УДК 351.863 +338.246.87

Єрменчук О.П.
к.ю.н.,
доцент кафедри оперативно-розшукової діяльності
Дніпропетровський державний університет внутрішніх справ

СТАН НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В КІБЕРСФЕРІ ЯК СКЛАДНИК ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Постановка проблеми. Постійний прогрес суспільства та розвиток новітніх технологій, невпинний процес їх впровадження в життя кожного засвідчує те, що кіберсфера стала надзвичайно важливою складовою частиною забезпечення сталого функціонування державного механізму. Останнім часом вона виступає основним із форпостів у протистоянні безпрецедентним загрозам національній безпеці [1]. Основними цілями деструктивних впливів завжди стають об'єкти, найбільш значимі для забезпечення функціонування певних регіонів чи держави загалом.

Саме тому одним із пріоритетних напрямів державної політики національної безпеки, передбачених Стратегією національної безпеки України, визначено забезпечення безпеки критичної інфраструктури (далі – КІ). Цією ж Стратегією закріплено першочергову необхідність створення системи державного управління її безпекою та комплексного вдосконалення правової основи захисту КІ [2].

Огляд останніх досліджень і публікацій. Окремі питання, пов'язані із захистом критичної інфраструктури, були порушені в наукових працях таких українських вчених: Д.С. Бірюкова, Є.В. Брежнєва, Д.Г. Бобро, О.Ф. Величка, Д.В. Дубова, В.П. Горбуліна, С.П. Іванюти, В.В. Зубарєва, В.К. Конах, С.І. Кондратова, М.В. Мірошника, О.І. Насвіт, М.А. Ожевана, В.М. Панченко, В.В. Петрова, І.М. Рижова, П.П. Скурського, О.М. Суходолі, В.М. Щербини, О.М. Юрченка. Однак сучасний стан нормативно-правової бази функціонування та захисту критичної інфраструктури у кіберсфері та його вплив і значення для забезпечення національної безпеки потребують комплексного наукового дослідження.

Зазначені обставини зумовлюють актуальність дослідження та стали основою для наукових пошуків автора і підготовки цих матеріалів.

Формулювання завдання дослідження. Наявні та потенційні загрози національній безпеці висувають на порядок денний завдання із побудови в Україні системи захисту критичної інфраструктури, невід'ємною складовою частиною якої є розробка якісної нормативно-правової бази. Саме належний стан захисту об'єктів КІ у кіберсфері є однією з важливих складових частин дієвості всієї системи захисту критичної інфраструктури держави та потребує якісного й детального наукового дослідження.

Виклад основного матеріалу. Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, про основні засади забезпечення кібербезпеки України та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

Важливо зазначити, що основні засади формування правової основи кіберзахисту об'єктів КІ загалом та формування системи захисту інформаційної критичної інфраструктури відображені у Стратегії кібербезпеки України (далі – Стратегія).

Необхідність кіберзахисту об'єктів КІ законодавець аргументує тим, що останнім часом дедалі частіше об'єктами впливу загроз стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій. Кіберзлочинність поширюється за межі держав та має транснаціональний характер. Значно зросла загроза атак на державні установи та веб-сайти, електронні адреси об'єктів критичної інфраструктури. Отже, захист кіберсфери значно переплітається із забезпеченням національної безпеки. Водночас забезпечення стабільного функціонування кіберпростору залежить від стану нормативно-правового регулювання цієї сфери.

Стратегія розроблена з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Основу національної системи кібербезпеки становлять Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи.

На Службу безпеки України покладаються: попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством, а також щодо готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидія кіберзлочинності, можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтересам України; розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечення реагування на комп'ютерні інциденти у сфері державної безпеки.

Аналіз положень Стратегії свідчить, що найбільш поширеними ризиками, що сприяють деструктивному впливу загроз у кіберсфері, можна вважати недостатній рівень захищеності критичної інфраструктури, безсистемність заходів кіберзахисту критичної інфраструктури, недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронних інформаційних ресурсів тощо.

Серед основних аспектів забезпечення кіберзахисту виділено доцільність таких першочергових заходів: вдосконалення правової основи кіберзахисту об'єктів критичної інфраструктури та визначення критеріїв належності інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем до критичної інформаційної інфраструктури; впровадження державного реєстру об'єктів критичної інформаційної інфраструктури; розробка вимог до кіберзахисту об'єктів критичної інфраструктури; покладання на власників (розпорядників) об'єктів критичної інфраструктури обов'язку створення підрозділів кіберзахисту; покращення державно-приватного партнерства у запобіганні та локалізації кіберзагроз та захисту інформації, а також сприяння власниками (розпорядниками) об'єктів критичної інфраструктури державним органам у виконанні завдань із забезпечення кібербезпеки та кіберзахисту; відпрацювання належного механізму обміну інформацією між партнерами з державного та приватного сектору стосовно загроз критичній інформаційній інфраструктурі [3].

До основоположних нормативно-правових актів, що регулюють захист об'єктів критичної інфраструктури у кіберсфері

необхідно зарахувати Закон України «Про основні засади забезпечення кібербезпеки України». Він визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Цей закон визначає організаційну структуру системи кіберзахисту об'єктів критичної інфраструктури. На нашу думку, зазначена інституційна побудова системи належить до так званої «децентралізованої». Вона охоплює і президентську, і урядову гілки влади. Так, координація діяльності у сфері кібербезпеки як складової частини національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України. Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України. Своєю чергою, Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури в банківській системі України).

Аналізуючи закон, необхідно зауважити, що функціонування національної системи кібербезпеки тісно пов'язане із забезпеченням національної безпеки України та реалізується шляхом розвитку системи контррозвідувального 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.

Важливо, що законодавець визначив національну систему кібербезпеки, надавши змогу на законодавчому рівні суб'єктам забезпечення кібербезпеки здійснювати об'єднані єдиним задумом заходи політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних заходів тощо, а також наділивши чіткими повноваженнями кожного з них.

Серед визначень варті уваги такі, як кіберзагроза, кіберзахист, кіберрозвідка, кібертероризм та кібершпигунство. Окремо слід зупинитись на тому, що законодавець дає визначення критично важливим об'єктам інфраструктури (далі – об'єкти критичної інфраструктури). Зокрема, в кіберсфері під ними розуміють підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, довкілля, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей. Крім того, визначено й «об'єкт критичної інформаційної інфраструктури» – це комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака, яка безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури [4].

Наступним надзвичайно важливим актом у сфері організації захисту критичної інфра-

структури є Постанова Кабінету Міністрів України «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» від 23.08.2016 р. № 563.

Саме вона вперше в Україні на рівні підзаконних актів дає визначення поняття «критична інфраструктура».

Хоча саме визначення є в певних аспектах дискусійним та потребує удосконалення, воно надає основний поштовх для організації захисту критичної інфраструктури, оскільки переростає з віртуального виміру у конкретний та стає умовною точкою відліку у вітчизняному нормотворенні. «Критична інфраструктура» тут розглядається як сукупність об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природнє середовище, спричинити значні фінансові збитки та людські жертви. Законодавець також визначив «об'єкти критичної інфраструктури» як підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення.

Низка дискусійних питань у зазначеному нормативно-правовому акті пов'язана з тим, стосуються самі визначення лише інформаційно-телекомунікаційної сфери, взаємовідносини в якій регулює зазначений акт КМ України чи вони мають міжгалузеве значення. Обговорення викликає також і сама дефініція – критична інфраструктура та об'єкти критичної інфраструктури. На думку автора, їх значення доцільно розглядати значно ширше.

Водночас необхідно зазначити, що саме завдяки положенням постанови, міністерствам, іншим центральним органам виконавчої влади разом із Службою безпеки, іншим заінтересованим державним органам передбачено подати пропозиції до переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. Тобто можна констатувати початок формування переліку об'єктів критичної інфраструктури в цій сфері [5].

Через розуміння того, що сфера забезпечення кібербезпеки перебуває у кризовому стані та потребує законодавчого закріплення достатніх повноважень для державних органів із метою її належного захисту, в 2016 р. РНБО було прийнято відповідне Рішення «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації». На Кабінет Міністрів України були покладені обов'язки щодо удосконалення законодавства стосовно організації кіберзахисту об'єктів критичної інфраструктури, підвищення фаховості кадрового потенціалу та взаємовідповідальності учасників. Для прикладу, важливим поштовхом до налагодження якісно нового рівня взаємодії з питань захисту критичної інфраструктури стала декларація затвердження протоколу спільних дій суб'єктів забезпечення кібербезпеки, власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час виявлення, попередження, припинення кібератак та кіберінцидентів, а також усунення їх наслідків.

Відповідний досвід іноземних держав, втілений у Конвенції про кіберзлочинність, свідчить про доцільність надання правоохоронним органам України повноважень щодо внесення обов'язкових до виконання приписів власникам комп'ютерних даних (операторам та провайдерам телекомунікацій, іншим юридичним і фізичним особам), що сприятимуть припиненню протиправної діяльності, запровадження відповідальності за невиконання законних вимог посадових осіб Служби безпеки України. Водночас Національну поліцію України разом із Службою безпеки України зобов'язано якісно повно та об'єктивно розслідувати кібератаки [6].

З метою завершення та остаточного вирішення піднятої проблематики в 2017 р.

РНБО приймає Рішення «Про стан виконання рішення Ради національної безпеки і оборони України від 29.12.2016 р.».

Зазначений нормативний акт є досить важливим для підняття рівня забезпечення державної безпеки та організації спільних міжвідомчих заходів із захисту критичної інфраструктури зокрема. Норми акта передбачають низку дій, які зміцнюють координаційно-виконавчу участь різних учасників та інтенсифікують взаємоінтеграційні процеси. Так, передбачено здійснити удосконалення системи інформаційного обміну про кіберзагрози, модернізацію ситуаційних центрів із кібербезпеки Служби безпеки України та Державної служби спеціального зв'язку та захисту інформації України, створити єдину інтерактивну базу даних про кіберінциденти та національну телекомунікаційну мережу державних органів. Адміністрації Державної служби спеціального зв'язку та захисту інформації України разом зі Службою безпеки України передбачено невідкладно визначити першочергові потреби розвитку організаційно-технічної моделі кіберзахисту.

На думку автора, дієвість диспозитивних норм чинного законодавства у сфері захисту критичної інфраструктури вдасться підвищити завдяки передбаченим завданням щодо підготовки за участю Служби безпеки України законопроекту щодо розмежування кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, вчинені щодо державних та інших інформаційних ресурсів, щодо об'єктів критичної інформаційної інфраструктури та інших об'єктів, а також відповідного розмежування підслідності [7].

Висновки. Таким чином, стан нормативно-правового регулювання захисту об'єктів критичної інфраструктури у кіберсфері варто вважати важливою складовою частиною забезпечення національної безпеки України. Від нього залежить ефективне функціонування всієї системи та її здатність протистояти наявним та потенційним загрозам, тобто здатність виконувати основні задачі, передбачені законодавцем.

Про важливість таких задач для національної безпеки свідчить також те, що основними повноваженнями в сфері захисту критичної інфраструктури законодавець наділяє представників сектору безпеки і оборони держави.

У процесі дослідження встановлено, що законодавство із зазначеного питання перебуває у стадії створення та потребує подальшого удосконалення.

Першочергових заходів з удосконалення вимагають і наведені нижче аспекти нормативно-правового регулювання сфери. Законом України «Про основні засади забезпечення кібербезпеки України» (ст. 4) та Постановою Кабінету Міністрів України № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» передбачено порядок формування переліку об'єктів критичної інфраструктури та інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури, водночас нині таких переліків фактично не існує. Крім того, невизначеними залишаються передбачені ч. 2 ст. 6 Закону України «Про основні засади забезпечення кібербезпеки України» критерії та порядок зарахування об'єктів до критичної інфраструктури, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз. Вони мають бути визначені Кабінетом Міністрів України, а в банківській сфері – Нацбанком.

Становить науковий інтерес та вимагає практичного вирішення порядок негласної перевірки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберзагроз, що передбачено ст. 8 зазначеного нормативного акта.

Низка дискусійних питань стосується положень Постанови Кабінету Міністрів України від 23.08.2016 р. № 563 та пов'язана з тим, стосуються вжиті визначення лише інформа-

ційно-телекомунікаційної сфери, взаємовідносини в якій регулює зазначений акт, чи вони мають міжгалузеве значення. На нашу думку, викликає обговорення та потребує удосконалення також і сама дефініція «об'єкти критичної інфраструктури», оскільки їх значення доцільно розглядати значно ширше.

Вирішення наявних недоліків та створення належного національного законодавства щодо захисту об'єктів критичної інфраструктури у кіберсфері сприятиме захисту національної безпеки та, відповідно, розвитку національної економіки та громадянського суспільства в Україні.

Анотація

Проаналізовано нормативно-правові акти, що формують основу захисту об'єктів критичної інфраструктури у кіберсфері. У процесі аналізу встановлено, що законодавство із зазначеного питання перебуває у стадії створення та потребує подальшого удосконалення. Вважається, що вирішення наявних недоліків та створення належного національного законодавства щодо захисту об'єктів критичної інфраструктури у кіберсфері сприятиме захисту національної безпеки та, відповідно, розвитку національної економіки та громадянського суспільства.

Ключові слова: критична інфраструктура, захист критичної інфраструктури, національна безпека, стан нормативно-правового регулювання.

Аннотация

Проанализированы нормативно-правовые акты, формирующие основу защиты объектов критической инфраструктуры в киберсфере. В ходе анализа установлено, что законодательство по данному вопросу находится в стадии создания и требует дальнейшего совершенствования. Считается, что решение имеющихся недостатков и создание надлежащего национального законодательства по защите объектов критической инфраструктуры в киберсфере будет способствовать защите национальной безопасности и, соответственно, развитию национальной экономики и гражданского общества.

Ключевые слова: критическая инфраструктура, защита критической инфраструктуры, национальная безопасность, состояние нормативно-правового регулирования.

Yermenchuk O.P. The state of normative-legal regulation of the protection of objects of critical infrastructure in the cybersphere as a composition of national security

Summary

The normative and legal acts forming the basis of protection of objects of critical infrastructure in the cybersphere are analyzed. The analysis revealed that the legislation on this issue is under construction and needs further improvement. It is believed that solving existing shortcomings and establishing proper national legislation to protect critical infrastructure in the cyberspace will contribute to the protection of national security and, accordingly, the development of the national economy and civil society.

Key words: critical infrastructure, critical infrastructure protection, national security, state of normative regulation.

Список використаних джерел:

1. Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : монографія. Дніпро : ДДУВС, 2018. 180 с.
2. Про Стратегію національної безпеки України : Указ Президента України «Про затвердження рішення Ради національної безпеки і оборони України від 6 травня 2015 року» від 26 травня 2015 р. № 287/2015. *Урядовий кур'єр.* 2015. № 95.

3. Про Стратегію кібербезпеки України : Указ Президента України «Про уведення в дію рішення Ради національної безпеки і оборони України від 27 січня 2016 року» від 15 березня 2016 р. № 96/2016. *Урядовий кур'єр*. 2016. № 52.
4. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. *Урядовий кур'єр*. 2017. № 215.
5. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави : Постанова Кабінету Міністрів України від 23 серпня 2016 р. № 563. *Урядовий кур'єр*. 2016. № 168.
6. Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації : Указ Президента України «Про уведення в дію Рішення РНБО від 29.12.2016 р.» від 13 лютого 2017 р. № 32/2017. *Урядовий кур'єр*. 2017. № 30.
7. Про стан виконання рішення Ради національної безпеки і оборони України від 29.12.2016 р. «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13.02.2017 р. № 32 : Указ Президента України «Про Рішення РНБО від 10.07.2017 р.» від 30.08.2017 р. № 254/2017. *Урядовий кур'єр*. 2017. № 162.