УДК 351.86:659.3/.4:004.738.5]:005.334(477)

О. І. Жайворонок,
аспірант кафедри глобалістики, євроінтеграції та управління національною безпекою,
Національна академія державного управління при Президентові України, м. Київ

ВДОСКОНАЛЕННЯ МЕХАНІЗМУ ПРОТИДІЇ ІНФОРМАЦІЙНОМУ ТЕРОРИЗМУ В УКРАЇНІ В ЗАГАЛЬНОДЕРЖАВНІЙ СИСТЕМІ АНТИКРИЗОВОГО РЕАГУВАННЯ

O. Zhaivoronok,
post-graduate student of the Department of Globalistics, European Integration and National Security Management of the National Academy for Public Administration under the President of Ukraine

IMPROVING THE MECHANISM OF COUNTERACTION TO INFORMATION TERRORISM IN UKRAINE IN THE GENERAL SYSTEM OF ANTI-CRISIS REACTION

У статті, з урахуванням чинного вітчизняного законодавства, здійснено аналіз існуючих державних інституцій, що формують систему антикризового реагування в Україні (суб'єктів антикризового реагування), виявлено взаємозв'язок між виникненням кризових явищ у державі та неефективністю дії інформаційних механізмів публічного управління, між глобальним та національним рівнем прояву терористичних загроз (у тому числі загроз інформаційного тероризму), запропоновано можливі напрями вдосконалення вітчизняного державного механізму протидії інформаційному тероризму як складової загальнодержавної системи реагування на кризові ситуації.

Поміж інших, висловлено думку про необхідність створення моделі ефективної управлінської ланки держави, яка зможе керувати наявними ресурсами сил і засобів суб'єктів антикризового реагування під час виникнення будь-яких кризових ситуацій (довготривалих, системних, екстремально-часових) для надання керівництву держави необхідних варіантів антикризового реагування.

In the article, taking into account the current domestic legislation, the analysis of existing state institutions that form the system of crisis response in Ukraine (subjects of the crisis response), the relationship between the emergence of crisis phenomena in the state and the ineffectiveness of the information mechanisms of public administration, between the global and the national level of manifestation of terrorist threats (including threats of information terrorism), possible directions of improvement of the domestic state counter-mechanism information terrorism as an integral part of the nationwide crisis response system.

Among others, the opinion was expressed on the necessity of creating an effective management model of the state that would be able to manage the available resources of the forces and means of the subjects of the crisis response during the occurrence of any crisis situations (long-term, systemic, extreme-time) to provide the government with the necessary options crisis response.

Ключові слова: інформаційний тероризм, кіберпростір, кібератака, державне управління, інформаційна безпека, інформаційний тероризм, гібридна війна, антикризове реагування.

Key words: information terrorism, cyber space, cyberattack, public administration, information security, information terrorism, hybrid warfare, anti-crisis response.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК З ВАЖЛИВИМИ НАУКОВИМИ ТА ПРАКТИЧНИМИ ЗАВДАННЯМИ

У результаті глобалізації світ стає більш зв'язаним і залежним від дій міжнародних суб'єктів, відбувається збільшення кількості спільних для держав проблем [1]. У зв'язку з цим збільшуються кількість довгострокових викликів та загроз національній безпеці України, де ключовим стає саме інформаційний чинник: збройний конфлікт на Сході країни, гібридна війна Російської Федерації, дестабілізація внутрішньополітичної си-

туації. Механізми державного реагування на інформаційні загрози, агресивну ворожу пропаганду проти України показують свою слабку ефективність: неспроможність органів державної влади налагодити цілісну стратегію інформаційно-комунікативної політики, слабка захищеність власного інформаційного простору, постійний пошук балансу між свободою слова та необхідним рівнем контролю в інтересах національної безпеки.

Усі ці обставини підкреслюють актуальність практики протидії інформаційному тероризму як функції загальнодержавної системи антикризового реагування та її зв'язок з найбільш важливими науковими та практичними завданнями сучасного державного управління у сфері інформаційної безпеки. Інформаційна безпека забезпечує безперешкодну реалізацію у суспільстві конституційних прав, які спрямовані на вільне одержання, створення й розповсюдження інформації. Відповідний рівень інформаційної безпеки необхідно забезпечити шляхом реалізації певних політичних, економічних та організаційних заходів, пов'язаних з попередженням, виявленням і нейтралізацією таких обставин, чинників і дій, що можуть завдати збиток чи перешкодити реалізації інформаційних прав, потреб та інтересів країни та її громадян.

Перш за все, необхідно провести аналіз існуючих державних інституцій, що формують систему антикризового реагування в Україні, виявити і зрозуміти можливий зв'язок між виникненням кризових явищ в державі та неефективністю публічного і державного управління, між глобальним та національним рівнем прояву терористичних загроз (у тому числі загроз інформаційного тероризму), окреслити можливі напрямки (шляхи) вдосконалення державного механізму протидії інформаційному тероризму, як складової загальнодержавної системи реагування на кризові ситуації.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Аналіз стану наукової розробленості проблеми забезпечення інформаційної безпеки вказує на безсумнівно велику кількість наукових досліджень з цієї тематики. Так, В. Ліпкан, Ю. Максименко, В. Желіховський у своїй праці "Інформаційна безпека України в умовах євроінтеграції" глибоко аналізують і роблять очевидний висновок про те, що інформаційний тероризм застосовується з метою дезінформації, дезорієнтації і профанації для помилкового сприймання, помилкового розуміння і неадекватної поведінки суспільства [2, с. 15].

Науковому осмисленню проблем реалізації інформаційної безпеки в сучасному суспільстві сприяли праці таких дослідників: А. Даллеса, М. Кастельса, В.С. Шапіро, М.В. Баглая, А.В. Крутських, І.Л. Сафронова, О.А. Смірнова, Є.Б. Бєлова та ін. Серед українських дослідників, які розробляють методологічні засади інформаційної безпеки, слід відзначити таких, як: О.Г. Широкова-Мурараш, В.І. Гурковський, Г.М. Сащук, Г.Г. Почепцов, В.Г. Королько, О.П. Голобуцький, В.М. Брижко, В.С. Цимбалюк, Б.А. Кормич, Є.Я. Кравець, О.В. Олійник, Л.Є. Шиманський та ін. Відомий дослідник В.М. Фурашев визначає основні стримуючі фактори правового забезпечення інформаційної безпеки для України [3, с. 117—118].

У наукових джерелах останніх років окремим питанням розглядалися правові засади діяльності військових формувань і правоохоронних органів в умовах збройного протистояння у роботах А.В. Басова, С.В. Бєлая, Ю.В. Дубка, О.В. Гуляка, І.В. Євтушенка, С.О. Кузніченка, В.А. Лаптія, С.О. Магди, В.Я. Настюка, О.В. Негодченка, Г.М. Перепелиці, В.М. Плішкіна, М.Б. Саакяна, М.П. Стрельбицького, Д.В. Талалая, О.С. Шаптали та ін. Означеними науковцями зроблено значний доробок у дослідження проблем службово-бойової діяльності військових формувань та правоохоронних органів спеціального призначення в умовах збройного протистояння, однак вони досліджували окремі питання реагування на збройні конфлікти. Ґрунтовного дослідження нормативно-правового забезпечення з реагування на кризові ситуації, що супроводжуються збройним протистоянням, не здійснювалось. Так само залишаються відкритими і потребують подальших досліджень питання вироблення ефективних механізмів державного управління інформаційною сферою у контексті забезпечення безпеки людини, суспільства і держави. Тож тематика дослідження є сучасною та актуальною.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Завданнями цієї статті є аналіз існуючих державних інституцій (суб'єктів), що формують систему антикризового реагування в Україні, виявлення взаємозв'язку між виникненням кризових явищ в державі та неефективністю дії механізмів публічного управління, між глобальним та національним рівнем прояву терористичних загроз (у тому числі загроз інформаційного тероризму), а також окреслення можливих напрямків (шляхів) вдосконалення державного механізму протидії інформаційному тероризму, як складової загальнодержавної системи реагування на кризові ситуації.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Серед науковців триває полеміка щодо визначення природи і сутності кризи. На даний час серед фахівців немає єдиного підходу до з'ясування як сутності кризи, так і до змісту антикризового управління. Однак при відповідній організації управління та ухваленні необхідних управлінських рішень держава має усі можливості подолати ризики і загрози, що постають перед нею, незважаючи на негативний вплив зовнішнього оточення. Тому, насамперед, необхідно визначитися з суб'єктами реагування на кризові ситуації в Україні та законодавством, що лежить в основі формування системи антикризового реагування.

Відповідно до Конституції України, координаційним органом з питань національної безпеки і оборони при Президентові України є Рада національної безпеки і оборони України, функціями якої є "внесення пропозицій Президентові України щодо реалізації засад внутрішньої і зовнішньої політики у сфері національної безпеки і оборони, координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони у мирний час, а також координація та здійснення контролю за діяльністю органів вико-

навчої влади у сфері національної безпеки і оборони в умовах воєнного або надзвичайного стану та при виникненні кризових ситуацій, що загрожують національній безпеці України" [4].

Основою нормативно-правового забезпечення з реагування на кризові ситуації, що супроводжуються збройним протистоянням є Закон України "Про основи національної безпеки України" [5]. Він дає визначення поняття "воєнна організація держави" ("сукупність органів державної влади, військових формувань, утворених відповідно до законів України, діяльність яких перебуває під демократичним цивільним контролем з боку суспільства і безпосередньо спрямована на захист національних інтересів України від зовнішніх та внутрішніх загроз"). Закон визначає загрози національній безпеці як наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України. Серед них, поміж інших, у внутрішньополітичній сфері виділяються загрози інформаційної сфери:

— прояви обмеження свободи слова та доступу до публічної інформації;

— поширення засобами масової інформації культу насильства, жорстокості, порнографії;

— комп'ютерна злочинність та комп'ютерний тероризм;

— розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави;

— намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Закон України "Про основні засади забезпечення кібербезпеки України" деталізує та поглиблює нормативно-правове забезпечення з реагування на кризові ситуації в інформаційній сфері, 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 [6].

Особливе значення серед нормативно-правових актів щодо забезпечення національної безпеки України взагалі, а реагування на кризові ситуації, що супроводжуються збройним протистоянням, зокрема, є Стратегія національної безпеки України (далі — Стратегія) [7], яка спрямована на реалізацію до 2020 року визначених нею пріоритетів державної політики національної безпеки. Стратегія має основоположне значення, оскільки відповідає сучасним викликам і загрозам безпеки держави (серед яких інформаційно-психологічна війна, приниження української мови і культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу; загрози кібербезпеці і безпеці інформаційних ресурсів; загрози безпеці критичної інфраструктури), а також визначає основоположні позиції з реагування сил сектору безпеки і оборони на кризові ситуації, що супроводжуються збройним протистоянням, серед яких:

забезпечення інформаційної безпеки;

забезпечення кібербезпеки і безпеки інформаційних ресурсів.

Більш глибокі позиції з реагування сил сектору безпеки і оборони на кризові ситуації в кіберпросторі формулює Стратегія кібербезпеки України [8]. Національна система кібербезпеки має насамперед забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури.

Наступним першорядним нормативно-правовим актом є Воєнна доктрина України, яка є "системою поглядів на причини виникнення, сутність і характер сучасних воєнних конфліктів, принципи і шляхи запобігання їх виникненню, підготовку держави до можливого воєнного конфлікту, а також на застосування воєнної сили для захисту державного суверенітету, територіальної цілісності, інших життєво важливих національних інтересів" [9]. Воєнна доктрина, в першу чергу, грунтується на результатах аналізу та прогнозування воєнно-політичної обстановки та високої готовності до оборони. Так, до воєнно-політичних викликів, які можуть перерости в загрозу застосування воєнної сили проти України, серед інших віднесено цілеспрямований інформаційний (інформаційно-психологічний) вплив з боку РФ з використанням сучасних інформаційних технологій, спрямований на формування негативного міжнародного іміджу України, а також на дестабілізацію внутрішньої соціально-політичної обстановки, загострення міжетнічних та міжконфесійних відносин в Україні або її окремих регіонах і місцях компактного проживання національних меншин.

Основними завданнями воєнної політики України серед інших визначено:

— удосконалення державної інформаційної політики у воєнній сфері;

— попередження та ефективна протидія інформаційно-психологічним впливам іноземних держав, спрямованим на підрив обороноздатності, порушення суверенітету і територіальної цілісності України, дестабілізацію внутрішньої соціально-політичної обстановки, провокування міжетнічних та міжконфесійних конфліктів в Україні.

Ще одним значимим нормативно-правовим актом забезпечення з реагування на кризові ситуації, що супроводжуються збройним протистоянням, є Концепція розвитку сектору безпеки і оборони України (Концепція) [10]. Концепцією визначено, що основною метою реформування та розвитку сектора безпеки і оборони є формування та підтримання спроможностей, що дасть змогу гарантовано забезпечити адекватне і гнучке реа-

гування на весь спектр загроз національній безпеці України, раціонально використовуючи наявні у держави можливості і ресурси. Відповідно до неї, для ефективного розвитку сектора безпеки і оборони в сучасних умовах найбільш перспективними є заходи з забезпечення ISSN 1995-6134 417 Forum Prava, 2017. (5). 415-420 ефективної координації та функціонування державної системи кризового реагування; удосконалення системи державного прогнозування та стратегічного планування, системи планування застосування військ (сил) і засобів сектору безпеки і оборони на основі принципів і стандартів ЄС та НАТО та налагодження та підтримання взаємодії з авторитетними міжнародними організаціями та державами, спрямованої на нейтралізацію негативних наслідків прямих, позаконвенційних, гібридних та інших актів агресії проти України [10].

Також важливими шляхами досягнення необхідних спроможностей складових сектору безпеки і оборони є раціональний розподіл завдань у секторі безпеки і оборони, формування системи управління силами безпеки і оборони та створення єдиної системи ситуаційних центрів державних органів для забезпечення взаємодії цієї системи із Ситуаційним центром НАТО [10]. До обговорення системи ситуаційних центрів ми ще повернемося пізніше, для того, щоб дати їй більш детальне розуміння і визначення її ролі в загальнодержавній системі антикризового реагування.

А підводячи попередній підсумок можливо зауважити таке:

1. Єдиного, врегульованого вітчизняним законодавством підходу до з'ясування як сутності кризи, так і до змісту антикризового управління в Україні немає, що безумовно може бути предметом майбутніх досліджень науковців.

2. Аналізуючи існуючі державні інституції (суб'єкти), що повинні формувати основу загальнодержавної системи антикризового реагування в Україні слід звернути увагу на нещодавно введений в дію Закон України "Про національну безпеку України" [11]. В ньому законодавець дає визначення сектору безпеки і оборони та у статтях 13, 14 пояснює сам принцип і порядок державного реагування на загрози національній безпеці України, у тому числі у разі виникнення кризових ситуацій.

Натомість, можливо констатувати, що високотехнологічні терористичні акції нової епохи здібні сьогодні продукувати системні кризи не тільки в Україні, а й всієї світової спільноти і поставити під загрозу існування окремих регіонів світу. Цей процес підсилюється ще й розвитком інформаційних технологій та появою феномену кібертероризму — явища, яке впливає на стабільність політичної, соціальної, духовної сфери суспільства. В нашій країні кризові явища поміж іншого ще й ускладнюються та підсилюються веденням проти України гібридної війни з боку Російської Федерації.

Тому, очевидним постає питання виявлення взаємозв'язку між виникненням кризових явищ в державі та неефективністю дії механізмів публічного управління, між глобальним та національним рівнем прояву терористичних загроз (у тому числі загроз інформаційного тероризму).

Для початку необхідно проаналізувати сутність та першопричини виникнення кризи, або кризових ситуацій. Кризові явища соціально-економічних систем досліджувалися в працях таких учених, як: С. Бессонов, В. Волконський, С. Говриленков, С. Гурієв, В. Дребенцов, М. Делягін, В. Івантер, А. Ілларіонов, Г. Канторович, Г. Клейнер, О. Луговий, В. Макаров, В. Синельніков, П. Сорокін, Р. Яковлев, Є. Ясін, а також у роботах таких іноземних учених, як: G. Alfandan, J. Dlanchard, G. Calvo, F. Szyrmer, E. Porotti, B. Pinto, J. Rostowski, M. Chafftr та в розробках багатьох інших фахівців. Але основним недоліком більшості теоретичних праць є їх спеціалізована обмеженість щодо криз управлінських структур. Вітчизняні вчені зосередили свою увагу на вивченні таких аспектів подолання кризи в державному управлінні:

— механізми управління кризами суспільного розвитку в системі державного управління (Т.І. Пахомова);

— становлення й розвиток антикризових технологій як механізму реалізації цілей державного управління в Україні (В.І. Шарий).

Серед сучасних зарубіжних досліджень (С. Фланаган, Е. Циммерманн, Т. Парсонс), присвячених політичній кризі, варто відзначити праці, в яких розглядаються питання концептуалізації поняття кризи, методології її дослідження, а також еволюції наукової рефлексії щодо цієї проблематики.

Аналізуючи роботи вчених можливо дійти висновку, що з одного боку криза системи публічного управління підштовхує країну до більш глибоких внутрішніх кризових явищ у політичній, соціальній та духовній сферах і може виражатися в невдоволеннях мас (мітинги, страйки, протести) і призводити до екстремістських, терористичних дій, у тому числі виражених у формі інформаційного тероризму (або кібертероризму). З іншого боку, процеси глобалізації світу та розвитку інформаційно-комунікаційних технологій породили такий вид тероризму як інформаційний. Інформаційний тероризм здійснюється в області, що охоплює політичні, філософські, правові, естетичні, релігійні й інші погляди й ідеї, тобто у духовній сфері, там, де ведеться боротьба ідей. Доступність інформаційних технологій значно підвищує його ризики, бо, чим інформатизованішим є суспільство, тим більше воно піддатливе до впливів масово-психологічного терору. Отже, є підстави говорити про інформаційно-психологічний вплив спрямований на свідомість і душу людини. Об'єктом даного впливу є як окремі особи, групи осіб, так і цілі держави.

Отже, можливо дійти висновку про існування взаємозв'язку між кризою системи публічного управління та збільшенням загрози інформаційного тероризму, що у свою чергу повинно спонукати державні органи до пошуку нових шляхів стабілізації політичної ситуації, вдосконалення державних механізмів протидії інформаційному тероризму як складової загальнодержавної системи антикризового реагування.

Пошук напрямів (шляхів) вдосконалення державного механізму реагування на кризові ситуації та її складової — механізмів протидії інформаційному тероризму, справа не проста і ускладнюється вона, перш за все, налагодженням дієвого механізму координації суб'єктів різної відомчої підпорядкованості зі своїми, визначеними законодавством, завданнями. В цьому

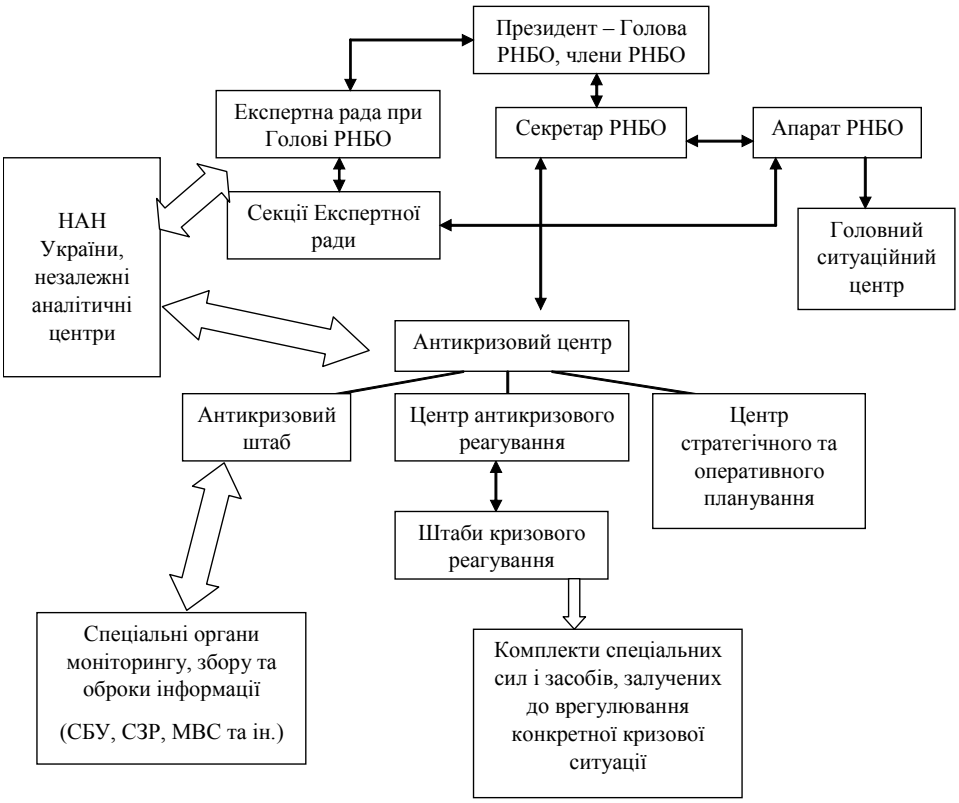

Рис. 1. Модель управлінської ланки реагування на кризові ситуації в Україні

аспекті важливим є дослідження системи ситуаційних центрів.

Так, Указом Президента України від 28.02.2015 № 115/2015 введено в дію рішення Ради національної безпеки і оборони України від 25.01.2015 року "Про створення та забезпечення діяльності Головного ситуаційного центру України" [12]. Мережа ситуаційних центрів створюється на інформаційно-технологічній платформі національного центру управління телекомунікаційними мережами, що забезпечить можливість прийняття оперативних та ефективних управлінських рішень щодо використання ресурсів наявних в державі телекомунікаційних мереж в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, зокрема в інтересах управління державою, забезпечення потреб оборони та безпеки держави.

Створення Головного ситуаційного центру України (далі — ГСЦ) може відіграти основоположну комунікативну роль в рамках створення ефективного механізму протидії інформаційному тероризму як складової загальнодержавної системи антикризового реагування.

З усіх зазначених вище функцій антикризового реагування створення мережі ГСЦ лише частково забезпечує пошук, збір, обробку даних, прийняття рішень, координацію і контроль. Не забезпеченими залишаються: сформований відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" перелік об'єктів захисту, загрози, сценарії їхньої ескалації, спроможності системи національної безпеки; моніторинг, моделювання, прогноз сценаріїв ескалації загроз; планування організації, підготовки, розгортання та застосування сил і засобів; оперативне управління ними.

Це вимагає продовження та поглиблення реформи. Необхідно визначитись з управлінською ланкою, що зможе на основі отриманої інформації, з урахуванням наявних ресурсів сил і засобів напрацьовувати варіанти адресного антикризового реагування та надавати загальній системі варіанти своєчасної та адекватної протидії кризовим явищам і реагування на них (міністерства та відомства, сили, що перебувають у їхньому розпорядженні, відповідають за протидію загрозам у відповідних сферах і мають у своєму складі функціональні модулі, що залучаються до антикризових заходів на випадок комбінованих сценаріїв).

Пропонується наступна модель управлінської ланки реагування на кризові ситуації в Україні (рис. 1).

Функціями Антикризового центру мають бути: структурування проблемних галузей; збір і комплексний аналіз інформації за всіма сферами національної безпеки; моніторинг ескалації загроз; моделювання і прогнозування кризових ситуацій; визначення потрібних спроможностей із запобігання ескалації кризових ситуацій і з реагування на них. Центр стратегічного та оперативного планування має відповідати за підготовку, розробку, експертизу концептуальних і стратегічних документів, законодавчих і підзаконних актів, а також опрацювання оперативних питань, що виносяться на розгляд Президента, ВРУ та РНБО — на замовлення Адміністрації Президента, секретаріатів ВРУ та РНБО. Взаємодія Центру стратегічного та оперативного планування та Антикризового центру із силовими відомствами, іншими органами влади, науковими установами та широким експертним середовищем має забезпечити повноту аналізу всього спектру загроз, раннє їх виявлення, відстеження, попередження про небажаний розвиток подій, можливість запобігти їх ескалації і перетворенню на кризові ситуації. Центр антикризового реагування забезпечує комплексне планування та координацію спільних дій з підготовки та застосування структур системи національної безпеки. У складі Центру створюються ситуативні групи (організаційне ядро штабів) — відповідно до заздалегідь визначених сценаріїв (категорій кризових ситуацій). Вони очолюються особами з числа керівників відповідних міністерств, відомств, силових структур або заступників Секретаря РНБО, відповідальними за врегулювання кризових ситуацій. У докризовому періоді ці групи відповідають за опрацювання документації, необхідної для залучення і спільного застосування потрібних сил і засобів, і підтримують зв'язок з міністерствами, відомствами та визначеними

силами. У випадках проведення операцій із запобігання ескалації загроз і реагування на кризові ситуації ці групи доукомплектовуються до повних штатів відповідних штабів, які починають виконувати функції керівництва спільними діями силових структур з врегулювання криз і ліквідації їхніх наслідків. Прикладами ситуативних груп (штабів) можуть бути Ставка Верховного Головнокомандувача, штаби з подолання наслідків природних лих чи техногенних катастроф, штаби із забезпечення соціально-політичної стабільності під час виборчих кампаній тощо. У їхнє підпорядкування на час підготовки, спільних навчань і проведення антикризових заходів передаються відповідні сили кризового попередження та реагування у складі потрібних функціональних модулів міністерств і відомств. Комплекти сил, до яких залучаються потрібні підрозділи спеціального призначення силових структур, можуть розглядатися як Сили спеціальних операцій. Таким чином, запропонована організаційна структура дає змогу забезпечити функції всього життєвого циклу управлінської ланки та за умов якісного правового, адміністративного, фінансового, кадрового та інформаційного забезпечення — домогтися високого рівня національної безпеки.

Отже, своєчасним наразі є актуалізація питання міжвідомчої взаємодії складових сектору безпеки і оборони та створення сучасних ситуаційних центрів. А проведена в рамках комплексного огляду сектору безпеки і оборони оцінка стану воєнної безпеки держави, а також набутий досвід участі складових сектору безпеки і оборони у антитерористичній операції призвели до створення об'єднаного керівництва силами оборони держави відповідно до Закону України "Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях" [13]. В ньому чітко визначено функціонування об'єднаних сил оборони, здійснюється розподіл відповідальності за формування та застосування сил оборони, що позитивно позначається на здатності керівництва держави здійснювати ефективне управління у сфері оборони; наявність об'єднаного керівництва силами оборони, яке здійснюється відповідно до принципів і стандартів, прийнятих державами-членами НАТО.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Підсумовуючи думку щодо визначення та аналізу державних інституцій (суб'єктів) антикризового реагування в Україні можливо стверджувати про достатні інституціональні засади реагування на кризові ситуації в Україні через суб'єктів антикризового реагування в контексті розглянутого вище вітчизняного законодавства. Проте єдиного, врегульованого вітчизняним законодавством, підходу до з'ясування як сутності кризи, так і до змісту антикризового управління в Україні немає, що безумовно може бути предметом майбутніх досліджень науковців.

Кризові ситуації, які виникають у країні можуть створювати реальну загрозу самозбереженню діючої системи, здійснювати виклик чинній владі, що може призвести до зміни політичного курсу та політичної системи загалом. Кризові процеси підсилюються радикальними діями в інформаційному просторі породжуючи нову форму протиправних дій XXI століття — інформаційний тероризм (кібертероризм). Процеси глобалізації породжують сприйнятливі умови для інформаційного тероризму, нав'язуючи світовій спільноті, а також будь-якій країні свої радикальні ідеї, які у свою чергу можуть спровокувати кризові явища на рівні країни, регіону, світу.

Отже, інформаційний фактор став невід'ємною складовою тероризму як суспільно-політичного явища, а дослідження останнього вказує на необхідність розвитку дієвого антитерористичного механізму (насамперед боротьби з інформаційним тероризмом), як складової загальнодержавної системи антикризового реагування. А на шляху вдосконалення механізмів протидії інформаційному тероризму як складової загальнодержавної системи антикризового реагування має стати створення моделі ефективної управлінської ланки держави, яка зможе керувати наявними ресурсами сил і засобів суб'єктів антикризового реагування під час виникнення будь-яких кризових ситуацій (довготривалих, системних, екстремально-часових) для надання керівництву держави необхідних варіантів антикризового реагування.

Визначені та обгрунтовані пріоритетні напрями аналізу інформаційної безпеки українського суспільства та удосконалення державного механізму реагування на виклики і загрози інформаційного тероризму не можна вважати закінченими. Очевидно, що удосконалення безпекових процесів у цій сфері вимагає подальших фахових дискусій науковців і практиків.

Література:

1. Вікіпедія, Глобалізація [Електронний ресурс]. — Режим доступу: https://uk.wikipedia.org/wiki/%D0%93%D0%BB%D0%BE%D0%B1%D0%B0%D0%BB%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F

2. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції / В. Ліпкан, Ю. Максименко, В. Желіховський [Електронний ресурс]. — Режим доступу: http://mobile.pidruchniki.com/15800119/politologiya/ponyattya_ zmist_zagroz_informatsiyniy_bezpetsi

3. Фурашев В.М. Основні стримуючі фактори правового забезпечення інформаційної безпеки / В.М. Фурашев // Інформація і право. — 2013. — № 2 (8). — С. 117—118.

4. Про Раду національної безпеки і оборони України: Закон України від 05.03.1998 № 183/98-ВР. URL: http://zakon4.rada.gov.ua/laws/show/183/98-вр

5. Про основи національної безпеки України: Закон України від 15.12.2005. — № 3200-IV: http://zakon0.rada.gov.ua/laws/show/964-15

6. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII.: http://zakon3.rada.gov.ua/laws/show/2163-19

7. Про рішення Ради національної безпеки і оборони України від 06.05.2015 "Про Стратегію національної безпеки України": Указ Президента України від 26.05.2015 № 287/2015. URL: http://zakon5.rada.gov.ua/laws/show/287/2015

8. Про рішення Ради національної безпеки і оборони України від 27.01.2016 "Про Стратегію кібербезпеки

України": Указ Президента України від 15.03.2016 № 96/2016. URL: http://zakon5.rada.gov.ua/laws/show/96/2016/paran11#n11

9. Про рішення Ради національної безпеки і оборони України від 02.09.2015 р. "Про нову редакцію Воєнної доктрини України": Указ Президента України від 24.09.2015 № 555/2015. URL: http://zakon4.rada.gov.ua/laws/show/555/2015

10. Про рішення Ради національної безпеки і оборони України від 04.03.2016 "Про Концепцію розвитку сектору безпеки і оборони України": Указ Президента України від 14.03.2016 року № 92/2016. URL: http://zakon4.rada.gov.ua/laws/show/92/2016

11. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII.: http://zakon2.rada.gov.ua/laws/show/2469-19

12. Про рішення Ради національної безпеки і оборони України від 25.01.2015 "Про створення та забезпечення діяльності Головного ситуаційного центру України": Указ Президента України від 28.02.2015 № 115/2015. URL: http://www.president.gov.ua/documents/1152015-18567

13. Про особливості державної політики із забезпечення державного суверени терту України на тимчасово окупованих територіях у Донецькій та Луганській областях: Закон України від 18.01.2018 № 2268-VIII.: http://zakon0.rada.gov.ua/laws/show/2268-19/page1

References:

1. wikipedija (2018), "Globalization", available at: https://uk.wikipedia.org/wiki/%D0%93%D0%BB%D0%BE%D0%B1%D0%B0%D0%BB%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F (Accessed 15 Aug 2018).

2. Lipkan V. Maksymenko, Ju. Zhelikhovsjkyj V. (2006), "Information security of Ukraine in the conditions of European integration", available at: http://mobile.pidruchniki.com/15800119/politologiya/ponyattya_-zmist_zagroz_informatsiyniy_bezpetsi (Accessed 15 Aug 2018).

3. Furashev, V.M. (2013), "The main constraints of the legal security of information security", Informacija i pravo, vol. 2 (8), pp. 117—118.

4. Verkhovna Rada of Ukraine (1998), The Law of Ukraine "On Council of National Security and Defense of Ukraine", available at: http://zakon4.rada.gov.ua/laws/show/183/98-vr (Accessed 15 Aug 2018).

5. Verkhovna Rada of Ukraine (2005), The Law of Ukraine "On the Fundamentals of National Security of Ukraine", available at: http://zakon0.rada.gov.ua/laws/show/964-15 (Accessed 15 Aug 2018).

6. Verkhovna Rada of Ukraine (2017), The Law of Ukraine "About the basic principles of providing cyber security of Ukraine", available at: http://zakon3.rada.gov.ua/laws/show/2163-19 (Accessed 15 Aug 2018).

7. President of Ukraine (2015), Decree "On the decision of the National Security and Defense Council of Ukraine dated 05/06/2015 "On the Strategy of National Security of Ukraine"", available at: http://zakon5.rada.gov.ua/laws/show/287/2015 (Accessed 15 Aug 2018).

8. President of Ukraine (2016), Decree "On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016 "On the Strategy of Cybersecurity of Ukraine"", available at: http://zakon5.rada.gov.ua/laws/show/96/2016/paran11#n11 (Accessed 15 Aug 2018).

9. President of Ukraine (2015), Decree "On the decision of the National Security and Defense Council of Ukraine dated 02.09.2015 "On the new edition of the Military Doctrine of Ukraine"", available at: http://zakon4.rada.gov.ua/laws/show/555/2015 (Accessed 15 Aug 2018).

10. President of Ukraine (2016), Decree "On the decision of the National Security and Defense Council of Ukraine dated March 4, 2016 "On the Concept of Development of the Security and Defense Sector of Ukraine"", available at: http://zakon4.rada.gov.ua/laws/show/92/2016 (Accessed 15 Aug 2018).

11. Verkhovna Rada of Ukraine (2018), The Law of Ukraine "On National Security of Ukraine", available at: http://zakon2.rada.gov.ua/laws/show/2469-19 (Accessed 15 Aug 2018).

12. President of Ukraine (2015), Decree "On the decision of the Council of National Security and Defense of Ukraine dated January 25, 2015 "On Creation and Maintenance of the Main Situational Center of Ukraine"", available at: http://www.president.gov.ua/documents/1152015-18567 (Accessed 15 Aug 2018).

13. Verkhovna Rada of Ukraine (2018), The Law of Ukraine "About the peculiarities of the state policy on ensuring state sovereignty of Ukraine in temporarily occupied territories in the Donetsk and Luhansk oblasts", available at: http://zakon0.rada.gov.ua/laws/show/2268-19/page1 (Accessed 15 Aug 2018).

Стаття надійшла до редакції 17.08.2018 р.