УДК 351.741+347.73

Організаційно-правові засади забезпечення техногенної безпеки в умовах зростання терористичної загрози

Павлов Дмитро Миколайович –
заступник начальника кафедри економіко-правових дисциплін Національної академії внутрішніх справ, кандидат юридичних наук, доцент

Стаття присвячена аналізу правових та організаційних проблем забезпечення техногенної безпеки і захисту критичної інфраструктури держави в умовах зростання військової та терористичної загрози, питанням реформування сектору безпеки і оборони та підвищення ефективності цивільного захисту в Україні з урахуванням специфіки його здійснення в умовах проведення антитерористичної операції. Досліджується стан правового регулювання діяльності суб'єктів забезпечення техногенної безпеки, питання організації взаємодії в цій сфері.

Ключові слова: цивільний захист, тероризм, технологічний тероризм, критична інфраструктура, техногенна безпека.

Постановка проблеми. З моменту проголошення незалежності Україна розвивалася як держава, зовнішня та внутрішня політика якої мала абсолютно неагресивний характер. У 2014 році, внаслідок ескалації соціально-політичних і військових загроз, різко зросли ризики надзвичайних ситуацій техногенного характеру, в тому числі пов'язані зі збоєм або некомпетентним втручанням у системи управління виробництвом й інфраструктурою. Адже, як слушно відзначає Ю. Костюченко, кризовий регіон – Донбас – є найбільш техногенно навантаженою територією України. У практично кожному населеному пункті розташовано хоча б один потенційно небезпечний об'єкт, щільність інфраструктури – спадку минулої мобілізаційної індустріалізації – є тут надмірною, зношення основних фондів досягає в середньому більше 60–75 % (за найскромнішими оцінками), а умови захисту шкідливих виробництв і зберігання відходів – більш ніж у 80 % випадків не відповідають сучасним нормам безпеки [1].

Розміщення населення, джерел водопостачання, комунікації і шляхів евакуації відносно джерел небезпеки є очевидно незбалансованим. А у зв'язку із загальною економічною депресивністю регіону і драматичними поточними подіями, наявність і доступність засобів захисту і порятунку населення – очевидно низькі.

Все це буквально означає, що загальна вразливість регіону по відношенню до загроз техногенного характеру (з урахуванням спровокованих ескалацією соціально-політичних і військових ризиків) виросла до неприйнятної межі. Іншими словами, ризик катастрофи критично зростає, при зростаючій імовірності техногенної аварії. Такого типу різнорідні взаємопов'язані ризики в сучасній теорії безпеки мають назву когерентних або системних ризиків, а пов'язані з ними катастрофи є найбільш руйнівними за наслідками і непередбачуваними.

Зважаючи на специфіку дій терористів, аналітики навіть припускають, що загрози, пов'язані з техногенною компонентою безпеки, на сьогодні – найзначиміші. Тому на захист об'єктів критичної інфраструктури при проведенні антитерористичних операцій слід направляти окремі суттєві зусилля [1].

Аналіз останніх публікацій за темою дослідження. Дослідженню проблематики правового регулювання забезпечення техногенної безпеки увагу приділяли у своїх працях такі вітчизняні вчені, як Ю. Ю. Азаров, А. І. Берлач, С. С. Засунько, В. К. Колпаков, С. Ф. Константінов, О. В. Копан, С. О. Кузніченко, О. В. Кузьменко, О. П. Рябченко, Л. А. Жукова, М. М. Козяр, М. Я. Откідач, О. О. Труш, А. Г. Чубенко та інші. В той же час, спеціальні дослідження забезпечення техногенної безпеки від загроз терористичного характеру відсутні, що обумовлює необхідність здійснення активного наукового пошуку в цьому напрямі.

Метою статті є теоретико-правовий аналіз особливостей забезпечення техногенної безпеки від загроз терористичного характеру, розробка на цій основі пропозицій до законодавства.

Виклад основного матеріалу. Термін "критична інфраструктура" ще не отримав свого визначення у національному законодавстві, він, де-факто, вже використовується. За відсутності дефініції терміну "критична інфраструктура" у національному законодавстві у подальшому

розгляді будемо спиратися на його визначення в законодавстві США, які першими серед інших країн почали розвивати і втілювати в життя відповідний концептуальний підхід.

В американському законодавстві під критичною інфраструктурою розуміються "системи та ресурси, фізичні чи віртуальні, настільки життєво важливі для Сполучених Штатів, що недієздатність або знищення таких систем чи ресурсів підриває національну безпеку, національну економіку, здоров'я або безпеку населення, або має своїм результатом будь-яку комбінацію з переліченого" (USA PATRIOT Act, 2001) [2].

Факторами, які впливають на рівень терористичної загрози, є функціонування на території України диверсійно-привабливих об'єктів підвищеної небезпеки, значна кількість яких виступають об'єктами критичної інфраструктури, та незадовільний рівень фізичної охорони вказаних об'єктів.

До об'єктів техносфери, що мають найвищий ступінь небезпеки і можуть стати метою терористичних груп, відносяться: чотири атомні електростанції (Запорізька, Рівненська, Південно-Українська, Хмельницька АЕС); Чорнобильська АЕС та зона відчуження; гідроелектростанції ДАК "Укргідроенерго" (Дніпровська ГЕС, Дніпродзержинська ГЕС, Каховська ГЕС, Кременчуцька ГЕС, Канівська ГЕС, каскад Київських ГЕС, малі та середні ГЕС Дністровського каскаду) греблі, відкриті розподільчі пристрої; дослідницькі ядерні реактори в Київському інституті ядерних досліджень і Севастопольському інституті ядерної енергії та промисловості; хімічно небезпечні об'єкти 1-го ступеня небезпеки, вибухо- і пожежонебезпечні об'єкти, транспортні вузли, магістральні трубопроводи, військові склади і бази.

Сьогодні одним із самих небезпечних підприємств у хімічній галузі з точки зору техногенної небезпеки та вразливості до терористичних актів є виробниче об'єднання "Трансаміак", яке здійснює диспетчерське управління української частини аміакопроводу "Тольятті-Одеса", забезпечує його безпечне та безперебійне функціонування. Організувати належну охорону диспетчерської кімнати, де знаходиться весь обсяг інформації відносно районів розміщення аміакопроводу, процесів його функціонування, стану ремонтних робіт тощо, практично неможливо у зв'язку з відсутністю в "Укрхімтрансаміак" окремого спеціально обладнаного приміщення. Вказані обставини створюють сприятливі умови для захоплення щита управління аміакопроводом і здійснення терористичних і диверсійних актів [3].

Крім цього, в Україні зосереджена велика кількість інших хімічних виробництв, яке є диверсійно-уразливим. Це такі, як: ПАТ "Концерн "Стирол" (м. Горлівка Донецької області), ПАТ "Рівнеазот" (м. Рівне), ПАТ "Черкасиазот" (м. Черкаси), ПАТ "Дніпроазот" (м. Дніпродзержинськ Дніпропетровської області), Одеський державний припортовий завод (ОДПЗ, м. Одеса), ПАТ "Лисичанська сода" (м. Луганськ), ДГХП "Сірка" (м. Розділ Івано-Франківської області), ДГХП "Сірка" (м. Яворів Львівської області).

Техногенні аварії в результаті терористичних проявів на зазначених об'єктах можуть призвести до катастрофічних наслідків як для екології України, так і сусідніх держав, травмування та загибелі великої кількості людей.

Крім того, об'єктами підвищеної терористичної уразливості є шлюзи Дніпровського каскаду, їх безпечне функціонування є важливою складовою техногенно-екологічної та економічної безпеки країни. Проте, внаслідок недостатнього фінансування, система охорони шлюзів працює незадовільно.

Крім того, в окремих випадках, функції охорони шлюзів виконують непідготовлені особи, переважно пенсійного віку, які неспроможні забезпечити належну їх охорону, що призводить до несанкціонованого проникнення на територію, яка охороняється, сторонніх осіб, крадіжок державного майна та пошкодження устаткування.

Неналежний стан системи охорони судноплавних шлюзів може бути використаний для проведення терористичних і диверсійних акцій з настанням тяжких наслідків для населення та суб'єктів господарювання.

Враховуючи акумуляцію в Дніпровському каскаді значних об'ємів водних ресурсів, руйнування будь-якого шлюзу може призвести до виникнення ланцюгової реакції руйнувань на інших гідротехнічних спорудах, розташованих нижче за течією, і, як наслідок, до затоплення значних територій та населених пунктів поблизу р. Дніпро [3].

Відзначимо, що не слід недооцінювати або ігнорувати загрозу диверсій та терористичних актів на згаданих вище об'єктах. Адже сучасні події на сході України експерти називають гібридною війною. Гібридна війна (англ. Hybrid warfare) – це змішання класичного ведення війни з використанням нерегулярних збройних формувань. Держава, яка веде гібридну війну, здійснює операцію з недержавними виконавцями – бойовиками, групами місцевого населення, організаціями, зв'язок з якими формально повністю заперечується. Ці виконавці можуть робити такі речі, які сама країна робити не може, тому що будь-яка держава зобов'язана слідувати Женевській конвенції та Гаазькій конвенції про закони сухопутної війни, домовленостям з іншими країнами [4]. В таких умовах існує висока вірогідність вчинення терористичних актів з метою дестабілізації ситуації у мирних регіонах або з метою залякування населення.

Адже, до загроз, які включає в себе гібридна війна, фахівці відносять: традиційні, нестандартні, катастрофічний тероризм і підривні загрози, коли використовуються технології для протидії перевазі у військовій силі [4]. Полковник Армії США Джек МакКуен визначив гібридну війну як основний метод дій в асиметричній війні, що ведеться на трьох напрямках:

1. Серед населення конфліктної зони.

2. Тилового населення.

3. Міжнародної спільноти [5].

Девід Кілкаллен, автор книги "Випадкова герилья" (англ. "The Accidental Guerilla"), стверджує, що гібридна війна – це краще визначення сучасних конфліктів, але підкреслює, що вона включає в себе комбінацію партизанської та громадянської воєн, а також заколоту і тероризму [4].

Журналіст Френк Хоффман визначає гібридну війну у вигляді будь-яких дій ворога, який миттєво й злагоджено використовує складну комбінацію – дозволену зброю, партизанську війну, тероризм і злочинну поведінку на полі бою, щоб домогтися політичних цілей [5]. Тому одним із елементів гібридної війни виступає технологічний тероризм. Відповідно до норм чинного законодавства технологічний тероризм – це злочини, що вчиняються з терористичною метою із застосуванням ядерної, хімічної, бактеріологічної (біологічної) та іншої зброї масового ураження або її компонентів, інших шкідливих для здоров'я людей речовин, засобів електромагнітної дії, комп'ютерних систем і комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об'єктів, які прямо чи опосередковано створили або загрожують виникненням надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру [6].

Останнім часом відмічається підвищена увага до проблеми так званого "електромагнітного тероризму" [7]. Під цим терміном мається на увазі використання електротехнічних пристроїв для створення електромагнітного випромінювання і полів високої напруги з метою впливу на конкретні технічні засоби і системи, внаслідок чого буде дезорганізована їхня робота або повне виведення з ладу. На думку зарубіжних фахівців, "електромагнітний тероризм", який може бути елементом ведення інформаційної війни недружніми країнами, є новим, досить небезпечним видом тероризму з огляду на масштаби можливих наслідків для державної інфраструктури. За оцінками західних експертів у галузі інформаційної безпеки, державні системи управління і зв'язку європейських країн недостатньо захищені від впливу електромагнітних випромінювань і є потенційними об'єктами "інформаційної агресії". Таким чином, поруч із ядерним, хімічним, біологічним та іншими видами сучасного тероризму, "електромагнітний тероризм" як складова "інформаційного тероризму" став реальним і небезпечним явищем, оскільки має можливість таємно впливати на технічні системи державного управління та об'єкти інфраструктури [7].

Відсутність необхідного рівня визначеності воєнної та антитерористичної політики України, тобто недостатня конкретність відповідей на питання стосовно терористичних і воєнних загроз, сценаріїв протидії та союзників у ній, призвели до неадекватного визначення потрібних сил і засобів збройної боротьби та постійних коливань у реформуванні Збройних Сил (ЗС), МВС та Національної гвардії, інших суб'єктів забезпечення національної безпеки і оборони.

При оцінці ризиків, пов'язаних із загрозами природного, техногенного та соціально-політичного (в т.ч. терористичного) характеру виявляється, що найбільш складним завданням є оцінка саме терористичних ризиків, що обумовлено самою природою інформації та даних, які використовуються при цьому. В сучасних умовах, що характеризуються тенденцією до наростання загроз тероризму на тлі глобальних кризових процесів у фінансово-економічній сфері, актуальність проблеми оцінки терористичних ризиків для критичної інфраструктури загострилася ще більше, адже без оцінки ризиків не можливе їх ефективне зниження.

Важливою особливістю, яку слід брати до уваги при розробці та застосуванні методологічних підходів до оцінки терористичних ризиків у сфері техногенної безпеки, зокрема в нашій країні, є те, що різні сфери забезпечення життєдіяльності держави мають занадто різний досвід урахування загроз тероризму. Наприклад, на оборонних та ядерних об'єктах, на авіатранспорті історія урахування загроз зловмисних дій в т.ч. терористичного характеру, налічує десятки років, то, наприклад, у нашій країні для трубопровідного та деяких інших видів транспорту терористичні акти не розглядаються як можлива причина надзвичайних ситуацій, що можуть призвести до важких наслідків, включаючи людські жертви. З огляду на це, існує потреба внесення відповідних змін до Закону України "Про трубопровідний транспорт" [8].

Крім того, необхідно суттєво корегувати нормативно-правові акти, присвячені регламентації повноважень суб'єктів сектору безпеки і оборони у сфері протидії технологічному тероризму. Виправданим є чітке закріплення функцій та завдань підрозділів МВС, у тому числі Національної гвардії, щодо забезпечення техногенної безпеки та збереження критичної інфраструктури держави.

Висновки. Підсумовуючи викладене вище, маємо відзначити, що нормативно-правове регулювання в сфері забезпечення техногенної безпеки та протидії технологічному тероризму не має в своїй основі загальної стратегії. Існує потреба негайного корегування законодавства у цій сфері з урахуванням принципової зміни характеру загроз військово-терористичного характеру, перетворення їх з потенційних на абсолютно реальні. Забезпечення техногенної безпеки та захист об'єктів критичної інфраструктури має стати пріоритетом політики у сфері національної безпеки, адже у ситуації, що склалася, наслідки від терористичних актів можуть становити загрозу життю та здоров'ю мільйонів людей.

Звідси виникає гостра необхідність у приведенні всіх актів у галузі безпеки та передбачуваних програм і проектів у цій сфері в єдину систему, усуненні прогалин, повторів і суперечностей, встановленні належної кореляції між ними. Першим кроком у цьому напрямі має стати розробка

та прийняття Концепції реформування сектору безпеки і оборони в Україні, яка повинна містити характеристику загроз у цій сфері та визначати рівень їх небезпеки; критерії оцінки загроз; основні елементи системи забезпечення громадської безпеки та напрями діяльності суб'єктів цієї системи, механізм координації та взаємодії між ними, показники ефективності їх діяльності; особливості фінансового забезпечення заходів у сфері громадської безпеки. У ній повинна бути також визначена довгострокова стратегія розвитку даної системи, побудована з урахуванням існуючих і потенційних загроз, факторів соціально-економічного характеру, а також конкретно визначено суб'єкт, відповідальний за реалізацію цієї стратегії.

Крім того, ми підтримуємо наступні пропозиції щодо вдосконалення існуючої системи реагування на надзвичайні ситуації (соціальні загрози та тероризм) з урахуванням оцінки ймовірності виникнення та особливостей реалізації цих загроз у майбутньому:

– внесення змін до Статуту Національної гвардії щодо дій в разі проникнення через зовнішній периметр охорони ядерного об'єкту [3], а також інших об'єктів критичної інфраструктури, які характеризуються високою привабливістю для актів технологічного тероризму;

– розробка та впровадження надійної системи технічної охорони та фізичного захисту об'єктів підвищеної небезпеки;

– забезпечення контролю за технічним станом засобів виробництва та своєчасним проведенням регламентних робіт на об'єктах підвищеної небезпеки;

– розробка дієвих планів ліквідації наслідків техногенних аварій на об'єктах підвищеної небезпеки;

– удосконалення існуючої системи обліку та контролю за радіоактивними відходами;

– постійного наукового супроводу систем обліку та контролю радіоактивних відходів [3].

При розробці методологічних підходів до оцінки ризиків терористичних загроз національній критичній інфраструктурі доцільно використовувати зарубіжний і національний досвід, набутий на інших напрямах контртерористичної діяльності, насамперед, у сфері протидії ядерному тероризму [8].

Крім того, в сучасних умовах виникла необхідність відмови від розуміння забезпечення техногенної безпеки виключно як напрямку забезпечення функції цивільного захисту населення і територій від наслідків надзвичайних ситуацій.

Перспективи подальшого використання. Використання у правотворчій та правозастосовній практиці вказаних вище висновків має сприяти підвищенню ефективності правової регламентації забезпечення техногенної безпеки від загроз терористичного характеру.

Список використаних джерел

1. Костюченко Ю. Когерентна катастрофа: про палаючі заводи і здоровий глузд [Електронний ресурс] / Ю. Костюченко. – Режим доступу : http://espreso.tv/blogs/2014/06/10/koherentna_katastrofa_pro_palayuchi_zavody_i_zdorovyy_hluzd.

2. USA PATRIOT Act, 2001 / [Electronic resource]. – Mode of access : http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.

3. Національна доповідь про стан техногенної та природної безпеки у 2012 році / [Електронний ресурс]. – Режим доступу : http://www.mns.gov.ua/files/prognoz/report/2012/3_9_2012.pdf.

4. Гибридная война. Материалы из Википедии – свободной энциклопедии / [Электронный ресурс]. – Режим доступа : https://ru.wikipedia.org/wiki_cite_note-AFJ-4.

5. Hybrid vs. compound war / [Electronic resource]. – Mode of access : http://www.armedforcesjournal.com/2009/10/4198658/.

6. Про боротьбу з тероризмом : Закон України від 20 берез. 2003 р. № 638 // Відомості Верховної Ради України. – 2003. – № 25. – Ст. 180.

7. Кравченко В. И. Электромагнитный терроризм [Текст] / В. И. Кравченко ; М-во образования и науки, молодежи и спорта Украины. Нац. техн. ун-т "Харьк. политехн. ин-т". – Харьков : "НТМТ", 2012. – 390 с.

8. Щодо оцінки ризиків та загроз тероризму для елементів критичної інфраструктури держави : аналітична записка [Електронний ресурс] / Нац. ін-т стратег. досл. при Президентові України. – Режим доступу : http://www.niss.gov.ua/articles/1205/.

Статья посвящена анализу правовых и организационных проблем техногенной безопасности и защиты критической инфраструктуры государства в условиях роста военной и террористической угрозы, вопросам реформирования сектора безопасности и обороны и повышения эффективности гражданской защиты в Украине с учетом специфики его осуществления в условиях проведения антитеррористической операции. Исследуется состояние правового регулирования деятельности субъектов обеспечения техногенной безопасности, вопросы организации взаимодействия в этой сфере.

This article analyzes the legal and organizational problems of technogenic safety and protection of the critical infrastructure of the state in terms of its military and terrorist threats, security sector reform and defense and improve the efficiency of civil protection in Ukraine, taking into account the specifics of its implementation in terms of counter-terrorism operations. We investigate the state of the legal regulation of technogenic safety issues of cooperation in this area.

Стаття надійшла до редакції журналу 18 листопада 2014 року.