УДК 351.863 +338.246.87

АНАЛІЗ ОРГАНІЗАЦІЇ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА СТРАТЕГІЧНОМУ РІВНІ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ЯК ВАЖЛИВА СКЛАДОВА ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

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

Постановка проблеми. Сьогодні українська держава у безпековому вимірі протистоїть безпрецедентним загрозам. Бажання належним чином відстояти національні інтереси та при цьому продовжувати вигідний нам шлях розвитку, забезпечувати захист інтересів наших громадян від загроз розвідувально-підривного, терористичного, кіберінформаційного, техногенного і іншого характеру, настання яких можливе через ураження об'єктів критичної інфраструктури, зумовлюють необхідність раціонального системного підходу до побудови належної нормативно-правової бази щодо захисту об'єктів критичної інфраструктури (далі – КІ) [1].

Стан дослідження. Окремі питання, пов'язані з захистом критичної інфраструктури, були порушені в наукових працях Д. С. Бірюкова, Є. В. Брежнєва, Д. Г. Бобро, О. Ф. Величка, Д. В. Дубова тощо. Однак сучасний стан нормативно-правової бази у сфері функціонування та захисту критичної інфраструктури та його вплив і значення для забезпечення національної безпеки потребують комплексного наукового дослідження.

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

Мета статті. Все нові та небезпечні виклики національній безпеці висувають на порядок денний завдання із побудови в Україні системи захисту критичної інфраструктури, невід'ємною складовою якої є розробка якісної нормативно-правової бази. Саме належний стан захисту об'єктів КІ на стратегічному рівні нормативно-правового регулювання є запорукою дієвості всієї системи захисту критичної ін-

фраструктури держави та потребує якісного й детального наукового дослідження.

Основний матеріал. Правову основу діяльності із організації захисту об'єктів критичної інфраструктури становлять: Конституція України, Кодекси та закони України, акти Президента України та Кабінету Міністрів України, а також ратифіковані Верховною Радою України міжнародні нормативно-правові акти.

Аналізуючи стан захисту об'єктів КІ на стратегічному рівні нормативно-правового регулювання, необхідно в першу чергу зазначити, що обов'язок держави з організації захисту КІ в Україні вимагає Основний Закон. У його статті 3 закріплено, що безпека людини визнається в Україні найвищою соціальною цінністю. Водночас відповідно до загальних засад Конституції України, захист суверенітету держави, забезпечення її економічної, інформаційної та екологічної безпеки належать до найважливіших функцій держави та є справою всього Українського народу (ст. ст. 16, 17).

Регулятивну роль держави у захисті економіки від різних загроз та необхідність вжиття відповідних управлінських заходів закріплюють положення ст. ст. 13, 42 Конституції України, де передбачено обов'язок держави у забезпеченні соціальної спрямованості економіки та захист інтересів суб'єктів господарювання та споживачів.

У контексті нашого дослідження існує першочергова доцільність здійснити аналіз концептуальних документів, що закладають основу функціонування системи захисту критичної інфраструктури. Так, метою Концепції розвитку сектору безпеки і оборони України (далі – Концепції) є визначення шляхів формування національних безпекових та оборонних спроможностей, що в тому числі забезпечать створення національної 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.

Водночас у Концепції визнано важливим та передбачено проведення контррозвідувального захисту об'єктів критичної інфраструктури, що мають стратегічне значення, та критичної інформаційної інфраструктури, здійснення тестування готовності захисту об'єктів критичної інформаційної інфраструктури до можливих кібератак та кіберінцидентів.

Крім цього, стосовно функціонування критичної інфраструктури також пріоритетним зазначається упровадження нових і розвиток базових та критичних технологій; проведення аудиту захищеності об'єктів критичної інформаційної інфраструктури на вразливість; забезпечення стійкого функціонування в умовах надзвичайних ситуацій та в особливий період об'єктів критичної інфраструктури.

Забезпечення комплексної безпеки на об'єктах критичної інфраструктури згідно з Концепцією можливе за умов удосконалення нормативно-правової бази, запровадження інтегрованої системи освіти і підготовки кадрів, централізації управління та підвищення рівня міжвідомчої координації і взаємодії, в тому числі функціонування державної системи кризового реагування.

Основними державними органами, відповідальними за захист КІ, визначено Службу безпеки України (здійснює контррозвідувальне забезпечення діяльності об'єктів критичної інфраструктури), Державну службу спеціального зв'язку та захисту інформації України (кіберзахист інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем і мереж об'єктів критичної інформаційної інфраструктури України, протидія та реагування на комп'ютерні інциденти), Міністерство внутрішніх справ України (Національна поліція – протидія злочинній діяльності у сфері, Національна гвардія України – підтримання громадської безпеки та фізичний захист об'єктів критичної інфраструктури) [2].

Основи 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 в економічній, соціальній, гуманітарній та інших сферах, закладає Стратегія національної безпеки України від 6 травня 2015 р.

Серед актуальних загроз національній безпеці важлива увага приділена загрозам кібербезпеці і безпеці інформаційних ресурсів. Серед них виділено: уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом.

Водночас вперше в законодавчих актах такого високого стратегічного рівня у державі визначається перелік загроз безпеці критичної інфраструктури. Найважливішими серед яких законодавець вважає такі: критична зношеність основних фондів об'єктів інфраструктури України та недостатній рівень їх фізичного захисту; недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій; неефективне управління безпекою критичної інфраструктури і систем життєзабезпечення.

У цьому ж документі передбачено комплексний державний

підхід до захисту критичної інфраструктури. Так, одним із завдань Національної гвардії України як військового формування з правоохоронними функціями, визначено її участь у забезпеченні громадської безпеки та фізичному захисті об'єктів критичної інфраструктури.

Важливо вказати, що забезпечення безпеки критичної інфраструктури визначено одним із пріоритетних напрямів державної політики національної безпеки України. У цьому процесі основу складають такі напрями: комплексне вдосконалення правової основи захисту критичної інфраструктури, створення системи державного управління її безпекою; посилення охорони об'єктів критичної інфраструктури, зокрема, енергетичної і транспортної; налагодження співробітництва між суб'єктами захисту критичної інфраструктури, розвиток державно-приватного партнерства у сфері запобігання надзвичайним ситуаціям та реагування на них; розробка та запровадження механізмів обміну інформацією між державними органами, приватним сектором і населенням стосовно загроз критичній інфраструктурі та захисту чутливої інформації у цій сфері; профілактика техногенних аварій та оперативне і адекватне реагування на них, локалізація і мінімізація їх наслідків; розвиток міжнародного співробітництва у цій сфері [3].

Про надзвичайно вагоме значення КІ для безпеки держави свідчить те, що необхідність її захисту у разі збройного конфлікту передбачає Воєнна доктрина України (далі – Доктрина).

Оскільки Доктрина закладає принципи і шляхи запобігання воєнним конфліктам, а також підстави застосування воєнної сили для захисту державного суверенітету, територіальної цілісності, інших життєво важливих національних інтересів України, визначені в ній завдання і пріоритети повинні стати справою всього українського народу та беззаперечно виконуватись.

Водночас зазначений стратегічний документ доктринального характеру чітко визначає серед завдань органів сектору безпеки і оборони вжиття заходів із забезпечення кіберзахисту об'єктів критичної інфраструктури, посилення охорони і захисту важливих державних об'єктів та об'єктів критичної інфраструктури, у разі збройного конфлікту всередині держави тощо.

Враховуючи зазначене, як передбачено у Доктрині, важливими для забезпечення воєнної безпеки вважаються збереження і розвиток базових та критичних технологій, створення державного фонду розвитку базових і критичних технологій та підтримки інновацій в оборонно-промисловому комплексі, упровадження комплексу організаційних, технічних, економічних, правових та інших заходів, спрямованих на зниження залежності України від критичного імпорту продукції (товарів, робіт, послуг). Разом з тим забезпеченню воєнної безпеки, захисту прав і свобод людини і громадянина, державного суверенітету і територіальної цілісності сприятиме організація належного захисту об'єктів критичної інфраструктури [4].

У січні 2017 року, керуючись вимогами Стратегії національної безпеки України, з метою забезпечення комплексного вдосконалення правової основи захисту критичної інфраструктури та створення системи державного управління її безпекою, Президент України своїм Указом № 8/2017 передбачив розробити і схвалити Концепцію створення державної системи захисту критичної інфраструктури та план заходів з її реалізації. У цьому акті президентської гілки влади також передбачено створити та внести в установленому порядку на розгляд Верховної Ради України проект Закону України «Про критичну інфраструктуру та її захист». Згідно з поставленими керівництвом держави вимогами, зазначений Закон має передбачити врегулювання питань, зокрема, щодо: створення державної системи захисту критичної інфраструктури; визначення органу, відповідального за координацію діяльності із захисту критичної інфраструктури в мирний час та в умовах особливого періоду; визначення функцій, повноважень та відповідальності центральних органів виконавчої влади та інших органів у сфері захисту критичної інфраструктури, а також прав, обов'язків та відповідальності власників і операторів об'єктів критичної інфраструктури; запровадження єдиної методології проведення оцінки загроз критичній інфраструктурі та реагування на них, зокрема щодо аварій і технічних збоїв, небезпечних природних явищ, зловмисних дій; запровадження критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядок їх паспортизації та категоризації; засад державно-приватного партнерства та ресурсного забезпечення у сфері захисту критичної інфраструктури; міжнародного співробітництва у сфері захисту критичної інфраструктури.

Службі безпеки України поставлено завдання з удосконалення контррозвідувального забезпечення та захисту критичної інфраструктури [5].

Питання формування правової основи кіберзахисту об'єктів КІ загалом та формування системи захисту інформаційної критичної інфраструктури відображено у Стратегії кібербезпеки України. Доцільність належної організації кіберзахисту сфери засвідчує недостатній рівень захищеності критичної інфраструктури, безсис-

темність заходів кіберзахисту критичної інфраструктури, недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронних інформаційних ресурсів тощо [6].

Організаційну структуру та правові основи системи кіберзахисту об'єктів критичної інфраструктури визначає Закон України «Про основні засади забезпечення кібербезпеки України». Аналізуючи норми закону, важливо зауважити, що функціонування національної системи кібербезпеки забезпечується в тому числі шляхом розвитку системи контрозвідувального забезпечення кібербезпеки, призначеної для запобігання, своєчасного виявлення та протидії зовнішнім і внутрішнім загрозам безпеці України з використанням кіберпростору; усунення умов, що їм сприяють, та причин їх виникнення. Серед визначень звертають увагу такі, як кіберзагроза, кіберзахист, кібертероризм та кібершпигунство, а також критично важливі об'єкти інфраструктури [7].

Окрім вищезазначених нормативно-правових актів, одним з основоположних документів у сфері функціонування критичної інфраструктури та організації її захисту в Україні стала Концепція створення державної системи захисту критичної інфраструктури 2017 р.

Серед основних завдань Концепції згадаємо такі: розроблення і прийняття законодавчих та інших нормативно-правових актів з питань функціонування державної системи захисту критичної інфраструктури, визначення органу, відповідального за координацію діяльності із захисту критичної інфраструктури; створення організаційно-правової основи та організаційно-інституційної структури державної системи захисту критичної інфраструктури; завершення створення та забезпечення ефективного функціонування державної системи захисту критичної інфраструктури.

Основною метою стратегічного документа законодавець вважає створення системи захисту критичної інфраструктури та визначення основних напрямів, механізмів і строків її комплексного правового врегулювання. Під системою захисту критичної інфраструктури розуміється сукупність об'єктів, які є стратегічно важливими для економіки і безпеки держави, суспільства, населення та порушення функціонування яких може завдати шкоди життєво важливим національним інтересам України.

Реалізація цієї Концепції розрахована з 2017 по 2027 рр. та поєднує у собі проведення законодавчих перетворень, інституційні й організаційні зміни існуючої системи захисту критичної інфраструктури.

Згідно з положеннями зазначеного нормативного акта, каталізатором для запровадження системного підходу до захисту критичної інфраструктури є наявні загрози національній безпеці усіх видів, включаючи загрози природного та техногенного характеру, підвищення рівня терористичних загроз, збільшення кількості та підвищення складності кібератак, загрози, спричинені протиправними діями, а також пошкодження та знищення цілісності інфраструктурних об'єктів держави у зоні проведення Операції об'єднаних сил.

Для визначення необхідного рівня захисту об'єктів критичної інфраструктури Концепцією пропонується ввести їх такі чотири категорії: критично важливі об'єкти – об'єкти, які мають загальнодержавне значення, розгалужені зв'язки та значний вплив на іншу інфраструктуру. Зазначені об'єкти включаються до переліку об'єктів критичної інфраструктури, щодо яких на державному рівні формуються вимоги до забезпечення їх захисту та регламентується використання державних ресурсів і сил; життєво важливі об'єкти – об'єкти, порушення функціонування яких призведе до кризової ситуації регіонального значення. Зазначені об'єкти включаються до переліку об'єктів критичної інфраструктури, щодо яких формуються вимоги стосовно розмежування завдань і повноважень органів державної влади та власників (розпорядників) об'єктів критичної інфраструктури із забезпечення їх захисту та відновлення їх функціонування; важливі об'єкти – об'єкти, пріоритетом захисту яких є забезпечення швидкого відновлення функцій шляхом диверсифікації та залучення резервів. Відповідальність за стійкість функціонування об'єктів несуть їх власники (розпорядники) відповідно до законодавства; необхідні об'єкти – об'єкти інфраструктури, що не належить до критичної, безпосередній захист яких є відповідальністю власника (розпорядника), який у кризовій ситуації діє згідно з відповідним планом реагування [8].

Розбудові системи захисту критичної інфраструктури сприятиме розробка та подання на розгляд Кабінету Міністрів України проекту Закону України «Про критичну інфраструктуру та її захист».

Новий поштовх у процес захисту об'єктів критичної інфраструктури від терористичних проявів вносить Указ Президента України від 5 березня 2019 р. № 53/2019, що затвердив Концепцію боротьби з тероризмом [9].

Крім того, серед актів стратегічного рівня нормативно-правового регулювання важливо зазначити Закон України «Про національну безпеку України» від 2018 р. Він вперше визначає необхідність контррозвідувального забезпечення об'єктів кри-

тичної інфраструктури одним з основних завдань СБ України поряд із завданнями з боротьби з тероризмом, контррозвідувального захисту кібербезпеки, економічної та інформаційної безпеки держави [10].

Висновки. Таким чином, аналіз стану захисту об'єктів КІ на стратегічному рівні нормативно-правового регулювання свідчить, що загалом існує достатня кількість нормативних актів, які закладають основи для створення системи захисту критичної інфраструктури в Україні.

Водночас наявна правова база, що регулює діяльність різних державних систем реагування та захисту, які в тому числі забезпечують протидію загрозам критичній інфраструктурі, розроблена нерівномірно та переважно регулює правовідносини галузевого характеру, зокрема: захист кіберсфери, протидії терористичній діяльності, загрозам природного та техногенного характеру, організації захисту ядерних матеріалів, ядерних установок, радіоактивних відходів, інших джерел іонізуючого випромінювання тощо.

При цьому структура, організація, основи діяльності та вертикальна інтегрованість вищезазначених систем також різні. Це в свою чергу передусім вимагає детального аналізу для побудови нової системи захисту критичної інфраструктури в Україні. Доцільним є вивчення можливостей та проведення наукового аналізу її створення у централізованій та децентралізованій формі.

Для функціонування зазначеної системи все ж доцільно окреслити організаційно-інституційну структуру, суб'єктів забезпечення та їх повноваження і чітко окреслити сферу діяльності, а також передбачити основи, принципи й форми організації їх діяльності. Беззаперечно, цьому сприятиме подальше удосконалення організаційно-правової основи функціонування системи захисту критичної інфраструктури в Україні. ■

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : моногр. / О. П. Єрменчук. – Дніпро : ДДУВС, 2018. – 180 с.
2. Указ Президента України від 14 березня 2016 р. № 92/2016 «Про затвердження рішення Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України» / Урядовий кур'єр від 18.03.2016. – № 52.
3. Указ Президента України від 26 травня 2015 р. № 287/2015 «Про затвердження рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» / Урядовий кур'єр від 29.05.2015. – № 95.
4. Указ Президента України «Про уведення в дію рішення Ради національної безпеки і оборони України від 2 вересня 2015 р. «Про нову редакцію Воєнної доктрини України» від 24 вересня 2015 року № 555/2015 / Урядовий кур'єр від 26.09.2015. – № 178.
5. Указ Президента «Про уведення в дію рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» від 16 січня 2017 р. № 8/2017 / Урядовий кур'єр від 18.01.2017. – № 9.
6. Указ Президента України від 15 березня 2016 р. № 96/2016 «Про уведення в дію рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» / Урядовий кур'єр від 18.03.2016. – № 52.
7. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII / Урядовий кур'єр від 15.11.2017. – № 215.
8. Розпорядження Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р «Про схвалення Концепції створення державної системи захисту критичної інфраструктури» / Урядовий кур'єр від 10.01.2018. – № 5.
9. Указ Президента України «Про концепцію боротьби з тероризмом в Україні» від 5 березня 2019 р. № 53/2019 / Урядовий кур'єр від 12.03.2019. – № 48.
10. Закон України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII / Урядовий кур'єр від 18.07.2018. – № 132.