завдань щодо боротьби з тероризмом.

Загалом будь-яка антитерористична діяльність у місцях компактного проживання є залежною від тлумачення категорії «проживання у сім'ї», яка, у свою чергу, дає змогу розглядати як основне завдання забезпечення антитерористичної безпеки в місцях проживання особи перетворення «сім'ї» та суспільних відносин, що наявні в її межах, на джерело антитерористичної безпеки, у т.ч. завдяки на перетворення «проживання у сім'ї» у середовище інформаційно-роз'яснювальної роботи у сфері боротьби з тероризмом. Так, з метою підвищення рівня правової свідомості та обізнаності населення з питань запобігання і припинення терористичної діяльності Служба безпеки України за участю Міністерства внутрішніх справ, Міністерства оборони, Державної служби України з надзвичайних ситуацій, інших суб'єктів, що безпосередньо здійснюють боротьбу з тероризмом, та суб'єктів, що згідно із законодавством залучаються до боротьби з тероризмом зобов'язані забезпечувати: висвітлення в засобах масової інформації заходів з реалізації державної політики у сфері боротьби з тероризмом для формування в суспільстві негативного ставлення до терористичної діяльності в усіх її формах і проявах; своєчасне виявлення та припинення розповсюдження матеріалів із закликами до насильницької зміни, повалення конституційного ладу, захоплення державної влади, до посягання на територіальну цілісність і недоторканність України, до розпалювання національної, расової чи релігійної ворожнечі, ненависті, до вчинення терористичних актів, дій, що загрожують громадському порядку, а також матеріалів, що пропагують расову, національну чи релігійну нетерпимість, дискримінацію; інформування громадськості про розкриті терористичні злочини, їх суспільно небезпечний характер та передбачену законом відповідальність за вчинення таких злочинів, а також про проведення антитерористичних навчань та їх результати; впровадження в діяльність суб'єктів, що безпосередньо здійснюють боротьбу з тероризмом, міжнародного досвіду щодо інформування громадськості про антитерористичні заходи.

При цьому слід зауважити, що відповідне завдання не може суперечити основній меті й завданням розвитку суспільства та є гарантією забезпечення інформаційних прав та свобод членів сім'ї, а також формування на цій основі системи інформаційних ресурсів забезпечення антитерористичної безпеки.

Статичне забезпечення антитерористичної безпеки на рівні сім'ї пов'язана із врегулювання каналів «передавання» третій особі (суб'єкту боротьби з тероризмом або установі чи організації, що залучена до заходів боротьби із тероризмом) інформації, зміст якої свідчить про навмисні дії спрямовані на розпалювання національної, расової чи релігійної ворожнечі, ненависті, призов до вчинення терористичних актів, дій, що загрожують громадському порядку, а також матеріалів, що пропагують расову, національну чи релігійну нетерпимість, дискримінацію в місцях компактного проживання.

Додатковим елементом моделі статичного забезпечення антитерористичної безпеки на рівні «проживання в сім'ї» є механізми отримання відповідних відомостей з джерел поза місцями проживання та реєстрації.

Андрій Собакарь,
завідувач кафедри адміністративного права,
процесу та адміністративної діяльності
Дніпропетровського державного
університету внутрішніх справ
доктор юридичних наук, професор

ВИКОРИСТАННЯ ДОСВІДУ США У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

В умовах світової соціально-культурної кризи людство опинилося перед необхідністю формування нової парадигми забезпечення національної безпеки, переосмислення традиційних уявлень про її сутність і способи забезпечення з урахуванням соціально-політичних та етноконфесійних чинників.

Одним з найбільш важливих завдань забезпечення національної безпеки будь-якої країни був і залишатиметься захист об'єктів критично важливої інфраструктури. Останній

включає вжиття заходів, які повинні забезпечити їх збереження через різні впливи природного або техногенного характеру.

Однією із перших країн, що почала активно впроваджувати заходи із забезпечення безпеки та захисту об'єктів критично важливої для країни інфраструктури є США, фахівці якої до переліку загроз критичній інфраструктурі відносять зловмисні дії (зловмисні дії груп або окремих осіб, таких як терористи і злочинці), природні небезпеки (урагани, торнадо, землетруси, цунамі, повені та ін.) і техногенні надзвичайні ситуації (авіаційні катастрофи, ядерні аварії, пожежі, аварії у системах енергозабезпечення, викиди небезпечних речовин тощо) [1].

За американським законодавством критична інфраструктура розділена на 16 секторів: хімічна галузь; зв'язок; виробництво; шлюзи і греблі; військово-промисловий комплекс, екстрені служби, енергетика, фінансовий сектор, харчова промисловість і сільське господарство; державні установи; охорона здоров'я; ядерні реактори і ядерні відходи; транспортна інфраструктура; система водопостачання та водовідведення, а також комерційний сектор. Цікаво, що до комерційного сектору критичної інфраструктури американські законодавці віднесли будь-які комерційні об'єкти у сфері бізнесу, торгівлі, розваг або проживання, в яких перебуває «велике скупчення людей». До речі, схоже визначення для таких комерційних об'єктів існує і в законодавстві України. Так, у статті 32 Закону України «Про регулювання містобудівної діяльності» усі об'єкти будівництва розділено на три класи наслідків (відповідальності): незначні наслідки – СС1, середні наслідки – СС2 і значні наслідки – СС3. За аналогією з американським законодавством, саме об'єкти комерційної нерухомості з класом наслідків СС3 (ТРЦ і Бізнес-центри), можна було б віднести до критичної інфраструктури України в комерційному секторі [2].

Головною метою створення державної системи запобігання та протидії загрозам критичної інфраструктури в США стала необхідність значного підвищення рівня взаємодії різних державних органів та суб'єктів господарювання, що було реалізовано шляхом утворення комісії із захисту критичної інфраструктури при президентові США

Американська системи захисту об'єктів критичної інфраструктури включає розробку необхідної законодавчої основи, значний обсяг фінансування, освіту необхідних суб'єктів управління та підпорядкування їм надзвичайних служб, оснащення необхідними технічними та програмними засобами.

Важлива роль у регулюванні питань організації захисту об'єктів критичної інфраструктури в США належить актам президента, серед яких слід виділити:

– адміністративні накази № 13010 «Про роботу з дослідження вразливості захисту критичної інфраструктури від кібернетичних і фізичних загроз» (липень 1996 р.); № 13228 «Організація захисту США від терористичних загроз» (жовтень 2001 р.) та № 13231 «Про захист національних критичних інформаційних систем» (жовтень 2001 р.);

– указ президента США № 13636 «Удосконалення кібербезпеки критичної інфраструктури» (лютий 2013 р.);

– президентська політична Директива 8 «Національна готовність» (березень 2011 р.);

– президентська Директива 7 з питань внутрішньої безпеки «Ідентифікація, пріоритетизація та захист критичної інфраструктури» (грудень 2003 р.) тощо.

Окремо слід виділити президентську політичну Директиву 21 «Безпека та стійкість критичної інфраструктури» (лютий 2013 р.), якою було визначено створення в системі Міністерства внутрішньої безпеки двох національних центрів критичної інфраструктури, що мають кожен свою сферу відповідальності, відповідно (фізичні об'єкти критичної інфраструктури і об'єкти кіберінфраструктури), до сфери відповідальності яких було включено інформаційне забезпечення і аналіз. В названому документі було поставлено ряд завдань, спрямованих на вдосконалення захисту і життєздатності об'єктів критичної інфраструктури, в тому числі, пов'язаних із посиленням ролі розвідки і контррозвідки щодо запобігання терористичним актам [3, с. 85].

Більше того, США у 2018 році кардинально переглянули підходи до убезпечення власної критичної інфраструктури, що пов'язано із безпосередньою загрозою китайських інвестицій в критично важливі інфраструктурні об'єкти, шляхом прийняття в серпні 2018 року закону, який чітко закріпив ключовий інваріант підходу до регулювання іноземного інвестування в економіку США: іноземні інвестиції повинні оцінюватися через призму відповідності інтересам забезпечення національної безпеки в їх традиційному розумінні

Корисним для України поряд із необхідністю формування належної законодавчої ба-

зи захисту об'єктів критично важливої інфраструктури, може стати запозичення позитивної практики США створення багаторівневої системи секторального та міжсекторального партнерства, зокрема:

1) урядові координувальні ради (Government Coordinating Councils), призначені для координування виконання урядових стратегій, програм та забезпечення зв'язків між урядовими органами;

2) секторальні координувальні ради (Sector Coordinating Councils), що утворюються на добровільній основі та призначені для координації виконання стратегій і здійснення відповідної діяльності власників та операторів об'єктів і систем критично важливої інфраструктури;

3) міжсекторальні ради (Cross-Sector Councils) – створено три структури: Партнерство для безпеки критичної інфраструктури (координує діяльність представників приватного сектору); Рада вищих федеральних керівників (Federal Senior Leadership Council), призначення якої – координувати інтереси федеральних органів; Рада координації діяльності штатів, місцевих органів управління, призначена для координації всіх інших державних органів нефедерального рівня [4].

Забезпечення безпеки критично важливої інфраструктури в США здійснюється через створену систему стратегічного керівництва, яка в структурному плані є організаційно-технічною єдністю вищих державних та інших органів, технічних систем і засобів управління і зв'язку, побудованої за принципами: єдиного уявлення обстановки в усіх ланках системи управління; можливості отримання відео, аудіо або графічної інформації з будь-якого терміналу системи з глобально розподілених баз даних; можливості організації автоматизованої високошвидкісної передачі даних між будь-якими засобами автоматизації управління, в тому числі й тих, які входять до складу інформаційних систем різних органів; безпосередньої передачі даних про загрозу об'єкта критичної інфраструктури в будь-яку точку, організації державно-приватного партнерства, якому, до речі, приділяється значна увага, зокрема передбачена необхідність учасників-партнерів колективно визначати національні пріоритети та формулювати чіткі заходи задля пом'якшення ризиків, прогнозувати та аналізувати прогрес і вигоду та відслідковувати зворотний зв'язок. У свою чергу, національний план є формою організації національних зусиль, він сприяє прогресу на основі залучення широкого кола учасників-партнерів з різних рівнів урядової гілки влади, приватних та некомерційних секторів, у тому числі й громадянського суспільства, до розуміння важливості забезпечення безпеки і стійкості критично важливої інфраструктури [5].

Таким чином, передовий досвід США дає можливість запозичення кращих тенденцій забезпечення безпеки критичної інфраструктури в українських реаліях сьогодення з огляду на військові загрози таким об'єктам, в тому числі розташованим на окупованій території України. Водночас повне копіювання якогось одного варіанту побудови системи захисту критичної інфраструктури в Україні здається неприємним, адже кожний з них враховує менталітет населення, територіальні особливості розташування об'єктів критичної інфраструктури, повноваження центральних та місцевих органів влади, розвиненість державно-приватного партнерства, наявні загрози об'єктам тощо.

1. Бірюков Д.С., Кондратов С.І., Насвіт О.І., Суходоля О.М. Зелена книга з питань захисту критичної інфраструктури в Україні: Національний інститут стратегічних досліджень, 2015 URL: http://www.dut.edu.ua/uploads/l_428_42547724.pdf

2. Валерій Жуков Захист критичної інфраструктури: досвід США. URL: https://ig-security.tech/zahist-kritichnoi-infrastrukturi-dosvid-ssha.html

3. Ковалева Т.К. Критическая инфраструктура в системе обеспечения национальной безопасности США. Инновации и инвестиции. 2019. № 9. С. 81-89.

4. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналіт. доп. / [Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М.] / за заг. ред. О.М. Суходолі. К.: НІСД, 2019. 224 с.

5. Єрменчук О.П., Пальчик М.Л. Проблемні аспекти правового регулювання державно-приватного партнерства у сфері захисту критичної інфраструктури URL: http://www.academy.ssu.gov.ua/ua/page/page_1581342397.htm.