відповідальність, діяти ініціативно та ефективно, що і відпрацьовується під час занять гуртку. Виховання та підготовка майбутніх правоохоронців через екстремальні ситуації має дуже ефективну результативність. Польові виїзди з ночівлею, багатокілометрові марші з випробуваннями, опрацювання нових способів ведення вогняного контакту у тирі, тренування штурму різних будівель, альпіністська підготовка, подолання різних смуг перешкод, маскування, дії в умовах екстремальних температур та недостатньої видимості, тактична акробатика, подолання водних перешкод, паркур, вольтижировка, екстремальне водіння, стрибки з парашутом не тільки гартували гуртківців але і давали можливість на практиці випробувати набуті під час тренувань навички. Після кожного тактичного виходу або виїзду члени гуртку на засіданні аналізують результати та визначають висновки і основні напрямки щодо покращення свої дій.

Окремо необхідно сказати про відпрацювання можливого вогняного контакту. Найбільш приближений спосіб опрацювання цієї ситуації, це пейнтбол. Члени гуртку приймали участь у багатьох експериментах з залученням пейнтбольного обладнання: у одноповерхових та багатоповерхових будівлях, у лісі, на великих майданчиках з великою кількістю супротивників (загальна кількість до 1000 учасників), в ночі, узимку, під дощем, під час висотних переправ, при моделюванні отримання поранення, з учасниками бойових дій та спецпризначенцями. Ними розроблялися загальна тактика, тактичні ходи, схеми бою і корегувалися під час змагань. Крім того з 2008 року ТСП «Щит» приймає участь у першості Харківської пейнтбольної ліги спортивного та тактичного пейнтболу. Вони ставали неодноразово переможцями на етапах першості та у загальному заліку. Майбутні правоохоронці успішно захищають честь нашого університету у двобої з професіональними спортсменами.

Психологічна підготовка спрямована на забезпечення особистої безпеки правоохоронців та на підвищення ефективності виконання службово-бойових задач. Для цього розроблені методики підвищення боєздатності та боєготовності бійців, так, наприклад, методика емоційної реабілітації дозволяє значно підвищити ці дві якості правоохоронців за малий час і без великих зусиль. На гуртку розроблені тестові завдання, які постійно опрацьовуються, визначається рівень розвитку кожного гуртківця та обирається суто індивідуальний підхід щодо удосконалення його бойових якостей.

Багаторічний досвід роботи гуртку вказує на підвищену ефективність цієї діяльності у сфері підготовки професіональних майбутніх правоохоронців. Методики та методи діяльності гуртку потребують поширення та використання у навчальному процесі вищих навчальних закладів системи МВС. Діяльність науково-практичного гуртку кафедри Тактичної і спеціальної фізичної підготовки багатогранна і має певні традиції, зневажати та не підтримувати які кожне покоління гуртківців не має право. Тільки повна віддача, прагнення перемоги та науковий підхід дає змогу підтримувати високий рівень готовності та самовіддачі курсантів та студентів ТСП «Щит».

Одержано 29.10.2019

УДК 341:351.862.4

Андрій Васильович ВОЙЦІХОВСЬКИЙ,
кандидат юридичних наук, доцент,
професор кафедри конституційного і міжнародного права факультету № 4
Харківського національного університету внутрішніх справ;
https://orcid.org/0000-0001-5629-8852

ПИТАННЯ ФОРМУВАННЯ МІЖНАРОДНО-ПРАВОВОГО МЕХАНІЗМУ ПРОТИДІЇ ЗАГРОЗАМ КРИТИЧНІЙ ІНФРАСТРУКТУРІ

Критична інфраструктура стала одним із найбільш часто обговорюваних у міжнародній спільноті питань. У розвинутих країнах, що займають значимі в світі позиції щодо розвитку системи інфраструктури, питання, пов'язані із забезпеченням захисту його від криз, ризиків і загроз, є одними з найбільш актуальних на порядку денному.

Критична інфраструктура є життєво важливою структурою, тобто найнеобхіднішою, винятковою, стратегічно орієнтованою структурою, що забезпечує життєдіяльність держави. Існують певні критерії, завдяки яким інфраструктури стають «критично» значущими. Найважливіші з них: навіть короткочасне порушення діяльності і функцій об'єктів може призвести до серйозних ризиків для держави і суспільства, а також, до економічних втрат. Ланцюгова реакція катастрофи, викликаної аварією, є свого роду «ефектом метелика», який може паралізувати діяльність всього суспільства, поширившись за «принципом доміно» на інші галузі.

На сьогодні в більшості зарубіжних країн захист критичної інфраструктури став одним із пріоритетних напрямків забезпечення безпеки. З цією метою були створені і постійно вдосконалюються різноманітні системи захисту об'єктів критичної інфраструктури.

Критично важлива інфраструктура має ключове значення для публічного порядку, економічної стабільності і національної безпеки держав, тому це питання відноситься до компетенції держави. При цьому, найбільш уразливі в цій галузі є саме розвинені країни.

Значна частина об'єктів критичної інфраструктури знаходиться у власності приватного бізнесу, тому держава і приватний сектор змушені спільно нести відповідальність за безпеку і стабільне функціонування об'єктів критичної інфраструктури.

Значимість захисту критичної інфраструктури зростає по ряду причин, серед яких:

– широке поширення технологій, в тому числі, з метою забезпечення ефективної роботи більшості об'єктів критичної інфраструктури, систем держави і бізнесу;

– зростаюча залежність суспільства і держави від нормального функціонування об'єктів критичної інфраструктури;

– зростання складності, а, отже, уразливості складової критичної інфраструктури. Складні системи чутливі не лише по відношенню до кібератак, вони також схильні до збоїв в роботі через помилки в програмному забезпеченні, помилки в діях персоналу тощо. Виявити

справжню причину неполадок як правило буває дуже непросто.

Серед науковців робилися неодноразові спроби щодо вироблення загальноприйнятого визначення терміна «критично важлива інфраструктура», проте вони не увінчалися успіхом. На сьогоднішній день держави самостійно визначають, що відносити до об'єктів критично важливої інфраструктури. Перелік об'єктів життєво важливої інфраструктури різниться у тих чи інших країнах і визначається відповідно до традицій, суспільних і політичних причин, а також географічними та історичними особливостями кожної країни [1, с. 155–156].

Поняття «критична інфраструктура» було вперше використано в назві створеної в жовтні 1996 року за рішенням Президента США «Комісії по захисту критичної інфраструктури». Визначення «критичної інфраструктури» в «патріотичному Акті» (2001 р.), прийнятому після терактів 11 вересня в США звучить так: «об'єднання систем і засобів, надзвичайно важливих для держави, вихід з ладу або знищення яких може призвести до дуже тяжких наслідків для національної безпеки, економіки, охорони здоров'я та інших галузей» [2].

В Європі поняття критичної інфраструктури почали використовувати з 1998 року через посилення загрози терористичних атак. Першою про захист системи телекомунікації, банківського і фінансового сектора, водопостачання, енергозбереження та інших систем, які забезпечують життєдіяльність країни і її економічний потенціал, заговорила Великобританія, визначивши основні параметри критичної інфраструктури та відповідальність певних державних органів щодо її захисту.

Відповідно до Директиви 2008/114/ЄС про ідентифікацію та позначення європейської критичної інфраструктури та оцінювання необхідності покращення їх охорони та захисту, прийнятій Радою Європи 8 грудня 2008 року під критичною інфраструктурою розуміється «об'єкт, система, або її частина, розташована в державах-членах, що є суттєвою для підтримки життєво важливих громадських функцій, здоров'я, безпеки, захищеності, економічного або соціального добробуту населення, пошкодження або знищення якої матиме значний вплив у державі-члені через неспроможність такої інфраструктури підтримувати згадані функції» [3].

Головною характеристикою критичної інфраструктури є її ключове значення для безпеки суспільства і держави. Критично важливі інфраструктури можуть бути військовими і цивільними об'єктами, а також мати подвійне призначення.

У Резолюції Ради Безпеки ООН S/RES/2341 (2017) «Про захист критичної інфраструктури» від 13 лютого 2017 року зазначається, що «кожна держава сама визначає, які об'єкти його інфраструктури є критично важливими і як забезпечити їх ефективний захист…» [4]. Таким чином, сегменти інфраструктури, визначені в різних країнах, можуть відрізнятися від звичайного усвідомлення «стратегічних об'єктів». Наприклад, в США ця сфера, поряд з об'єктами, що забезпечують життєдіяльність суспільства, також включає в себе «Національні пам'ятники (статуї) і історичні площі», «Виборчу систему», дипломатичні місії, які також можуть стати об'єктом кібератак в інших країнах тощо.

На основі порівнянь міжнародного досвіду можемо визначити, що до системи критичної інфраструктури відносяться наступні об'єкти: державні органи влади, сільське господарство і продовольство, водні ресурси, охорона здоров'я, структури аварійної служби, військова промисловість, енергетика, нафта/газ, багатогранна транспортна/ логістична система, що включає в себе перевезення та доставку – авіація, залізничний транспорт, автошляхи, морські перевезення (морський транспорт), трубопроводи, метрополітен (як засіб масового перевезення громадян), банківські та фінансові послуги, поштові послуги, національні пам'ятники, атомні електростанції, комерційні об'єкти тощо.

У вищезгаданій Директиві 2008/114/ЄС основні напрямки захисту систем критичної інфраструктури держав-членів визначаються як: «інфраструктура, пошкодження або знищення якої матиме істотний вплив щонайменше на дві держави-членів» [3]. У Директиві до цієї системи відносять не лише «жорсткі» матеріально-фізичні, але й «м'які» соціальні, не матеріальні інфраструктури (інфраструктура ідентифікації та довіри, інфраструктура відкритих даних, інфраструктура онлайн-розрахунків та транзакцій, інфраструктура електронної комерції та онлайн-взаємодії суб'єктів бізнесу, інфраструктура державних послуг (електронне урядування), інфраструктура життєзабезпечення (медицина, освіта, громадська безпека, транспорт тощо), промислові цифрові інфраструктури тощо.

У розвинених країнах в умовах формування «цифрової економіки» спостерігається все більш широке поширення мережевої, інформаційної критичної інфраструктури. До об'єктів такої інфраструктури почали відносити як національну, так і міжнародну інформаційну критичну інфраструктуру, серед яких розрізняють системи доменних імен мережі Інтернет, комунікаційні супутники, міжконтинентальні кабелі та маршрутизатори тощо.

По ряду причин інформаційна критична інфраструктура є більш уразливою. Складність і взаємозалежність інформаційних систем призводить до того, що наслідки порушення їх нормальної роботи можуть бути непередбачуваними, в найгіршому варіанті викликати «ефект доміно». Таким чином, саме вплив на критичну інформаційну інфраструктуру є найбільш небезпечним для суспільства і цивільного населення, може спровокувати заворушення, нестабільність, хвилювання тощо. [1, с. 156–157]

Після трагічних подій 11 вересня 2001 року у Сполучених Штатах питання захисту критичної інфраструктури від терористичної загрози набуло особливої актуальності для європейських держав.

Так, у жовтні 2004 року Комісія Європейського Союзу розробила загальну методологію захисту критичної інфраструктури та рекомендувала посилити увагу на технологічних й інформаційних елементах захисту тих об'єктів, припинення функціонування яких матиме транскордонний плив. Створення інформаційної мережі попередження про критичну інфраструктуру (European Critical Infrastructure Warning Information Network, CIWIN) є одним із заходів, передбачених для сприяння реалізації Європейської програми захисту критичної інфраструктури (European Programme for Critical Infrastructure Protection, EPCIP). Програма спрямована на допомогу державам-членам та Комісії Європейського Союзу в обміні інформацією про спільні загрози, вразливості та відповідні заходи та стратегії для зменшення ризику для підтримки захисту критичної інфраструктури [5].

З метою вироблення спільних механізмів протидії загрозам критичної інфраструктури Європейський Союз налагоджує співробітництво з Організацією Північноатлантичного договору. У Спільній Декларації про співробітництво, підписаній на Брюссельському Саміті (11–12 липня 2018 р.), ЄС і НАТО визначили інфраструктуру в якості ключової галузі [6].

Для нашої держави є корисним досвід європейських сусідніх країн щодо законодавчого закріплення захисту критичної інфраструктури. Наприклад, уряд Словаччини у 2007 році ухвалив «Концепцію критичної інфраструктури Словацької Республіки, її захисту та оборони», де визначено загальну стратегію захисту життєво важливих об'єктів, але немає детального плану дій у кризових ситуаціях.

Вже у 2011 року було прийнято закон про критичну інфраструктуру Словацької Республіки, котрий чітко визначає об'єкти критичної інфраструктури, державні органи, що відповідають за захист останніх, а також детальний план заходів у разі виникнення надзвичайної ситуації.

У 2007 року польський уряд ухвалив закон про управління кризовими ситуаціями, в рамках якого подано чітке розуміння параметрів критичної інфраструктури та її захисту.

Угорщина у 2012 року прийняла закон про захист критичної інфраструктури, котрий можна назвати одним із найбільш комплексних документів у цій царині. Власне, закон чітко визначив порядок і принципи зарахування об'єктів до категорії критичної інфраструктури, умови забезпечення їхньої безпеки, проведення інспекцій, а також механізм взаємодії між державними інституціями у критичних ситуаціях, створення резервних ресурсних фондів тощо. Більш того, в Угорщині енергетику в розрізі критичної інфраструктури розглядають як особливу сферу, котра регулюється окремим урядовим наказом [7].

Зважаючи на серйозність загроз, що нині постали перед національною безпекою нашої держави, необхідно активізувати роботу державних органів щодо розробки і прийняття нормативно-правової основи, яка б регламентувала захист критичної інфраструктури.

За своїм географічним положенням Україна є частиною Європи, а отже, прямо пов'язана з європейською критичною інфраструктурою, саме тому український уряд повинен розвивати діалог з ЄС у питаннях протидії загрозам національної критичної інфраструктури (насамперед, енергетичної, інформаційної тощо). Окрім того, потрібно більш детально вивчити досвід розвинутих країн (США, Великобританія, Німеччина тощо), які вже мають законодавче поле щодо захисту критичної інфраструктури, та максимально використати їхній досвід у національній законотворчості.

Спираючись на досвід підготовки зелених книг в ЄС та у країнах-членів НАТО у 2015 році була опублікована Зелена книга з питань захисту критичної інфраструктури в Україні – збірник матеріалів міжнародних експертів з питань захисту критичної інфраструктури, підготовлений у Національному інституті стратегічних досліджень із залученням українських та зарубіжних експертів. У Зеленій книзі сформульовані стратегічні цілі державної політики в сфері захисту критичної інфраструктури в Україні, принципи побудови системи захисту критичної інфраструктури та завдання такої системи. На основі вивчення досвіду країн-членів ЄС та НАТО з урахуванням безпекової ситуації в Україні та особливостей розбудови елементів сектору безпеки країни були сформульовані першочергові кроки із побудови державної системи захисту критичної інфраструктури в Україні [8].

6 грудня 2017 року Кабінет Міністрів України опублікував Концепцію створення державної системи захисту критичної інфраструктури [9], яка стала основою для створення державної системи захисту об'єктів критичної інфраструктури, порушення роботи яких може завдати шкоди національним інтересам України. У ній наведено визначення усіх ключових понять та запропоновано механізм взаємодії державних органів.

Завдання практичної реалізації нових підходів у протидії загрозам критичної інфраструктури було закріплено прийнятим 21 червня 2018 року Законом України «Про національну безпеку України». Крім того, здійснюється підготовка проєкту Закону «Про критичну інфраструктуру та її захист», який дозволить забезпечити створення необхідної для цього законодавчої бази. У разі прийняття цей Закон закріпить принципи та напрями розбудови державної системи захисту критичної інфраструктури, визначить правові та організаційні засади забезпечення її діяльності і стане складовою частиною законодавства України у сфері національної безпеки.

Висновок. Підсумовуючи викладене, можемо зазначити, що питання протидії загрозам критичної інфраструктури вимагає зусиль усього міжнародного співтовариства щодо розробки і здійснення максимально ефективного міжнародно-правового механізму. Цей механізм включає розробку, прийняття і вдосконалення необхідної міжнародно-правової основи з регламентації протидії загрозам критичної інфраструктури, а також активізацію діяльності в цьому напрямку провідних міжнародних організацій (ООН, ЄС, ОБСЄ, НАТО тощо). Забезпечення захисту

об'єктів критичної інфраструктури повинно стати визначальним напрямом державної політики, у тому числі й України, від якого залежатиме існування самої держави, її національна безпека, соціально-економічний розвиток та відповідне місце у світовому співтоваристві.

Список бібліографічних посилань

1. Коротков А. В., Зиновьева Е. С. Безопасность критических информационных инфраструктур в международном гуманитарном праве. *Вестник МГИМО Университета. Серия: Политология.* 2011. № 4 (19). С. 154–162. URL: https://cyberleninka.ru/article/n/bezopasnost-kriticheskih-informatsionnyh-infrastruktur-v-mezhdunarodnom-gumanitarnom-prave (дата звернення: 17.10.2019).

2. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. H.R. 3162. URL: https://www.congress.gov/bill/107th-congress/house-bill/3162?q= %7B %22search %22 %3A %22Uniting+and+Strengthening+America+by+Providing+Appropriate+Tools+Required+to+Intercept+Obstruct+Terrorism+Act %22 %7D&r=9 (дата звернення: 17.10.2019).

3. COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. *Official Journal of the European Union.* 2008. L 345/77-82 URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF (дата звернення: 18.10.2019).

4. Про захист критичної інфраструктури : резолюція Ради Безпеки ООН від 13.02.2017 № S/RES/2341 (2017) // Організація Об'єднаних Націй : офіц. портал. URL: https://undocs.org/ru/S/RES/2341(2017) (дата звернення: 18.10.2019).

5. Critical Infrastructure Protection (EPCIP) // European Commission. URL: https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en (дата звернення: 18.10.2019).

6. Joint Declaration on EU-NATO Cooperation: signed at the NATO Summit in Brussels (11–12 July 2018) // North Atlantic Treaty Organization. URL: https://www.nato.int/cps/en/natohq/official_texts_156626.htm?selectedLocale=ru (дата звернення: 18.10.2019).

7. Слободян Н. «Критична інфраструктура» – досвід ЄС проти диверсійної війни // Європейська правда : сайт. 07.07.2015. URL: https://www.eurointegration.com.ua/experts/2015/07/7/7035609/ (дата звернення: 18.10.2019).

8. Бірюков Д. С., Кондратов С. І., Насвіт О. І., Суходоля О. М. Зелена книга з питань захисту критичної інфраструктури в Україні. Київ, 2015. 35 с. URL: http://www.dut.edu.ua/uploads/l_428_42547724.pdf (дата звернення: 19.10.2019).

9. Концепція створення державної системи захисту критичної інфраструктури : схвал. розпорядженням Кабінету Міністрів України від 06.12.2017 № 1009-р // Урядовий портал. URL: https://www.kmu.gov.ua/ua/npas/pro-shvalennya-koncepciyi-stvorennya-derzhavnoyi-sistemi-zahistu-kritichnoyi-infrastrukturi (дата звернення: 19.10.2019).

Одержано 23.10.2019

УДК 343.93(477)

Уляна Богданівна ВОРОБЕЛЬ,
аспірантка кафедри цивільно-правових дисциплін юридичного факультету
Львівського державного університету внутрішніх справ;
https://orcid.org/0000-0003-0480-5394

НАСЛІДКИ ЗАЛИШЕННЯ ЗАЛИ СУДОВОГО ЗАСІДАННЯ ПОЗИВАЧЕМ (НА МАТЕРІАЛАХ СУДОВОЇ ПРАКТИКИ)

Із прийняттям Закону України «Про *внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів*» [1] законодавець суттєво змінив підхід щодо трактування наслідків неявки учасників справи в судове засідання або його залишення. Так, відповідно до ч. 1 ст. 223 Цивільного процесуального кодексу України (далі – ЦПК України) [2] неявка у судове засідання будь-якого учасника справи за умови, що його належним чином повідомлено про дату, час і місце цього засідання, не перешкоджає розгляду справи по суті, крім випадків, визначених ст. 223 ЦПК України.

Якщо учасник справи або його представник були належним чином повідомлені про судове засідання, суд розглядає справу за відсутності такого учасника справи у разі: 1) неявки в судове засідання учасника справи (його представника) без поважних причин або без повідомлення причин неявки; 2) повторної неявки в судове засідання учасника справи (його представника), крім відповідача, незалежно від причин неявки; 3) неявки представника в судове засідання, якщо в судове засідання з'явилася особа, яку він представляє, або інший її представник; 4) неявки в судове засідання учасника справи, якщо з'явився його представник, окрім випадків, коли суд визнав явку учасника справи обов'язковою (ч. 3 ст. 223 ЦПК України).

У разі повторної неявки позивача в судове засідання без поважних причин або неповідомлення ним про причини неявки суд залишає позовну заяву без розгляду, крім випадку, якщо від нього надійшла заява про розгляд справи за його відсутності, і його нез'явлення не перешкоджає вирішенню спору (ч. 5 ст. 223 ЦПК України).

Відповідно до ч. 6 ст. 223 ЦПК України, у разі, якщо учасник справи (його представник) залишить залу судового засідання, настають наслідки, визначені ч. 3–5 ст. 223 ЦПК України. Системно-логічне тлумачення частин цієї статті,