

УДК 349 :323 : 355/359

Єрменчук О.П.кандидат юридичних наук
(Служба безпеки України)

НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ДІЯЛЬНОСТІ У СФЕРІ ЗАХИСТУ НАЦІОНАЛЬНОЇ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: АНАЛІЗ ТА УЗАГАЛЬНЕННЯ НОРМОТВОРЧОЇ ПРАКТИКИ США

Розглянуто особливості законодавчого регулювання діяльності у сфері захисту критичної інфраструктури США. Здійснено аналіз „Патріотичного акта США” від 2001 року та Закону США „Про захист критичної інфраструктури” від 2001 року. Запропоновано принципи побудови та підходи до вдосконалення законодавства України з питань захисту критичної інфраструктури.

***Ключові слова:** національна безпека і оборона, інфраструктура, національна критична інфраструктура, захист критичної інфраструктури, законодавство, закон.*

Yermenchuk O.P. Normative legal regulation of activity in the protection of national critical infrastructure: analysis and coordination of US normative practice. The article considers the peculiarities of legislative activities regulation in the sphere of critical infrastructure protection in the USA. An analysis of the „US Patriot Act of 2001” and the „US Critical Protection Infrastructure Act of 2001” has been conducted. The principles of construction and approach to improving the legislation of Ukraine on critical infrastructure protection are proposed.

***Keywords:** national security and defense, infrastructure, national critical infrastructure, protection of critical infrastructure, legislation, law.*

Постановка проблеми. Наукова проблема забезпечення захисту національної критичної інфраструктури (далі – КІ) України набуває все більшої актуальності, особливо в умовах посилення зовнішніх та внутрішніх загроз національній безпеці, неухильного зростання загроз від кібератак на різні об'єкти інфраструктури держави [1–3]. Якщо у країнах НАТО та ЄС вже створено та функціонує правову базу та систему нормативних документів і розроблено понятійно-категоріальний апарат, що дозволяє запровадити системне регулювання діяльності у сфері захисту КІ, то в Україні практично відсутня відповідна нормативно-правова база з регулювання діяльності у цій сфері [4; 5].

Саме тому рішенням Ради національної безпеки і оборони України від 29 грудня 2016 року „Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури”, уведеним в дію Указом Президента України від 16 січня 2017 року № 8/2017, визначено завдання щодо комплексного вдосконалення правової основи захисту КІ та системи державного управління її безпекою.

Важливим для вирішення такої науково-практичної проблеми може бути аналіз та узагальнення практичного досвіду нормативно-правового регулювання діяльності у сфері захисту КІ провідних країн світу, особливо досвіду США, встановлення та обґрунтування принципів такого регулювання, суб'єктів та об'єктів діяльності у цій сфері, їх повноважень та відповідальності. Такий аналіз може бути корисним для формування підходів та першочергових заходів з формування вітчизняного законодавства у цій сфері.

Деякі окремі питання державного регулювання діяльності у сфері захисту КІ вже розглядалися у роботах вітчизняних фахівців [6; 7]. В даній роботі пропонуємо більш детально зупинитися на аналізі особливостей апробованих на практиці механізмів законодавчого регулювання діяльності у сфері захисту КІ США на прикладі основних законів США.

Виклад основного матеріалу. Регулювання діяльності у сфері захисту КІ США на законодавчому рівні було викладено у так званому «Патріотичному акті» США у 2001 році (далі – Акт), який має назву «Про об'єднання і зміцнення Америки шляхом надання відповідних інструментів, потрібних для виявлення та попередження терористичної діяльності» [8]. Саме в цьому Акті вперше з'явилося поняття «критична інфраструктура» та юридичні норми з її захисту (Sec. 1016. Critical infrastructures protection).

Структуру „Патріотичного акта” схематично наведено на рис. 1.

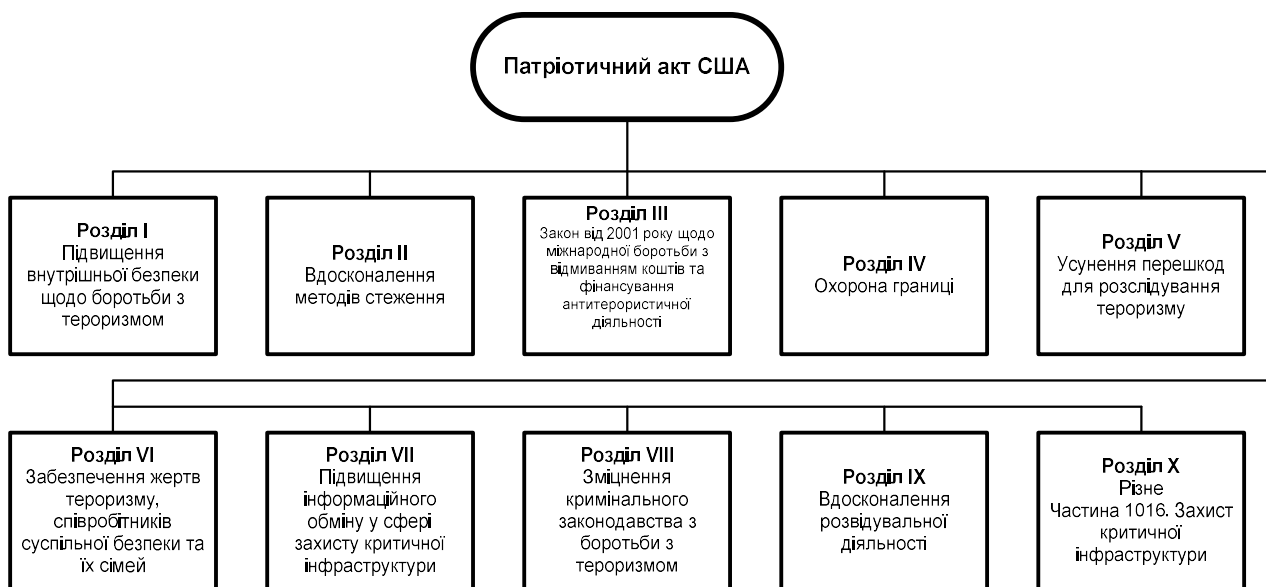


Рис. 1. Структура «Патріотичного акта», США

Першою особливістю цього Акта є те, що ним вносяться усі необхідні зміни та доповнення до інших законів США, що дозволяє побудувати цілісну систему законодавчого регулювання у цій сфері.

Далі слід звернути увагу на те, що в Акті на перші місця по необхідності виносяться заходи з підвищення внутрішньої безпекової ситуації, заходи з

удосконалення наявних форм і методів роботи відповідних органів. Також знайшли відображення такі аспекти діяльності, як посилення фільтраційних заходів на кордоні, розвідувальна діяльність, інформаційний обмін з питань захисту КІ та методи стеження, які мають важливе значення для забезпечення захисту КІ. Частиною 105 Акта («Ініціатива з розширення національних сил з попередження електронних злочинів») визначено «електронні злочини», якими можуть бути потенційні терористичні атаки на КІ.

Питання захисту КІ розглянуто у частині 1016 Акта, яка виділена в окремий закон – Закон «Про захист критичної інфраструктури» («Critical Infrastructures Protection Act of 2001» (далі – Закон).

У преамбулі до Закону визначено, що існують інфраструктури, які пов'язані із забезпеченням оборони та національної безпеки США. Серед них виділяються взаємозалежні *мережі критичних фізичної й інформаційної (або кібер-) інфраструктур*, включаючи сектори (галузі) телекомунікації, енергетики, фінансових послуг, водопостачання і транспорту, від яких все більше залежить діяльність приватного бізнесу, держави і національна безпека. Законом також дано визначення поняття КІ, а саме:

«Критична інфраструктура – це системи і активи, будь то фізичні або віртуальні, настільки життєво важливі для Сполучених Штатів, що неієздатність або руйнування таких систем і активів матиме катастрофічні наслідки для безпеки, захисту національної економіки, національного суспільного здоров'я або охорони здоров'я або для будь-якої комбінації з них».

З цього випливає, що критична інфраструктура формується на базі *існуючих інфраструктур держави* шляхом *виділення в них життєво важливих для держави систем і активів*. Поняття «життєва важливість» за своїми ознаками, по суті, еквівалентна поняттю «життєво важливі цінності» або «національні інтереси», які, наприклад, визначено у статті 1 Закону України «Про основи національної безпеки України». Цим самим можна стверджувати, що при формуванні національного законодавства у сфері захисту КІ його положення слід віднести до питань національної безпеки, а враховуючи сучасний внутрішньополітичний стан в Україні – й до питань її оборони.

В Законі також передбачено, що в США запроваджуються на постійній основі заходи із забезпечення функціонування КІ для підтримки національної оборони, функціонування влади, розвитку економіки та якості життя у США. Реалізація таких заходів повинна здійснюватися шляхом широкого запровадження методів моделювання та аналізу можливостей для оцінки механізмів забезпечення стійкості таких складних і взаємопов'язаних систем, а також розробки стратегічних рекомендацій для досягнення постійної стійкості та надійного захисту КІ.

Законом встановлено, що основна мета Стратегії США у сфері захисту КІ є досягнення того, щоб будь-які фізичні або віртуальні руйнування або порушення функціонування КІ траплялися рідше, були короткочасними, з обмеженими географічними ефектами, керованими, з мінімальним збитком для економіки, соціальних і державних послуг та національної безпеки, тобто

усі заходи спрямовані на підвищення "стійкості критичної інфраструктури". Така мета повинна бути досягнута шляхом встановлення державно-приватного партнерства із залученням корпоративних та недержавних організацій та постійної реалізації комплексної і ефективної програми діяльності уряду у цій сфері.

Важливе місце у Законі відведено розподілу юридичних повноважень у сфері захисту КІ. Так, Законом передбачено заснування Центру моделювання та аналізу національної інфраструктури (National Infrastructure Simulation and Analysis Center – NISAC), який має повноваження здійснювати діяльність у сфері захисту та забезпечення цілісності КІ для підтримки контртерористичної діяльності, оцінки загроз КІ та зниження ризиків. До повноважень Центру належать такі:

а) моделювання, імітація і аналіз систем, що входять до складу критичних інфраструктур, включаючи кібер-інфраструктуру, телекомунікаційну і фізичну інфраструктури, з метою підвищення розуміння масштабної складності таких систем і полегшення видозміни таких систем для нівелювання загроз для таких систем і критичних інфраструктур у цілому;

б) отримання від органів влади штатів, місцевих органів влади і приватного сектора даних, необхідних для створення і підтримки моделей таких систем і критичних інфраструктур у цілому;

в) використання моделювання, імітації і аналізу відповідно до пункту а) для забезпечення тренувань і підготовку вищих посадових осіб з питань, що стосуються:

- питань моделювання, імітації і аналізу відповідно до пункту а);
- наслідків випадкових або неумисних пошкоджень КІ;
- реагування на інциденти або кризи, що зачіпають КІ, включаючи функціонування органів влади і приватного сектора, в ході і після таких інцидентів і криз;

г) використання моделювання, імітації і аналізу відповідно до підпункту а) для підготовки рекомендацій для вищих посадових осіб і персоналу, а також підприємств міністерств і відомств федерального уряду і приватного сектора за їх проханням щодо заходів з підвищення стійкості і обертання критичних інфраструктур.

Фінансування Центру моделювання та аналізу національної інфраструктури здійснюється з державного бюджету США.

Моделювання, імітація і аналіз систем, що входять до складу критичних інфраструктур, повинно здійснюватися відповідними органами влади штатів та місцевими органами влади, які відповідають за реалізацію стратегії у сфері захисту КІ.

Окрім того, згаданою вище частиною 105 Акта встановлено обов'язки директора Секретної служби США з розширення національної мережі оперативних груп боротьби з електронними злочинами з метою виявлення та розслідування різних форм електронних злочинів, у тому числі потенційних терористичних атак на КІ.

З огляду на викладене вище, вважається за доцільне виділити такі принципи побудови структури проекту Закону України щодо захисту КІ:

1. Системність. Такий принцип дозволяє одночасно внести зміни та доповнення до чинного законодавства, зокрема до усіх необхідних розділів законодавства, що стосуються регулювання діяльності у сфері захисту КІ.

2. Повнота понятійно-категорійного апарату. Такий принцип дає можливість однозначного тлумачення основних термінів у сфері захисту КІ та забезпечити їх ув'язку з термінами та визначеннями, які наявні у чинному законодавстві.

3. Розподіл повноважень та взаємодія суб'єктів діяльності.

4. Визначення системи державного управління.

5. Визначення відповідальності.

6. Програмно-цільове планування захисту КІ.

З урахуванням відпрацьованого досвіду нормотворчої діяльності США у цій сфері вбачається, що проект закону України повинен бути, так би мовити, «вбудованим» у чинне законодавство з максимальною адаптацією до нього. Таким проектом може бути, наприклад, проект Закону України «Про внесення змін та доповнень до законів України щодо захисту критичної інфраструктури України».

Основні розділи законодавства України, в які повинно бути внесено відповідні зміни:

- законодавство у сфері забезпечення національної безпеки і оборони;
- законодавство щодо внутрішньої та зовнішньої політики;
- законодавство про надзвичайний стан;
- законодавство про контррозвідувальну діяльність та розвідувальні органи, оперативно-розшукову діяльність;
- законодавство про боротьбу з тероризмом та кіберзлочинністю;
- законодавство про державно-приватне партнерство;
- законодавство у сфері планування, зокрема, оборонного планування;
- кримінальне законодавство.

Висновки. З викладеного вище слід акцентувати увагу, що національна безпека, як захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, повинна включати й надійне функціонування національної КІ. Критична інфраструктура держави може бути визначена як сукупність особливо важливих (стратегічних) матеріальних та нематеріальних об'єктів національної інфраструктури, які забезпечують її стале функціонування, руйнація або пошкодження яких може призвести до людських жертв і значних матеріальних збитків з найсерйознішими негативними наслідками для життєдіяльності суспільства, соціально-економічного розвитку країни, забезпечення суверенітету і територіальної цілісності держави.

Бібліографічні посилання

1. Зелена книга з питань захисту критичної інфраструктури України : зб. матер. між нар. експерт. нарад. – Національний інститут стратегічних досліджень. – К., 2016 [Електронний ресурс]. – Режим доступу: <http://www.niss.gov.ua/articles/2213/>

2. Бірюков Д. С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні / Д. С. Бірюков, С.І. Кондратов. – К. : НІСД, 2012. – 96 с. [Електронний ресурс]. – Режим доступу: <http://www.niss.gov.ua>
3. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матер. міжнарод. експерт. нарад / упоряд. Д. С. Бірюков, С.І. Кондратов ; за заг. ред. О. М. Суходолі. – К. : НІСД, 2015. – 176 с. [Електронний ресурс]. – Режим доступу: [Suxodolya_ost.pdf](http://www.niss.gov.ua)
4. Work Programme 2011, Cooperation, Theme 10, Security (European Commission C(2010)4900 of 19 July 2010) [Електронний ресурс]. – Режим доступу: http://ec.europa.eu/research/participants/data/ref/fp7/89287/k-wp-201101_en.pdf
5. Study: Stock-taking of existing critical infrastructure protection activities. – Final report JLS/2007/D1/037 [Електронний ресурс]. – Режим доступу: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/2009_cip_stock_taking_en.pdf
6. Скурський П.П. Організація захисту критичної інфраструктури вітчизняного оборонно-промислового комплексу з використанням досвіду США / П. П. Скурський, О. П. Єрменчук // Інформаційна безпека людини, суспільства, держави. – № 3(7). – 2011. – С. 54–63.
7. Суходоля О. М. Захист енергетичної інфраструктури: аналіз зарубіжного законодавства. Аналітична записка / О.М. Суходоля // Національний інститут стратегічних досліджень [Електронний ресурс]. – Режим доступу: <http://www.niss.gov.ua/articles/1600/>.
8. PUBLIC LAW 107–56—ОСТ. 26, 2001 [Електронний ресурс]. – Режим доступу: [PLAW-107publ56.pdf](http://www.gpo.gov/plaw-107publ56.pdf).

Надійшла до редакції 30.10.2017

УДК 347.994.1

Нестерцова-Собакарь О.В.

кандидат юридичних наук, доцент

Свистак Ю.В.

студентка

*(Дніпропетровський державний
університет внутрішніх справ)*

ПРАВОВЕ РЕГУЛЮВАННЯ ІНСТИТУТУ НАКАЗНОГО ПРОВАДЖЕННЯ: ЗАРУБІЖНИЙ ДОСВІД ТА ВІТЧИЗНЯНІ ОСОБЛИВОСТІ

Проаналізовано зарубіжний досвід правового регулювання спрощених процедур судочинства. З'ясовано позитивну практику регулювання наказного провадження як невід'ємної складової цивільного процесу. Окреслено перспективи запозичення позитивних надбань зарубіжної практики для подальшого використання її в українських реаліях сьогодні.

Ключові слова: *зарубіжний досвід, правове регулювання, наказне провадження, цивільне судочинство, цивільний процес, позов, Європейський Союз, електронне провадження.*