УДК: 351/354 + 338.24.021.8

ПРІОРИТЕТИ ФОРМУВАННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАХИСТУ КРИТИЧНОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Суходоля Олександр Михайлович,
доктор наук з державного управління, доцент

Розглянуто актуальні завдання та проблеми захисту критичної енергетичної інфраструктури. Визначено методологічні засади формування та пріоритети реалізації державної політики України у цій сфері.

Ключові слова: **енергетична безпека, державна політика, захист критичної інфраструктури, захист енергетичної інфраструктури**

З кінця XX ст. завдання захисту важливої інфраструктури життєдіяльності суспільства стало одним з найважливіших пріоритетів національної безпеки та почало знаходити своє відображення в політиці низки країн. Проте нині тільки у США та ЄС концепцію захисту критичної інфраструктури вмонтовано в загальну стратегію безпеки, а її пріоритети відображено в державній політиці національної безпеки та відповідному законодавстві.

Актуальність питань формування цілісної політики США в цій сфері була обумовлена низкою непередбачуваних за своїми наслідками катастрофічних подій, таких як терористичні атаки 11 вересня 2001 р. чи ураган Катріна 2005 р. Аналіз наслідків цих подій, масштаби завданої суспільству шкоди та їх вплив на життєдіяльність країни вказали на необхідність посилення захисту критичної інфраструктури життєзабезпечення суспільства та надання більшої уваги цим питанням.

Виділення сфери та предмета діяльності системи державного управління з питань захисту критичної інфраструктури стало можливим завдяки визначенню поняття «критична інфраструктура». Наприклад, у законодавстві США воно трактується як «системи та об'єкти, фізичні чи віртуальні, настільки життєво важливі для держави, що недієспроможність або знищення таких систем чи об'єктів підриває національну безпеку, економіку, здоров'я чи безпеку населення або має своїм результатом будь-яку комбінацію з названого» (*Patriot Act*, 2001) [1, 2].

Подальший розвиток законодавства у цій сфері та результати практичної реалізації нового напряму державної політики вимагають підвищення уваги до забезпечення фізичного захисту об'єктів критичної інфраструктури, сталості виконання функції та надання послуг[1], які нею забезпечуються.

Інфраструктура систем енергозабезпечення також традиційно належить до критичної інфраструктури. Однак нині вагомість сталого функціонування саме енергетичної інфраструктури суттєво зросла. Зазначена ситуація зумовлена не тільки роллю, яку вона відіграє для забезпечення звичного нам стилю життя, а й використання окремими країнами та недержавними гравцями «енергетичної зброї» для досягнення своїх цілей далеко за межами енергетичної сфери.

Так, порушення функціонування окремих систем постачання електроенергії, нафти чи природного газу неодноразово використовувалося Росією для досягнення мети в політичній та економічній сферах на теренах СНД. Зокрема, В. П. Горбулін наводить низку прикладів щодо таких випадків [3]. Наприклад, у січні 2006 р. синхронні підриви енергетичної інфраструктури, які припинили постачання природного газу та електроенергії до Грузії, збіглися з періодом активізації політико-економічного тиску Росії на цю країну. У квітні 2009 р. порушення технологічного режиму функціонування основного експортного газопроводу з Туркменістану, яке призвело до його вибуху, «допомогло» Росії

[1] Наприклад, енергетичний сектор. Основна функція (послуга) цього сектору полягає в забезпеченні потреб суспільства в енергії. Якщо акцент робиться на енергетичних об'єктах і системах, то за такого підходу без належного аналізу до критично важливої інфраструктури можуть потрапити переважно об'єкти електрогенерації, тоді як об'єкти системи електропостачання є більш важливими для забезпечення послуг з електропостачання кінцевих споживачів. Як свідчить світовий досвід, найтяжчі наслідки для забезпечення суспільства електроенергією спричинені аваріями в системах передачі та розподілення електроенергії, а не у випадку виходу з ладу одного чи кількох об'єктів генерації.

призупинити дію незручного для неї договору з цією країною та фактично усунути конкурента з європейського ринку. Пошкодження та майбутній тривалий ремонт нафтопроводу, що забезпечував постачання нафти з Росії на нафтопереробний завод у Мажейкяй у Литві, використовувалося російськими компаніями як аргумент під час вирішення комерційного питання – приватизації цього заводу.

Останнім часом значно посилилися загрози сталому функціонуванню енергетичної інфраструктури через зростання терористичної активності. За даними проекту «Загрози енергетичній інфраструктурі» Цюріхського Центру дослідження проблем безпеки з 1980 по 2010 роки було ідентифіковано 8 тис. атак проти енергетичної інфраструктури [4]. Загалом за останні 10 років щорічно відбувалося в середньому по 327 таких атак. При цьому спостерігається і активізація атак недержавних гравців проти енергетичної інфраструктури, і поступове зникнення раніше чіткого розмежування мотивів цих атак (кримінальних, політичних, воєнних, економічних). Нині дедалі частіше вони мають на меті отримання економічних прибутків та впливу на динаміку цін на енергетичних ринках (на енергоресурси, страхові платежі, видатки на охорону тощо).

Для України актуальність загроз функціонування енергетичної інфраструктури було продемонстровано низкою актів тероризму проти інфраструктурних об'єктів, спричинених російською агресією, та захопленням окремих об'єктів паливно-енергетичного комплексу нашої держави в Автономній Республіці Крим (всієї енергетичної інфраструктури на півострові та на шельфі Чорного моря, газорозподільної станції в Херсонській області), а також вибухами на магістральних газопроводах і захоплення пунктів управління ними [5]. Саме тому питання захисту енергетичної інфраструктури нині вийшло за межі проблем лише суб'єктів господарювання та, крім того, з'являється розуміння необхідності формування державної політики у цій сфері.

Проблеми захисту критичної інфраструктури в межах чинного законодавчого забезпечення

Незважаючи на те, що в українському законодавстві діє низка нормативно-правових актів, якими задекларовано особливий характер функціонування та захисту об'єктів критичної інфраструктури, досі не визначено єдиних методологічних засад формування та практичної реалізації державної політики в цій сфері. Понад те, в законодавстві України відсутній сам термін «критична інфраструктура». Галузеве ж законодавство недостатньо врегульовує питання захисту енергетичної інфраструктури, не забезпечує належної координації та узгодження з іншими пріоритетами забезпечення національної безпеки. А сам предмет діяльності з охорони енергетичної інфраструктури та відповідних завдань визначається на галузевому (відомчому) рівні [5, 6].

Відсутність визначення терміна «критична інфраструктура» та відповідного переліку об'єктів, що відносяться до неї, перешкоджає ефективній діяльності щодо захисту критичної інфраструктури в тому розумінні, якого вимагає сьогодення.

Традиційне фокусування лише на фізичному захисті об'єктів, як це випливає з п. 6 Рішення Ради національної безпеки і оборони України «Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України» від 01 березня 2014 р. (введеного в дію Указом Президента України № 189/2014 від 02.03.2014 р.), передбачає завдання Міністерству внутрішніх справ України лише забезпечити «посилену охорону об'єктів енергетики та критичної інфраструктури». Поза увагою залишаються питання сталого виконання функцій і надання послуг, що забезпечуються енергетичною системою.

Саме функції та послуги, якими забезпечують суспільство й державу об'єкти та системи критичної інфраструктури, мають лежати в основі визначення їх критичності та, відповідно, визначати критерії формування переліку об'єктів, систем та їх елементів критичної інфраструктури, яка потребує захисту[2].

Окремо слід зазначити, що в чинному нормативно-правовому полі України, яким регулюються правовідносини в питаннях, близьких до захисту критичної інфраструктури, акцент робиться не на забезпеченні функціонування систем, здатності до швидкого відновлення функцій, які можуть бути перервані в результаті настання надзвичайної ситуації, а на захисті життя та здоров'я людей та довкілля від шкідливого впливу аварій на цих об'єктах [5].

Водночас пріоритетом системи захисту критичної інфраструктури має стати підвищення її безпеки та стійкості функціонування відносно всього спектра загроз і ризиків з метою гарантування постачання населенню, суспільству, бізнесу й державі життєво важливих товарів і послуг. Для виконання зазначеної функції необхідно гарантувати безперебійне стале функціонування об'єктів критичної інфраструктури у визначених режимах, мати можливість запобігати руйнуванню чи завданню невиправної шкоди, припиненню функціонування або втраті контролю над об'єктами внаслідок дії всіх чинників та забезпе-

[2] На сьогодні вже розроблено загальні підходи до формування переліку об'єктів критичної інфраструктури, що базуються на використанні таких характеристик, як географічне охоплення території; взаємозв'язок між елементами критичної інфраструктури; тривалість впливу; вразливість об'єкта до впливу небезпечних чинників; важкість можливих наслідків.

чувати швидке відновлення їх функціонування в разі, якщо воно було перерване.

У даному контексті слід підкреслити необхідність переорієнтування діяльності у цій сфері на запобігання виникненню загроз функціонуванню критичної інфраструктури. Відповідно, доцільно класифікувати загрози критичній інфраструктурі за джерелами їх формування визначаючи оцінки рівня можливого цілеспрямованого впливу умовного «суб'єкта загрози», а саме:

• *небезпечні природні явища* – загрози, які можуть реалізуватися незалежно від бажання умовного суб'єкта дії;

• *аварії й технічні збої* – загрози, спричинені технологічними обставинами, можуть сформуватися за опосередкованого впливу суб'єкта зловмисної дії (недогляд чи помилка проектування, недбалість і порушення режиму функціонування);

• *зловмисні дії* – загрози, спричинені цілеспрямованими діями суб'єкта.

Окремо слід зазначити, що загрози також доцільно розглядати не лише з погляду характеру їх походження, а й виділення елементів критичної інфраструктури, на які ці загрози спрямовані:

• *фізичні елементи*, зокрема обладнання та ресурси об'єктів критичної інфраструктури;

• *системи управління та комунікації*, зокрема системи автоматичного управління та регулювання роботи об'єктів, системи зв'язку тощо;

• *персонал об'єктів*, зокрема диспетчерський, оперативний, що безпосередньо забезпечує функціонування критичної інфраструктури в реальному часі.

Така класифікація загроз і спрямованості їх дії методологічно дає змогу більш системно підійти до формування державної політики та організації системи захисту на рівні операторів критичної інфраструктури. У планах захисту критичної інфраструктури, розроблених операторами, погоджених і схвалених відповідними державними органами, мають бути докладно описані заходи протидії загрозам за такими напрямами [7]:

• *фізичний захист* – спрямований на забезпечення захищеності об'єктів від несанкціонованого доступу, попередження та припинення диверсій, крадіжки або будь-якого іншого незаконного вилучення обладнання, пристроїв та матеріалів;

• *технічний захист* – підвищення відмовостійкості й живучості систем, функціональне резервування;

• *персонал* – підготовка та перевірка, захищеність, контроль здатності персоналу до виконання визначених функцій;

• *інформаційні технології* – захист систем управління, комунікації та інформаційного забезпечення;

• *юридичний захист* – врегулювання питань реагування персоналу та функціонування інфраструктури у кризових ситуаціях, закріплення розподілу відповідальності в нормативних і правових документах, розроблення посібників та інструкцій для персоналу, зокрема щодо взаємодії в умовах кризової ситуації;

• *плани відновлення* – створення планів, резервів та сервісів для швидкого відновлення втрачених функцій.

З огляду на пріоритети розвитку паливно-енергетичного комплексу України, зокрема щодо конкуренції та підтримки різних форм власності, слід виходити з того, що органи державної виконавчої влади не будуть безпосередньо здійснювати керівництво діяльністю суб'єктів господарювання. Відповідно, для формування системи захисту критичної енергетичної інфраструктури необхідно на законодавчому рівні чітко визначити функції та завдання органів державної влади й суб'єктів господарювання різних форм власності.

Загалом, у більшості розвинених країн світу основна відповідальність за безпеку об'єктів/систем критичної інфраструктури покладається на їх власників/операторів. Вони мають забезпечувати надійність (*reliability*), живучість (*resistibility*) і стійкість (*resilience*) своїх об'єктів/систем. Держава ж повинна гарантувати належне інформування власників/операторів, створення адекватної нормативно-правової бази та стимулів для інвестування в безпеку критичної інфраструктури, а також умов для збереження конкурентоспроможності бізнесу, що привабить інвестиції в цю сферу.

В умовах зростаючих ризиків і загроз енергетичній безпеці країни, критичній енергетичній інфраструктурі необхідно суттєво переглянути принципи та побудувати нову систему захисту стратегічних об'єктів енергетики. Кінцевою метою має стати багаторівнева, комплексна, добре скоординована система, що охоплює завдання попередження й захисту життєво важливих об'єктів енергетики та враховує особливості функціонування енергетичного сектору в особливий період[3].

Державна політика захисту критичної енергетичної інфраструктури має базуватися на єдиному методологічному підході до організації діяльності, зосередження наявних ресурсів та координації зусиль зацікавлених осіб. Стратегічною метою політики мусить стати формування системи захисту критичної інфраструктури та підвищення її стійкості на основі підходу до

[3] Під особливим періодом у стратегії мається на увазі період функціонування енергетичного сектору України в умовах обмежень, спричинених виникненням надзвичайної ситуації, введенням надзвичайного стану чи особливого періоду. Питання функціонування паливно-енергетичного комплексу в цей період, методів та інструментів його управління та регулювання, порядку переведення в особливий режим функціонування та припинення його застосування потребує законодавчого врегулювання.

управління ризиками, пов'язаними з усіма видами загроз. Потрібно передбачити такі заходи:

- підвищення стійкості критичної інфраструктури до ідентифікованих загроз;
- запобігання загрозам, пов'язаним зі зловмисними діями;
- планування своєчасного реагування на збої у функціонуванні критичної інфраструктури;
- планування швидкого ремонту й відновлення функціонування критичної інфраструктури.

Передусім слід систематизувати розпорошені правові норми та розробити єдиний законодавчий акт щодо захисту енергетичної інфраструктури від зловмисних дій, яким визначити пріоритетні завдання системи захисту, відповідальність відповідних суб'єктів і механізми реалізації політики.

Органи державної влади мають виконувати низку важливих функцій загальнодержавного рівня, насамперед законодавче й нормативно-правове регулювання діяльності у сфері захисту енергетичної інфраструктури; координацію та організаційне забезпечення функціонування єдиної державної системи захисту енергетичної інфраструктури; надання операторам інфраструктури вчасної інформації щодо можливих перспективних загроз і ризиків; об'єднання зусиль зацікавлених осіб (операторів, органів влади, громадськості) для визначення стратегічних пріоритетів і методології організації діяльності, а також мінімізації видатків на функціонування системи.

Необхідним є залучення приватного сектору до забезпечення енергетичної безпеки країни,

Таблиця

Засади державної політики захисту енергетичної інфраструктури

Напрями	Відповідальність та інструменти
Формування системи захисту критичної інфраструктури	Уряд відповідальний за законодавче врегулювання діяльності державної системи захисту енергетичної інфраструктури та координацію зусиль різних суб'єктів у спосіб встановлення вимог до діяльності системи захисту, інформування та обміну інформацією. Оператори енергетичної інфраструктури відповідальні за організаційно-ресурсне забезпечення функціонування системи захисту енергетичної інфраструктури та обмін інформацією відповідно до встановлених вимог. Уряд/оператори енергетичної інфраструктури визначають пріоритети власних дій у своїх стратегічних і програмних документах
Визначення критичної інфраструктури та ідентифікація критичних елементів (об'єктів)	Уряд відповідальний за розроблення методології ідентифікації критичної інфраструктури (вимоги, стандарти, методологія, методики огляду та оцінки), визначення енергетичної інфраструктури та критичних елементів (перелік критичної інфраструктури). Оператори відповідальні за визначення переліку об'єктів захисту й упровадження доведених вимог щодо захисту в операційну діяльність суб'єктів господарювання
Оцінка ризиків інфраструктурі: - оцінка загроз; - оцінка вразливості й наслідків	Уряд відповідальний за здійснення оцінки загроз у контексті загроз національній безпеці, формування методології оцінки ризиків та реагування на загрози. Оператори здійснюють оцінку загроз на технологічному й корпоративному рівнях та відповідають за розроблення паспорта загроз енергетичній інфраструктурі. Уряд/оператори відповідальні за періодичність проведення оцінки в межах стандартизованих вимог
Визначення та вжиття заходів захисту енергетичної інфраструктури	Уряд визначає вимоги до формування плану захисту енергетичної інфраструктури та сприяє операторам у розробленні плану захисту за допомогою затвердження стандартів і керівних принципів діяльності в цій сфері, а також надання інформаційної, технічної та ресурсної підтримки. Оператор розробляє та забезпечує реалізацію плану заходів захисту енергетичної інфраструктури відповідно до встановлених вимог
Забезпечення фізичного захисту у випадках вияву тероризму	Уряд забезпечує фізичний захист об'єктів енергетики в особливий період відповідними військовими підрозділами у випадку цілеспрямованих актів (тероризм, диверсія). Оператори забезпечують охорону та фізичний захист об'єктів енергетики у звичайний період відповідно до встановлених вимог у межах планів захисту
Встановлення джерел фінансування	Уряд визначає принципи розподілу фінансових зобов'язань між державою та операторами. Уряд визначає заходи, які він зобов'язується фінансувати в межах функціонування єдиної системи захисту (забезпечення фізичного захисту від безпосередніх атак, розроблення методології, наукове дослідження та оцінка загроз і методів реагування, розроблення керівних документів тощо). Оператор фінансує виконання плану захисту відповідно до законодавства та визначеної урядом методології покриття видатків
Перегляд та уточнення стратегії безпеки	Уряд та оператори інфраструктури періодично переглядають загрози безпеки, уточнюють цілі та визначають адекватні засоби реалізації політики у спосіб удосконалення методології оцінки загроз, перегляду паспорту загроз і планів захисту

впровадження механізмів узгодження дій органів державної влади та суб'єктів господарювання в кризових ситуаціях.

Суб'єкти господарювання – власники (оператори) об'єктів критичної енергетичної інфраструктури повинні забезпечити ідентифікацію критичної енергетичної інфраструктури й формування переліку об'єктів захисту; розроблення відповідно до встановленої методології паспорта загроз енергетичній інфраструктурі; формування планів захисту критичної інфраструктури та їх узгодження в межах єдиної державної системи захисту.

Для України необхідно законодавчо врегулювати питання державно-приватного партнерства у зазначеній сфері. Потрібно також розробити нормативно-правову базу щодо врегулювання питань взаємних зобов'язань держави й суб'єктів недержавної форми власності, запровадження в діяльність суб'єктів господарювання практики аналізу ризиків і реагування на загрози (*contingency planning*), механізмів та інструментів взаємодії та узгодження дій державних і недержавних суб'єктів господарювання, громадськості, механізму розподілу відповідальності та зобов'язань (зокрема фінансових).

Важливою стратегічною метою політики у цій сфері має стати формування системи обміну та аналізу інформацією, що включає збір, аналіз та усвідомлення інформації щодо загроз і ризиків, вразливостей і характеристик систем захисту елементів критичної інфраструктури, механізмів і процедур реагування тощо.

При цьому варто наголосити на необхідності існування окремого центру, на який буде покладено зазначені функції. Цей елемент системи, з одного боку, має забезпечити сценарний аналіз можливих загроз з метою оцінювання вразливості й потенційних наслідків припинення або руйнування інфраструктури, з іншого – здійснити «розподіл» завдань і формулювання цілей для інших елементів системи. При цьому важливим є визначення джерел фінансування діяльності такого центру, а також питання захисту інформації з обмеженим доступом, що вимагає розроблення певних правил і підготовки персоналу, відповідального за комунікацію та оброблення відповідної інформації.

Важливим є чітке врегулювання безпосереднього забезпечення фізичного захисту об'єктів критичної енергетичної інфраструктури, передусім питань підпорядкованості й повноважень охоронних структур; методів і засобів захисту (в нормальному та особливому режимах функціонування); залучення Збройних Сил України та правоохоронних органів; визначення джерел фінансування. Необхідно усвідомлення правоохоронними органами та Збройними силами України їх ролі й важливості захисту енергетичної інфраструктури [8]. Доцільно імплементувати питання енергетичної безпеки та захисту критичної енергетичної інфраструктури в політику підготовки кадрів, у планування та діяльність правоохоронних органів і Збройних Сил України, військ цивільної оборони.

Загалом необхідно розробити законодавчий акт, у якому слід визначити основні засади функціонування системи захисту енергетичної інфраструктури. У такому документі доцільно відобразити загальні підходи до змісту й напрямів реалізації державної політики в цій сфері, а також коло відповідальності зацікавлених осіб.

Пропозиції щодо зазначених питань наведено у таблиці.

Список використаної літератури

1. *Uniting* and strengthening America by providing appropriate tools required to intercept and obstruct terrorism : USA PATRIOT ACT. – 2001 [Електронний ресурс]. – Режим доступу: http://frwebgate.access.gpo.gov

2. *Бірюков Д. С.* Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні / Д. С. Бірюков, С. І. Кондратов. – К. : НІСД, 2012. – 57 с.

3. *Горбулін* В. П. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу // Дзеркало тижня. – 2015. – № 2.

4. *Energy* Infrastructure Attacks Examined: An Emerging Research Area [Електронний ресурс]. – Режим доступу: http://inec.usip.org/blog/2012/apr/27/energy-infrastructure-attacks-examined-emerging-research-area

5. *Суходоля О. М.* Захист енергетичної інфраструктури: аналіз української законодавчої бази : аналіт. зап. / О. М. Суходоля [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/1568/

6. *Суходоля О. М.* Захист енергетичної інфраструктури: аналіз зарубіжного законодавства : аналіт. зап. / О. М. Суходоля [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/1600/

7. *Бжозовскі К.* План захисту критичної інфраструктури: польський досвід / К. Бжозовскі [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/public/File/2015_table/0226_Bzhozovski_v.pdf

8. *Суходоля О. М.* Проблеми захисту енергетичної інфраструктури в умовах гідридної війни : аналіт. зап. / О. М. Суходоля [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/1891/