичної інфраструктури і в разі вчинення злочинів на її об'єктах саме з цими державними інституціями слідчий повинен установлювати взаємодію під час досудового розслідування.

На жаль, у нашій країні досі цьому аспекту проблеми на державному рівні не надано належного значення.

Директивою Європейської комісії № 786 2006 р. до загальноєвропейської критичної інфраструктури віднесено ті об'єкти національної критичної інфраструктури країн-членів ЄС, вплив яких у разі відмови інциденту або зловмисного втручання поширюватиметься і на країну, де такий об'єкт розташований, і на хоча б одну іншу країну-члена ЄС [1]. Іншою Директивою Ради 2008/114/ЄС від 8 грудня 2008 р. про ідентифікацію і визначення Європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту запроваджено процедуру ідентифікації та визначення європейських критичних інфраструктур, а також спільний для країн Європи підхід до оцінки необхідності вдосконалення захисту таких інфраструктур із метою сприяння захисту людей. Під «критичною інфраструктурою» для цілей зазначеної Директиви розуміють 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. «Європейська критична інфраструктура» означає критичну інфраструктуру, розташовану в державах-членах, пошкодження або знищення якої матиме істотний вплив щонайменше на дві держави-члени. Істотність впливу оцінюється за допомогою наскрізних

критеріїв, які охоплюють наслідки міжсекторальних залежностей від інфраструктур інших типів [13].

На відміну від України, а також більшості країн Європи, США, Канади та низки інших держав, є й такі країни, де питання критичної інфраструктури не є на часі, а якщо й мовлять про схожі проблеми, то поняттю критичної інфраструктури та її системі, об'єктам окремої уваги не приділяють. Так, вітчизняні дослідники цієї проблеми вказують на спробу віднайти приклади того, як підходять до питання визначення об'єктів критичної інфраструктури в Грузії. Здійснений ними пошук у відкритих джерелах цієї країни використання термінів «критична інфраструктура» або його синоніму «національна інфраструктура» грузинською, англійською та російською мовами, зокрема у базах даних із національного законодавства, дав нульовий результат. Також немає повідомлень з міжнародних форумів про створення і функціонування в цій країні національної системи захисту критичної інфраструктури. Все це дало науковцям підстави стверджувати, що в Грузії концепцію захисту критичної інфраструктури не запроваджено взагалі, але є система захисту кіберпростору. Наявна у відкритих джерелах інформація стосовно захисту критичної інфраструктури у Республіці Молдова свідчить про аналогічну ситуації, як і в Грузії, а саме – докладаються зусилля лише для кіберзахисту [6, с. 13–14].

**Висновки**

Провівши наукове дослідження зарубіжного досвіду з окремих питань захисту об'єктів критичної інфраструктури, варто зробити такі висновки.

По-перше, захист об'єктів критичної інфраструктури вийшов на загальноєвропейський чи навіть міжконтинентальний формат. Ще 17 лютого 2017 р. Рада Безпеки ООН одноголосно прийняла резолюцію № 2341 про захист критично важливих об'єктів інфраструктури й розширення можливостей держав з попередження нападів на критично важливі об'єкти інфраструктури й закликала держав-членів протистояти небезпеці терористичних атак на критично важливі об'єкти інфраструктури. В глобальній контртерористичній стратегії ООН, у рамках Розділу II «Міри по боротьбі з тероризмом та його попередження», держави-члени вирішили активізувати всі зусилля з підвищення безпеки й захисту особливо вразливих об'єктів, таких як інфраструктура і громадські місця, а також реагування на терористичні напади. Загострення зовнішньополітичного та внутрішньополітичного становища України в сучасних умовах актуалізувало питання розроблення концепції створення державної системи захисту об'єктів критичної інфраструктури.

По-друге, притаманні для України загрози критичній інфраструктурі можуть мати різновекторні спрямування та вияви. Особливу загрозу становить збройний конфлікт і ситуація неоголошеної гібридної війни, що має місце в Україні, та пов'язані із ними загрози деструктивних дій з боку диверсійних груп, учинення терактів, диверсій, шпигунства, кібератак, економічної експансії стосовно об'єктів критичної інфраструктури тощо.

По-третє, необхідність впровадження національної концепції захисту об'єктів критичної інфраструктури є важливою для модернізації системи національної безпеки України. Це дасть змогу ввести термін «об'єкти критичної інфраструктури» у законодавство України, що відповідає загальновизнаним міжнародним підходам.

**Список використаних джерел**


1. Бірюков Д. С. Про доцільність та особливості визначення критичної інфраструктури в Україні. Аналітична записка. 02.01.2013 р. URL: http://www.niss.gov.ua/articles/1026/ (дата звернення: 16.02.2021 р.).
2. Сметана М. Защита критической инфраструктуры: подходы государств Европейского Союза к определению элементов критической инфраструктуры. Острава : Czech Republic Development Cooperation, 2014/15. 60 с.
3. Курбанов Я. Л. Забезпечення природно-техногенної безпеки в Україні і проблема визначення поняття «критична інфраструктура». *Південноукраїнський правничий часопис*. 2016. № 2. С.150–154.
4. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT Act) ACT OF 2001. URL: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW-107publ56.htm (дата звернення: 14.02.2021 р.).
5. Critical Infrastructure Information Act of 2002 («CIIA»). URL: https:// www.fas.org/sgp/crs/RL31762.pdf (дата звернення: 14.02.2021 р.).
6. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналіт. доп. за ред. О. М. Суходолі. Київ : НІСД, 2020. 28 с.

7. Єрменчук О. П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : монографія. Дніпро : ДДУ ВС, 2018. 180 с.
8. National Strategy for Critical Infrastructure Protection (CIP Strategy) (17.06/2009). URL: https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/CIP-Strategy.pdf (дата звернення: 19.01.2021 р.).
9. USTAWA z dnia 26 kwietnia 2007 r. O zarządzaniu kryzysowym. Opracowano na podstawie: Dz.U. z 2007 r. Nr. 89, poz. 590. URL: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20070890590/T/D20070590L.pdf (дата звернення: 16.02.2021 р.).
10. Uchwała nr 121/2018 Rady Ministrów z dnia 7 września 2018 r. zmieniającej uchwałę w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej. URL: https://rcb.gov.pl/wp-content/uploads/Dokument-G%C5%82%C3%B3wny-1.pdf (дата звернення: 16.02.2021 р.).
11. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej / Prezydent Rzeczypospolitej Polskiej Bronisław Komorowski 5 listopada 2014 r., na wniosek Prezesa Rady Ministrów, zatwierdził Strategię Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. URL: https://wzk.poznan.uw.gov.pl/sites/default/files/zalaczniki/sbn_rp_2014.pdf (дата звернення: 16.02.2021 р.).
12. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej została zatwierdzona w dniu 12 maja 2020 roku przez Prezydenta Rzeczypospolitej Polskiej, na wniosek Prezesa Rady Ministrów. URL: https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf (дата звернення: 16.02.2021 р.).
13. Директива Ради 2008/114/ЄС від 8 грудня 2008 р. про ідентифікацію і визначення Європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту. *Офіційний вісник Європейського Союзу*. URL: https://zakon.rada.gov.ua/laws/show/984_002-08#Text (дата звернення: 18.02.2021 р.).

**References**

1. Biriukov, D. S. (2013). Pro dotsilnist ta osoblyvosti vyznachennia krytychnoi infrastruktury v Ukraini [On the expediency and features of determining the critical infrastructure in Ukraine]. *Analitychna zapyska (Analytical note)*. Retrieved from http://www.niss.gov.ua/articles/1026/ [in Ukr.].
2. Smetana, M. (2014). Zashchyta krytycheskoi ynfrastruktury: podkhodi hosudarstv Evropeiskoho Soiuza k opredelenyiu elementov krytycheskoi infrastrukturi [Critical Infrastructure Protection: European Union States' Approaches to Defining Critical Infrastructure Elements]. Ostrava: Czech Republic Development Cooperation [in Russ.].
3. Kurbanov, Ya. L. (2016). Zabezpechennia pryrodno-tekhnohennoi bezpeky v Ukraini i problema vyznachennia poniattia «krytychna infrastruktura» [Ensuring natural and man-made security in Ukraine and the problem of defining the concept of «critical infrastructure»]. *Pivdennoukrainskyi pravnychyi chasopys (South Ukrainian Law Journal)*, 2, 150–154 [in Ukr.].
4. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT Act) ACT OF 2001. Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW-107publ56.htm
5. Critical Infrastructure Information Act of 2002 («CIIA»). URL: https:// www.fas.org/sgp/crs/RL31762.pdf
6. Sukhodoli, O. M. (Ed.) (2020). Derzhavna systema zakhystu krytychnoi infrastruktury v systemi zabezpechennia natsionalnoi bezpeky: analit. dop [State system of critical infrastructure protection in the system of national security: an analytical report]. Kyiv: NISD [in Ukr.].
7. Iermenchuk 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]. Dnipro: DDU VS [in Ukr.].
8. National Strategy for Critical Infrastructure Protection (CIP Strategy) (17.06/2009). Retrieved from https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/CIP-Strategy.pdf.
9. USTAVA z dnia 26 kwietnia 2007 r. O zahządzaniu kryzysovym [ACT of April 26, 2007 on crisis management]. Retrieved from http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20070890590/T/D20070590L.pdf [in Pol].
10. Ukhvala nr 121/2018 Rady Ministrov z dnia 7 whzesnia 2018 r. zmieniającej ukhvalę v spravie prhzyjecia Narodovego Programu Okhrony Infrastruktury Krytychnei [Resolution No. 121/2018 of the Council of Ministers of September 7, 2018 amending the resolution on the adoption of the National Critical Infrastructure Protection Program]. Retrieved from https://rcb.gov.pl/wp-content/uploads/Dokument-G%C5%82%C3%B3wny-1.pdf [in Pol].
11. Strategia Bezpiechenstva Narodovego Rhzechypospolitei Polskiei / Prezydent Rhzechypospolitei Polskiei Bronislav Komorovski 5 listopada 2014 r., na wniosek Prezesa Rady Ministrov, zatwierdził Strategiie Bezpiechenstva Narodovego Rhzechypospolitei Polskiei [National Security Strategy of the Republic of Poland / President of the Republic of Poland Bronislav Komorovski On November 5, 2014, at the request of

the Prime Minister, approved the National Security Strategy of the Republic of Poland]. Retrieved from https://wzk.poznan.uw.gov.pl/sites/default/files/zalaczniki/sbn_rp_2014.pdf [in Pol.].

12. Strategiia Bezpiechenstva Narodovego Rhzechypospolitei Polskiei zostala zatvierdhzona v dniu 12 maja 2020 roku prhzez Prezydenta Rhzechypospolitei Polskiei, na wniosek Prezesa Rady Ministrov [The National Security Strategy of the Republic of Poland was approved on May 12, 2020 by the President of the Republic of Poland, at the request of the Prime Minister]. Retrieved from https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [in Pol.].
13. Dyrektyva Rady 2008/114/IeS vid 8 hrudnia 2008 r. pro identyfikatsiiu i vyznachennia Yevropeiskykh krytychnykh infrastruktur ta otsiniuvannia neobkhidnosti pokrashchennia yikh okhorony ta zakhystu [Council Directive 2008/114 / EU of 8 December 2008 on the identification and identification of European Critical Infrastructure and the assessment of the need to improve their protection and security]. *Ofitsiinyi visnyk Yevropeiskoho Soiuzu (Official Journal of the European Union)*. Retrieved from https://zakon.rada.gov.ua/laws/show/984_002-08#Text [in Pol.].

*Стаття: надійшла до редакції 24.11.2020*
*прийнята до друку 15.03.2021*
*The article: is received 24.11.2020*
*is accepted 15.03.2021*