

ДОСВІД ЗАРУБІЖНИХ КРАЇН У СФЕРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Братель С. Г.

Стаття присвячена дослідженню досвіду зарубіжних країн у сфері забезпечення безпеки об'єктів критичної інфраструктури. Встановлено, що захист об'єктів критичної інфраструктури України є важливою складовою забезпечення національної безпеки та одним із пріоритетних напрямків державної політики в умовах введення воєнного стану.

Для України важливість захисту інфраструктури особливої актуальності набула у 2022 році в умовах воєнного стану, правовий режим якого встановлювався на усій території нашої держави. Безпечне функціонування критичної інфраструктури є важливим чинником забезпечення національної безпеки, сталого функціонування економіки, добробуту та захисту населення країни.

У статті проаналізовано стан захисту критичної інфраструктури в зарубіжних країнах, розвиток державної політики у сфері забезпечення захисту та стійкості критичної інфраструктури. Здійснено огляд низки нормативно-правових актів, що регулюють питання захисту об'єктів критичної інфраструктури в таких зарубіжних країнах, як Сполучені Штати Америки, Сполучено Королівство Велика Британія та Північна Ірландія, Федеративна Республіка Німеччина, Республіка Польща, Французька Республіка. Звернуто увагу, що спільним у досліджуваних країнах є наявність об'єктів, систем, мереж 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.

Досвід провідних країн світу свідчить про те, що в Україні започатковане формування національної системи захисту об'єктів критичної інфраструктури. Запобігання та протидія можливим загрозам критичної інфраструктури потребує імплементацію світового досвіду у сфері системи захисту та підвищення стійкості критичної інфраструктури від військових загроз. За результатами аналізу досвіду низки зарубіжних країн виявлено кореляційні зв'язки між захистом критичної інфраструктури та станом національної безпеки. Зроблено висновки і сформувано пропозиції щодо можливих подальших ефективних кроків за напрямом.

Ключові слова: національна безпека, критична інфраструктура, закон, об'єкт, злочин, правопорушення, війна.

Bratel S. G. Experience of foreign countries in ensuring the safety of critical infrastructure

The article is devoted to the study of the experience of foreign countries in ensuring the safety of critical infrastructure. It is determined that the protection of objects of critical infrastructure of Ukraine is an important component of the infrastructure of society and one of the most important priorities of the State.

For Ukraine, the importance of protecting infrastructure became especially relevant in 2022 under the conditions of martial law, the legal regime of which was established over the entire territory of our state. The importance of the safe functioning of critical infrastructure is a factor in ensuring national security, sustainable functioning of the economy, well-being and protection of the country's population.

The article analyzes the state of protection of critical infrastructure in foreign countries, the development of state policy in the field of protection and stability of critical infrastructure. The normative legal acts regulating the protection of critical infrastructure in such foreign countries as the United States of America, Great Britain, Germany, Poland, France are analyzed. Attention is drawn to the fact that common in the studied countries are objects, systems, networks or their parts, disruption 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 capability and national security.

The experience of the leading countries of the world indicates that Ukraine is at the beginning of the formation of a national system for the protection of critical infrastructure. Preventing and countering possible threats to critical infrastructure requires the adaptation of world experience in the protection system and increasing the stability of critical infrastructure through the prism of military threats. Based on the results of a review of the national experience of a number of foreign countries, the connection between the protection of critical

infrastructure and national security was demonstrated. Conclusions are made and a number of recommendations on possible further steps in this area are proposed.

Key words: national security, critical infrastructure, law, object, crime, offense, war.

Постановка проблеми. Захист критичної інфраструктури є частиною забезпечення національної безпеки України. Застосування відносно України інструментів інформаційної та гібридної війн, фінансово-економічна, інформаційна та геополітична криза постійно присутні у спектрі загроз та небезпек як для національної безпеки України, так і галузевим суспільним відносинам, що охоплюють захист критичної інфраструктури зокрема [16, с. 119].

Збільшення кількості та підвищення складності кібератак, а також пошкодження інфраструктурних об'єктів у регіонах України внаслідок збройної агресії російської федерації зумовили актуалізацію питання захисту систем, об'єктів і ресурсів, які є критично важливими для функціонування суспільства, соціально-економічного розвитку держави та забезпечення національної безпеки [2, 3].

В умовах сучасного надзвичайно інтенсивного розвитку інфраструктури провідних країн світу існує чимало об'єктів критичної інфраструктури, виведення з ладу яких може призвести до надзвичайних ситуацій. Наслідки таких надзвичайних ситуацій здебільшого пов'язані із загибеллю людей, екологічними катастрофами, заподіянням значних матеріальних та економічних збитків.

Проведення військових дій на території України збройними силами країни-агресора не омине об'єкти критичної інфраструктури, що в свою чергу становить потенційну загрозу для безпеки всього світу. Сьогодні в українському науковому середовищі існує чимало кількості досліджень, предметом вивчення яких є різноманітні аспекти захисту, забезпечення безпеки об'єктів критичної інфраструктури, визначення потенційних загроз, а також особливості діяльності спеціальних суб'єктів.

Аналіз останніх досліджень і публікацій. Окремі аспекти правового забезпечення захисту об'єктів критичної інфраструктури України, забезпечення національної безпеки й оборони у своїх дослідженнях висвітлювали такі науковці, як: Авер'янов В.Б., Андрійченко Н.С., Антонюк В.В., Бандурка О.М., Барчук В.Б., Батраченко О.В., Битяк Ю.П., Васьковська В.П., Деркач А.Л., Додін Є.В., Жила С.С., Засулько С.С.,

Ільїна Н.Л., Кісіль З.Р., Кормич Б.А., Кузьменко Ю.В., Левицька М.Б., Мирошниченко М.М., Сокурєнко В.В., Стеценко С.Г., Теленик С.С., Яровий К.В. та ін.

Метою наукової статті є здійснення наукового дослідження досвіду зарубіжних країн у сфері забезпечення безпеки об'єктів критичної інфраструктури.

Виклад основного матеріалу. На сьогодні високий ступінь впровадження новітніх технологій є ознакою рівня розвиненості країни, визначальним чинником її економічної конкурентоспроможності, а, отже, і необхідною умовою для досягнення цілей, які визначаються національними інтересами. В той же час, поряд з багатьма перевагами технологічний прогрес утворює умови безпрецедентної залежності як окремої людини, так і суспільства від систем, що надають інформаційні, комунікаційні, транспортні, енергетичні, фінансові та інші послуги.

Враховуючи сучасні геополітичні реалії наша держава може розглядатися європейськими партнерами як елемент критичної інфраструктури, що має загальноєвропейське значення. Цей аспект, безперечно, заслуговує на увагу при розгляді проблем захисту національної критичної інфраструктури. Для України може бути корисним досвід деяких східноєвропейських країн в імplementації до законодавства концепції захисту критичної інфраструктури [10, 11].

Критична інфраструктура містить значну кількість об'єктів, які прийнято групувати за секторами. Кількість секторів і принцип групування залежно для кожної країни є особливим.

Під час визначення елементів критичної інфраструктури (віднесення об'єктів до критичної інфраструктури) будується ієрархія критеріїв, що охоплює такі основні групи: економічна безпека; безпека життєдіяльності та здоров'я населення; недопущення техногенних аварій регіонального або національного масштабів; державна безпека та оборона; національна самоповага та імідж держави [6, с. 24].

Становлення нормативно-правової бази у сфері захисту критичної інфраструктури є тривалим процесом. Найбільших успіхів вважається у цій сфері досягли Сполучені Штати Америки. Трагічні події 11 вересня 2001 року в місті Нью-Йорк мали величезний поштовх до розбудови у США однієї з найефективніших систем захисту об'єктів критичної інфраструктури в світі.

У першу чергу, прийнято нормативну основу функціонування такої системи - Акт про патріотизм (USA Patriot Act). У положеннях

нормативно-правового акта сутність критичної інфраструктури визначено як комплекс віртуальних і фізичних активів, мереж і систем, які мають життєво важливе значення для країни, руйнування або недієздатність яких, в тому числі й окремих їх елементів, матиме згубні наслідки для національної безпеки, економіки, безпеки та здоров'я населення чи матиме будь-яку комбінацію з перелічених наслідків [12, с. 362].

У 2002 р. в США прийнятий Акт щодо інформації з критичної інфраструктури (Critical Infrastructure Information Act («СІІА»)), яким регулювався обмін інформацією з питань оцінки вразливості та загроз інфраструктурі, також і пов'язаних із терористичними загрозами [5, с. 134]. Закон запровадив термін «інформація щодо критичної інфраструктури» і розуміння інформації, яка зазвичай не перебуває під увагою суспільства та належить до безпеки функціонування критичної інфраструктури чи захищених систем. Цим Актом 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. Відтоді США посіли лідерські позиції у цій сфері, зокрема завдяки застосуванню апробованих на інших напрямках 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 [5, с. 134].

Аналізуючи досвід правового регулювання системи захисту критичної інфраструктури в США, науковець Теленик С.С. зазначає, що вищенаведена директиву свого часу вивчали європейські країни в межах побудови й становлення власних систем захисту об'єктів критичної інфраструктури [15, с. 189].

Досвід США використано провідними країнами світу під час формування власних систем захисту об'єктів критичної інфраструктури. До нього звертаються й на сучасному етапі розвитку аналізованої сфери суспільних відносин. Використання досвіду США у сфері функціонування систем захисту об'єктів критичної інфраструктури є актуальним і для нашої держави.

В окремих європейських країнах поняття критичної інфраструктури та її об'єктів має відмінне значення. Сполучено Королівство Велика Британія та Північна Ірландія (далі - Великобританія) є одним із європейських лідерів у сфері захисту об'єктів критичної інфраструктури. У 1999 р. у Великобританії створений Координаційний центр з безпеки національної інфраструктури, який входив до складу Міністерства внутрішніх справ. Однак, у 2016 році з нього виділився Національний центр кібербезпеки [8, с. 24]. У Великобританії захист критичної інфраструктури спрямований на запобігання тероризму та недопущення порушення кіберпростору.

У законодавстві Великобританії сутність критичної інфраструктури розкривається як найважливіші елементи інфраструктури. До них належать: активи, об'єкти, системи, мережі, процеси та ключові посадові особи, втрата яких може призвести до згубного впливу на доступність, цілісність або надання основних послуг, порушення цілісності яких може призвести до втрати життя або виникнення нещасних випадків з урахуванням значних економічних і соціальних наслідків для національної безпеки, національної оборони або функціонування держави [12, с. 367].

У Великобританії значна увага відводиться питанню визначення секторів критичної інфраструктури, а також встановленню видів небезпек, яким вони можуть бути піддані. Так, структура системи забезпечення безпеки об'єктів критичної інфраструктури країни охоплює тринадцять секторів.

Під час дослідження зарубіжного досвіду забезпечення безпеки об'єктів критичної інфраструктури увагу слід звернути і на досвід Федеративної Республіки Німеччина (далі - Німеччина). До критичної інфраструктури країни відносяться організації та установи. Вони мають надзвичайно важливе значення для держави та суспільства. Поміж них десять секторів критичної інфраструктури за відповідними галузями: енергетична промисловість, водопостачання, харчова промисловість, інформаційні технології та телекомунікації, медичне обслуговування, банківські та фінансові

послуги, логістика, держава та адміністрація, засоби масової інформації, культура та інформаційна інфраструктура [8, с. 51].

Нормативно-правовими актами, які забезпечують критичну інфраструктуру в Німеччині є: Національна стратегія захисту критичної інфраструктури (2009 р.), Стратегія кібербезпеки Німеччини (2016 р.), Закон «Про безпеку інформаційних технологій (2015 р.), UP KRITIS: державно-приватне партнерство із захисту критичних інфраструктур, BSI (2014 р.), Спільна інтернет-платформа BSI та BVK щодо захисту критичної інфраструктури, плани захисту критичної інфраструктури [4, с. 5; 9, с. 11].

Основну участь у захисті критичної інфраструктури покладено на такі установи: Федеральне відомство з інформаційної безпеки, Федеральне відомство з охорони Конституції, Федеральне управління цивільного захисту та ліквідації наслідків стихійних лих, Федеральна кримінальна поліція, Федеральне агентство технічного сприяння.

У Республіці Польща до критичної інфраструктури відносяться елементи, які гарантують безпеку держави та її громадян, ефективно функціонування органів державного управління, інституту бізнесу. Привертає увагу те, що надзвичайно важливим є аспект забезпечення умов для охорони критичної інфраструктури. Нормативно-правовими актами, які регулюють питання захисту критичної інфраструктури є Закон Республіки Польща від 26 квітня 2007 р. «Про кризове управління», Регуляторний акт Ради Міністрів Польщі від 30 квітня 2010 р. «Про національну програму захисту критичної інфраструктури», «Стратегія національної безпеки Республіки Польща» від 21 жовтня 2021 року [4, с. 19]. Саме у «Стратегії національної безпеки Республіки Польща» започатковано основи функціонування системи, яка гарантує швидку та ефективну відповідь на всі види загроз і криз для країни. Необхідність створення такого документа в безпековій сфері та оновлення механізмів національної безпеки зумовлено активною участю держави у системах європейської безпеки, з одного боку, і високим рівнем терористичної загрози у світі - з іншого.

У Французькій Республіці основним документом правового забезпечення критичної інфраструктури є Закон про захист основних економічних секторів, який був прийнятий у 2014 році. Відповідно до цього закону дванадцять секторів, які призначені для забезпечення основних економічних і соціальних процесів: громадське управління; судочинство; збройні сили; сільське

господарство; електронні комунікаційні системи, аудіо- та відеоінформаційні технології; енергетика; космос і дослідницька діяльність; фінансовий сектор; вода; промисловість; громадське здоров'я; транспорт. Термін «критичні» дослівно вживається у значенні «життєво важливі» (фр., importance vitale) [7, с. 9]. Об'єкти критичної інфраструктури - установи, виробництво та споруди, які надають товари та послуги, незамінні для функціонування суспільства.

Висновки. Результати аналізу досвіду провідних країн світу свідчить про те, що Україна знаходиться на початку формування національної системи захисту об'єктів критичної інфраструктури. Запобігання та протидія можливим загрозам критичної інфраструктури потребують адаптації світової практики у сфері системи захисту та підвищення стійкості критичної інфраструктури крізь призму військових загроз, враховуючи, що з 24 лютого 2022 року на усій території України оголошено воєнний стан.

Особлива увага у сфері забезпечення безпеки критичної інфраструктури має бути спрямована на: по-перше, приведення нормативно-правових актів, які регулюють суспільні відносини у сфері захисту критичної інфраструктури, у відповідність до вимог сьогодення (кібератаки, масові заворушення, воєнні дії, епідемії); по-друге, впровадження національної системи стійкості; по-третє, створення головного органу, відповідального за захист об'єктів критичної інфраструктури на загальнодержавному рівні; по-четверте, налагодження взаємодії партнерства держави, органів місцевого самоврядування, громадських об'єднань, приватного бізнесу та міжнародних партнерів з питань забезпечення національної стійкості у сфері захисту об'єктів критичної інфраструктури; по-п'яте, проведення міжвідомчих навчань та тренувань за участю населення з метою підвищення рівня обізнаності та готовності до реагування на загрози об'єктам критичної інфраструктури; по-шосте, впровадження концепції захисту критичної інфраструктури з метою зміцнення національної безпеки нашої держави.

Література

1. Про критичну інфраструктуру : Закон України від 16 лист. 2021 р. № 1882-IX. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text> (дата звернення: 10.08.2023).
2. Стратегія громадської безпеки та цивільного захисту України : затверджено Указом президента України від 29.06.2021. Портал МВС : веб-сайт.

URL: <https://mvs.gov.ua/uk/ministry/normativna-baza-mvs/proekti-normativnix-aktiv/strategiya-gromadskoyi-bezpeki-ta-civilnogo-zaxistu-ukrayini-zatverdzeno-vid-29062021> (дата звернення: 10.08.2023).

3. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : розпорядження КМУ від 6 груд. 2017 р. № 1009-р. URL: <https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text> (дата звернення: 10.08.2023).

4. Бірюков Д. С. Про доцільність та особливості визначення критичної інфраструктури в Україні. Аналітична записка. 02.01.2013 р. *Національний інститут стратегічних досліджень* : веб-сайт. URL: <https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/pro-docilnist-ta-osoblivosti-viznachennya-kritichnoi> (дата звернення: 10.08.2023 р.).

5. Гора І.В., Батюк О.В. Окремі питання захисту об'єктів критичної інфраструктури: зарубіжний досвід. *Соціально-правові студії*. 2021. Вип. 1 (11). С. 132-139.

6. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки : аналітична доповідь / Кондратов С.І., Сухолодя О.М. Київ, 2020. URL: https://niss.gov.ua/sites/default/files/2020-08/dopovid-systema-zahystu-krytychnoyi-infrastruktury_0.pdf (дата звернення: 10.08.2023).

7. Європейський досвід розбудови системи захисту критичної інфраструктури: уроки для України. Аналітична записка. *Національний інститут стратегічних досліджень* : веб-сайт. URL: <https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/evropeyskiy-dosvid-rozbudovi-sistemi-zakhistu-kritichnoi> (дата звернення: 10.08.2023).

8. 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.

9. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні : аналітична доповідь / Бірюков Д.С., Кондратов С.І. Київ: НІДС, 2012. 57 с. URL: <https://niss.gov.ua/sites/default/>

files/2012-09/zah_ynfrastr-b98c0.pdf (дата звернення: 10.08.2023).

10. Зелена книга з питань захисту критичної інфраструктури в Україні. Київ, 2014. 31 с. URL: https://niss.gov.ua/sites/default/files/2014-11/1125_zelknuga.pdf (дата звернення: 10.08.2023).

11. Ігор Клименко: Чітка координація дій між відомствами - наше головне завдання на фоні існуючих загроз. *Портал МВС* : веб-сайт. URL: <https://mvs.gov.ua/news/igor-klimenko-citka-koordinaciia-dii-miz-vidomstvami-nase-golovne-zavdannia-na-foni-isnu-yuchih-zagrozh> (дата звернення: 10.08.2023).

12. Крикун В.В. Адміністративно-правовий механізм захисту об'єктів критичної інфраструктури в Україні : дис....д-ра юрид. наук : 12.00.07 / Харківський національний університет внутрішніх справ. Харків, 2021, 453 с.

13. Кузьменко Ю.В., Бондар В.В. Захист об'єктів критичної інфраструктури: адміністративно-правове забезпечення. *Юридичний бюлетень*. 2021, № 21. С. 67-72.

14. Кузьменко Ю.В., Коропатов О.М., Думанський Р.В. Адміністративно-правове забезпечення захисту об'єктів критичної інфраструктури України під час воєнного стану. *Юридичний бюлетень*. 2022, № 27. С. 59-65.

15. Теленик С. Критична інфраструктура як об'єкт адміністративно-правового регулювання. *Юридичний часопис Національної академії внутрішніх справ*. 2018. № 1 (15). С. 179-189.

16. Теленик С.С. Адміністративно-правове регулювання державної системи захисту критичної інфраструктури України : дис. ... д-ра юрид. наук : 12.00.07 / Запорізький національний університет міністерства освіти і науки України. Запоріжжя, 2021, 467 с.

Братель С. Г.,
кандидат юридичних наук, професор,
перший проректор
Одеського державного університету
внутрішніх справ