

НОРМАТИВНО-ПРАВОВЕ ВРЕГУЛЮВАННЯ ПРОЦЕДУРИ РОЗПІЗНАВАННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЯК ЗАПОРУКА ОРГАНІЗАЦІЇ ЇХ ЕФЕКТИВНОГО ЗАХИСТУ



О. П. Єрменчук
кандидат юридичних наук,
доцент Дніпропетровського державного
університету внутрішніх справ МВС України

Постановка проблеми. Захист критичної інфраструктури (далі – КІ) 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 [1].

Дослідження проблематики захисту критичної інфраструктури, зменшення ризиків, мінімі-

зації наслідків (англ. to mitigate – пом'якшити, зменшити, послабити, нейтралізувати) від впливу загроз, стійкості (англ. resilience), як здатності відновлюватися або легко адаптуватися до небезпеки або зміни, розпочали досить активно вивчати в США та Європі ще з початку 1990-х років [2].

При цьому у працях більшості науковців різних країн та у нормативних актах, як правило, розглядають захист критичної інфраструктури, починаючи з внесення об'єкта до переліку критичних.

Сам подальший алгоритм дій може різнитись.

На шляху побудови системи захисту критичної інфраструктури в Україні наразі також надзвичайно важливо визначити сутність і зміст, алгоритм дій та здійснити нормативно-правове врегулювання початкового етапу захисту об'єктів критичної інфраструктури.

Стан дослідження. Деякі питання, пов'язані з захистом об'єктів критичної інфраструктури, були порушені в наукових працях українських вчених Бірюкова Д. С., Бреж-

нева Є. В., Бобро Д. Г., Величка О. Ф., Дубова Д. В., Горбуліна В. П., Іванюти С. П., Зубарева В. В., Конач В. К., Кондратова С. І., Мірошника М. В., Насвіт О. І., Ожевана М. А., Панченко В. М., Петрова В. В., Рижов І. М., Скурського П. П., Суходолі О. М., Щербини В. М., Юрченка О. М. Однак сучасний стан нормативно-правового регулювання процедури розпізнавання об'єктів критичної інфраструктури, як важливого та незамінного елементу, потребує наукового дослідження. Якісне врегулювання зазначеної наукової проблеми стане запорукою організації ефективного та системного захисту об'єктів КІ.

Зазначені обставини обумовлюють актуальність дослідження та стали основою для наших наукових пошуків та підготовки цих матеріалів.

Мета статті. Наразі існує потреба у побудові на національному рівні належної та ефективної системи захисту критичної інфраструктури з використанням вітчизняного досвіду державотворчих процесів і кращих прикладів відповідних іноземних підходів. Існує обґрунтована необхідність у застосуванні системного підходу для побудови на загальнодержавному рівні та інтегрованого залучення зацікавлених гравців, в тому числі місцевого і об'єктового масштабів до управління та захисту об'єктів критичної інфраструктури, забезпечення їх стійкості та безпеки. Нових імпульсів та поглядів вимагає наукова проблема організації спільних заходів задіяних учасників до аналізу компонентів об'єктів національної інфраструктури та виокремлення з їх числа критичних.

Зазначена тема потребує якісного й детального наукового дослідження, оскільки без її глибокого розуміння розпочати ефективний захист критичної інфраструктури в Україні буде вкрай складно.

Основний матеріал. Основною метою діяльності із організації захисту об'єктів КІ в Україні має бути забезпечення безперервного та стійкого функціонування таких об'єктів, запобігання проявам актів несанкціонованого втручання, прогнозування та запобігання кризовим ситуаціям з негативним впливом на об'єкти критичної інфраструктури, а також удосконалення захисту та підвищення його рівня, підняття ефективності заходів безпеки і стійкості цих об'єктів від існуючих загроз.

Забезпечити належний позитивний сценарій їх функціонування можна за умови розробки та впровадження відповідних заходів державної політики та розробки регулятивних норм, що охоплюватимуть ключові аспекти механізму їх захисту на загальнодержавному, регіональному, галузевому, місцевому та об'єктовому рівнях.

Відповідно до вимог Концепції розвитку сектору безпеки і оборони України серед задач державного апарату визначено створення ефективної системи реагування на кризові ситуації, своєчасне виявлення, запобігання та нейтралізацію зовнішніх і внутрішніх загроз національній безпеці, гарантування особистої безпеки, конституційних прав і свобод людини і громадянина, забезпечення кібербезпеки, оперативне спільне реагування на кризові та надзвичайні ситуації. Серед пріоритетних заходів також передбачено проведення контрольно-розвідувального захисту об'єктів КІ, що мають стратегічне значення, та критичної інформаційної інфраструктури, здійснення тестування готовності захисту об'єктів критичної інформаційної інфраструктури до можливих кібератак та кіберінцидентів [3].

Стратегія національної безпеки України від 6 травня 2015 р. та Концепція створення державної системи захисту критичної інфраструктури від 10 січня 2018 р.

передбачають необхідність комплексного реформування системи забезпечення національної безпеки та створення ефективного сектору безпеки і оборони України, а також проведення якісно нової державної політики, спрямованої на ефективний захист національних інтересів та забезпечення функціонування системи захисту КІ [4; 5].

В Указі Президента України № 8/2017 також визначена загальна задача уповноваженим органам розробити і схвалити Концепцію створення державної системи захисту критичної інфраструктури та план заходів з її реалізації, а Службі безпеки України поставлено завдання з удосконалення контрольно-розвідувального забезпечення та захисту критичної інфраструктури [6].

Водночас, окрім вищезазначених концептуальних та стратегічних задач, слід констатувати про відсутність на законодавчому та підзаконному рівні розробленої процедури захисту об'єктів критичної інфраструктури.

Саме такий стан формування нормативно-правової бази вимагає наукового аналізу та пропозицій щодо змісту та алгоритму дій кожного і спільних заходів задіяних учасників з державного та приватного сектору.

При цьому, якщо стосовно процедури паспортизації об'єктів КІ (далі – паспортизація) хоча б на науковому рівні започатковані обговорення, в тому числі за ініціатииви представників Національного інституту стратегічних досліджень, відбулися круглі столи із залученням учасників з різних відомств, то не менш важливий етап, що передуює паспортизації, а саме «розпізнавання об'єктів критичної інфраструктури» (авторська назва, далі – розпізнавання), тобто відбір таких об'єктів для формування переліків об'єктів критичної інфраструктури, наразі залишається не дослідженим [7].

Метою проведення паспортизації є вжиття планових упреждувальних заходів з захисту об'єкта. Її доцільно здійснювати відповідно до переліків об'єктів КІ, які складаються на підставі результатів розпізнавання.

На нашу думку, розпізнавання об'єктів критичної інфраструктури доцільно проводити за участі представників оператора КІ та територіального уповноваженого державного органу у сфері захисту критичної інфраструктури, а у разі його створення не на базі СБ України – також представниками СБ України.

За результатами розпізнавання об'єкти національної інфраструктури можуть бути віднесені до критичної.

Суть розпізнавання об'єктів критичної інфраструктури полягає у виявленні на об'єктах національної інфраструктури джерел та чинників небезпеки, у разі можливого впливу на них загроз, визначенні ризиків настання негативних наслідків, а також оцінці максимального рівня можливих негативних наслідків від ураження об'єкта КІ (наслідків).

Розпізнавання об'єктів критичної інфраструктури має здійснюватися за територіальним та галузевим принципом на підставі письмового звернення суб'єктів ініціювання процесу розпізнавання до територіального уповноваженого державного органу у сфері захисту критичної інфраструктури та СБ України з обов'язковим повідомленням об'єктів національної інфраструктури, які підлягають розпізнаванню.

Вважається, що суб'єктами ініціювання процесу розпізнавання можуть бути: власники та керівники конкретного об'єкта національної інфраструктури, уповноважені державні органи у сфері захисту критичної інфраструктури, органи СБ України, відповідні центральні та місцеві

органи виконавчої влади, органи місцевого самоврядування.

Підставою для проведення розпізнавання доцільно передбачити письмове звернення уповноважених органів у сфері захисту критичної інфраструктури до конкретного об'єкта національної інфраструктури.

Відповідальність за проведення розпізнавання у визначені терміни (тридцятиденний термін після отримання письмового звернення) за аналогією до європейської практики та подібно з діючим в нашій державі порядком обліку потенційно небезпечних об'єктів доцільно покласти на керівників об'єктів критичної інфраструктури.

Центральні та місцеві органи виконавчої влади, органи місцевого самоврядування, територіальні уповноважені державні органи у сфері захисту критичної інфраструктури зобов'язані сприяти відповідальним особам об'єктів національної інфраструктури в організації і проведенні розпізнавання у повному обсязі та контролювати додержання установлених вимог.

Об'єкт розпізнається як об'єкт критичної інфраструктури за наявності достатнього ризику настання негативного наслідку від можливого ураження такого об'єкта.

Шкала оцінювання ризику при розпізнаванні об'єктів критичної інфраструктури має містити градацію на «високий – середній – низький – вкрай низький».

Згідно з нашою позицією, результати розпізнавання об'єкта КІ мають консолідуватись у формі Акта розпізнавання об'єкта критичної інфраструктури, який підписує керівник об'єкта критичної інфраструктури та представники задіяних учасників. Такий Акт узгоджується з відповідним місцевим уповноваженим державним органом у сфері захисту критичної інфраструктури.

Примірники Акта розпізнавання доцільно зберігати на підпри-

ємстві та в уповноваженого державного органу у сфері захисту критичної інфраструктури. Кількість уповноважених суб'єктів зберігання може бути розширена в ході створення відповідного розпорядчого документа Кабінету Міністрів України.

Місцеві уповноважені державні органи у сфері захисту КІ щороку уточнюють переліки об'єктів, що підлягають розпізнаванню, та подають їх до відповідного територіального уповноваженого державного органу у сфері захисту КІ. Галузеві переліки об'єктів критичної інфраструктури складають відповідні центральні органи виконавчої влади. В подальшому Національний перелік об'єктів критичної інфраструктури доцільно затверджувати на рівні Кабінету Міністрів України за поданням Державного органу у сфері захисту критичної інфраструктури. У такий спосіб засвідчується важливість зазначеного переліку та його вагомості значення для інтересів держави та суспільства.

Державний облік об'єктів КІ та ведення Національного реєстру об'єктів критичної інфраструктури доцільно здійснювати одному державному органу. Це може бути Державний орган у сфері захисту критичної інфраструктури, СБ України, чи за аналогією з обліком потенційно небезпечних об'єктів – Державна архівна служба України. Вибір вищезазначеного органу доцільно здійснити вже за умови чіткого розуміння основ функціонування Державного органу у сфері захисту критичної інфраструктури та його компетенції після прийняття Закону України «Про критичну інфраструктуру України та її захист».

Висновки. Таким чином, можна стверджувати, що впровадження процедури розпізнавання об'єктів критичної інфраструктури стане запорукою організації їх ефективного та системного захисту.

Захист об'єктів критичної інфраструктури доцільно розпочинати саме з процесу розпізнавання.

Суть розпізнавання об'єктів критичної інфраструктури полягає у виявленні на об'єктах національної інфраструктури джерел та чинників небезпеки, у разі можливого впливу на них загроз, визначенні ризиків настання негативних наслідків, а також оцінці максимального рівня можливих негативних наслідків від ураження об'єкта КІ (наслідків).

Пропонується результати розпізнавання об'єкта КІ формувати у вигляді Акта розпізнавання об'єкта критичної інфраструктури.

Саме ґрунтовно опрацьована наукова проблема розпізнавання та подальша імплементація в нормативно-правову сферу процедури розпізнавання об'єктів критич-

ної інфраструктури забезпечить якісний та оптимальний за кількістю перелік об'єктів критичної інфраструктури. Це дозволить, при подальшій організації їх захисту, раціонально застосовувати наявні сили і засоби державних структур.

Розпізнавання об'єктів критичної інфраструктури має здійснюватися за територіальним та галузевим принципом.

Об'єкт розпізнається як об'єкт критичної інфраструктури за наявності достатнього ризику настання негативного наслідку від можливого ураження такого об'єкта за шкалою оцінювання ризику з градацією на «високий – середній – низький – вкрай низький».

За результатами розпізнавання, об'єкти національної інфраструктури можуть бути віднесені

до критичної. Після чого формуватимуться галузеві переліки об'єктів критичної інфраструктури та затверджуватиметься на рівні Кабінету Міністрів України Національний перелік об'єктів критичної інфраструктури.

Згідно з нашою позицією закріплення запропонованого порядку проведення розпізнавання доцільно передбачити у розпорядчому акті Кабінету Міністрів України «Про затвердження процедури розпізнавання, паспортизації та проведення перевірки надійності об'єктів критичної інфраструктури». Структура і зміст цього акта можуть стати темою подальших наукових досліджень.

Зазначені заходи сприятимуть побудові у державі чіткої вертикальної та міжгалузевої системи захисту критичної інфраструктури. ■

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ерменчук О. П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : монографія. Дніпро : ДДУВС, 2018. 180 с.
2. Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress. John D. Moteff, Specialist in Science and Technology Policy. August 23, 2012. Prepared for Members and Committees of Congress. URL: <https://fas.org/sgp/crs/homesec/R42683.pdf>. (дата звернення: 17.06.2019).
3. Про затвердження рішення Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України» : указ Президента України від 14 березня 2016 р. № 92/2016 / Президент України. Урядовий ку'єр. 2016. № 52 (18.03.2016).
4. Про затвердження рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» : указ Президента України від 26 травня 2015 року № 287/2015 / Президент України. Урядовий кур'єр. 2015. № 95 (29.05.2015).
5. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : розпорядження Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р. / Кабінет Міністрів України. Урядовий кур'єр. 2018. № 5 (10.01.2018).
6. Про уведення в дію рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» : указ Президента від 16 січня 2017 р. № 8/2017 / Президент України. Урядовий кур'єр. 2017. № 9 (18.01.2017).
7. Круглий стіл «Паспортизація об'єктів критичної інфраструктури: формування системи аналізу інформації». 23.03.2018. Офіційний сайт Національного інституту стратегічних досліджень. URL: <http://old2.niss.gov.ua/articles/2951>. (дата звернення: 17.06.2019).