НАЦІОНАЛЬНИЙ ІНСТИТУТ СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ

ЗЕЛЕНА КНИГА
З ПИТАНЬ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

Аналітична доповідь

Київ – 2015

УДК 354

Автори:
Д.С. Бірюков, к.т.н., С.І. Кондратов, О.І. Насвіт, О.М.Суходоля, д.деж.упр., доцент

За заг. ред. д.держ.упр., доцента Суходолі О.М.

Електронна версія: http://www.niss.gov.ua
Зелена книга з питань захисту критичної інфраструктури в Україні: аналітична доповідь / Д.С. Бірюков, С.І. Кондратов, О.І. Насвіт, О.М.Суходоля. – К. : НІСД, 2015. – 35 с.

В Зеленій книзі підняті питання створення в Україні системи захисту критичної інфраструктури. 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 процесу реформування елементів сектору безпеки та оборони країни сформульовані першочергові кроки для створення державної системи захисту критичної інфраструктури в Україні.

Зелена книга розроблена відповідно до пункту Річної національної програми співробітництва Україна-НАТО в 2015р.

Передмова

Підготовка та публікація «зелених книг» є поширеною практикою стимулювання і організації професійних дискусій щодо актуальних безпекових проблем і шляхів їх вирішення як на національному, так й на міжнародному рівнях. Як правило видання «зеленої книги» з певної проблематики передує наступному етапу – розробці та виданню офіційного документу, де формулюються основи державної політики, спрямованої на розв’язання окресленої проблеми. Дана зелена книга присвячена питанням захисту критичної інфраструктури в Україні, напряму, що нині посідає важливе місце в забезпеченні національної безпеки країн-членів ЄС та НАТО, і є елементом загальноєвропейської безпекової політики ЄС.

Без сумніву глобальним безпековим змінам, що відбуваються в світі протягом останніх двох десятиліть, властиво виникнення багатьох криз різного походження та характеру. Це свідчить про скорочення горизонту або навіть неспроможність прогнозування в сучасних механізмах управління в сфері безпеки, їх нездатність попереджати малоймовірні надзвичайні ситуації комплексного характеру, такі як терористичні атаки 11 вересня 2001 р. у США, ураган Катріна у США (2005 р.), світова фінансова криза (2008 р.), руйнівні землетрус і цунамі, спричинена ними аварія на АЕС «Фукусіма Дайічі» в Японії (2011 р.), події «арабської весни» (2011 р.), ведення Росією гібридної війни проти України, цьогорічна криза із біженцями в ЄС. Аналіз вказаних та інших масштабних комплексних викликів регіональній і глобальній системам безпеки, винесені з них уроки з усією очевидністю висувають на порядок денний завдання забезпечення захисту критично важливих для існування держави об'єктів, систем та ресурсів (критичної інфраструктури) від усіх видів загроз та їх комбінацій.

Захист критичної інфраструктури як безпековий напрям був започаткований у США ще у період «*холодної війни*», а на початку нинішнього століття став активно розвиватися у провідних країнах світу як відповідь на різке зростання терористичних загроз. Цей безпековий напрям є пріоритетним і для таких міжнародних структур, як ЄС і НАТО, оскільки поруч з тими перевагами та благами, які несуть з собою процеси глобалізації та інформатизації, посилюється економічна, фінансова, технологічна, ресурсна взаємопов’язаність та взаємозалежність між окремими державами, їх об'єднаннями, а також між регіонами світу, що робить сучасне суспільство дуже вразливим до загроз, особливо тих, що спрямовані на «вузлові» пункти згаданих взаємозв'язків.

Усвідомлення зростання терористичних загроз в Європі призвело до того, що Європейська Комісія розробила та у листопаді 2005 р. оприлюднила *Зелену книгу щодо Європейської програми захисту критичної інфраструктури*[1], а згодом, у 2006 р., коли завершився етап консультацій між країнами-членами ЄС, була запроваджена *Європейська програма захисту критичної інфраструктури*[2]. Особливості підходу ЄС, як об'єднання суверенних держав, у подальшому знайшли своє відображення у документі ЄК "*Захист критичної енергетичної та транспортної інфраструктури Європи*" (лютий 2007)[3] та у спеціальній директиві щодо визначення об’єктів критичної інфраструктури та оцінки потреб у підвищенні рівня їхнього захисту (грудень 2008)[4]. Захист критичної інфраструктури енергопостачання було віднесено до числа пріоритетних напрямів забезпечення енергетичної безпеки для держав-членів НАТО та самого Альянсу Декларацією Чиказького саміту (20 травня 2012 р.).

Драматичні події 2014-2015 років в Україні актуалізували для країни питання захисту інфраструктури, об’єктів та систем важливих для життєдіяльності суспільства та сформували потребу створення системи захисту критичної інфраструктури в Україні. Вважаємо, що гармонізація підходів щодо її створення з тими, що активно запроваджуються в ЄС та НАТО сприятиме удосконаленню механізмів забезпечення національної безпеки та посилить потенціал нашої держави стосовно інтеграції до європейського безпекового простору. Біфуркаційний характер поточного історичного моменту відкриває перед нашою країною коридор додаткових можливостей для зменшення відставання від провідних країн світу і для знаходження свого місця у системі європейської колективної безпеки, ревізія якої вже почалася.

У зв'язку з цим, спираючись на досвід підготовки зелених книг в ЄС та у країнах-членах НАТО у Національному інституті стратегічних досліджень (далі – НІСД) було ініційовано розробку проекту Зеленої книги з питань захисту критичної інфраструктури в України.

Розробка Зеленої книги з питань захисту критичної інфраструктури в Україні здійснювалася за підтримки Офісу зв’язку НАТО в Україні у рамках виконання Річної національної програми співробітництва Україна-НАТО на 2014 рік та 2015 рік. Робота над Зеленою книгою була виконана у НІСД за активної участі залучених вітчизняних і зарубіжних експертів.

Зокрема, при підготовці проекту Зеленої книги були використані результати роботи створеної при Національному інституті стратегічних досліджень (далі – НІСД) у 2011 р. Міжвідомчої експертної робочої групи (МЕРГ) з питань протидії загрозам розповсюдження зброї та матеріалів масового знищення, а також пов’язаних з ними терористичних загроз і захисту критично важливої для забезпечення життєдіяльності держави інфраструктури, підготовленої НІСД аналітичної доповіді[i], висновки та рекомендації проведеного НІСД у липні 2012 р. круглого столу з даної тематики, а також міжнародної науково-практичної конференції «Концепція захисту критичної інфраструктури: стан, проблеми та перспективи її впровадження в Україні» (листопад 2013 р.), організованої НІСД спільно з Офісом зв’язку НАТО в Україні та ПАТ «Укргідроенерго».

Були враховані численні пропозиції від вітчизняних та іноземних експертів. Ми щиро дякуємо за активну участь в опрацюванні положень Зеленої книги вітчизняним експертам: В.М.Білоконю, В.Ф.Гречанінову, О.М.Євдіну, В.А.Заславському, В.І.Лучкову, М.В.Сунгуровському, О.М.Фалю, а також іноземним експертам: Валерію Ратчеву та Тодору Тагареву (Женевський Центр демократичного контролю над збройними силами), Кшиштофу Бжозовскі (Урядовий центр безпеки, Польща), Мартіну Лінхарту (Офіс зв’язку НАТО в Україні), Крістіану Папстхарту (Федеральне міністерство внутрішніх справ, Німеччина), Моніці Джон-Кох (Федеральний офіс цивільного захисту та допомоги в надзвичайних ситуаціях, Німеччина), Хейке Яксону (Центр передового досвіду НАТО з енергетичної безпеки).

Обговорення тексту проекту Зеленої книги експертами, врахування пропозицій, надісланих заінтересованими державними органами, підприємствами, науковими і науково-дослідними інститутами дозволило НІСД представити фінальну версію Зеленої книги з питань захисту критичної інфраструктури в України на міжнародній експертній нараді 15-16 жовтня 2015 року.

---

[i] Бірюков Д.С. Кондратов С.І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. - К.: НІСД, 2012. - 57 с.

Зміст

1. Вступ

Нині Українська держава протистоїть найсерйознішому безпековому виклику за роки своєї незалежності. Гостра соціально-політична криза в умовах іноземного військового втручання у внутрішні справи України, різке посилення екстремізму та тероризму, небувалий ріст злочинності, у т.ч. із використанням зброї, падіння економіки та зростання масштабів гуманітарної кризи у східних регіонах країни, руйнування та пошкодження численних підприємств, інфраструктурних об’єктів – все це визначає ті новітні реалії, в яких сьогодні існує Україна, і в яких має забезпечуватися безпека її громадян, суспільства і державних інституцій.

Цілком очевидно, що сектор безпеки України потребує докорінного реформування, яке має відбуватися з урахуванням світового досвіду та проголошеного курсу на євроінтеграцію. Зазначені чинники у теперішніх умовах роблять особливо актуальним запровадження в нашій державі концептуального поняття «захист критичної інфраструктури», яке активно використовується у провідних країнах Заходу, країнах-членах ЄС та НАТО як один із сучасних інструментів реалізації безпекової політики.

Терміном «критична інфраструктура», зазвичай, охоплюються ті об’єкти, системи, мережі або їх частини, порушення функціонування або руйнування яких призведе до найсерйозніших наслідків для соціальної та економічної сфери держави, негативно вплине на рівень її обороноздатності та національної безпеки. Крім того, функціонування критичної інфраструктури в мирний час пов’язується із підтримуванням життєво важливих функцій в суспільстві, захистом базових потреб його членів і формуванням у них відчуття безпеки і захищеності.

Як і в інших країнах, в Україні існують такі системи, об'єкти та ресурси, знищення або пошкодження яких матиме істотний негативний вплив на громадян, суспільство і державні інституції. При цьому було б невірно стверджувати, що в нашій країні не приділяється увага їх захисту та безпеці. Навпаки, на сьогоднішній день діє ціла низка законодавчих і нормативних актів, що визначають повноваження та компетенцію державних органів у цій та суміжних сферах, встановлюють особливості забезпечення охорони та безпечного функціонування зазначених об’єктів і систем. Проте, в Україні й досі відсутній системний підхід на національному рівні до управління захистом та безпекою усього комплексу таких систем, об'єктів та ресурсів, з врахуванням взаємопов’язаності об’єктів, які прийнято відносити до критичної інфраструктури. Крім того досі відсутній механізм попередження можливих кризових ситуацій, що пов’язані із функціонуванням критичної інфраструктури.

Впровадження такого механізму потребує ґрунтовного вивчення існуючої практики забезпечення захисту об’єктів критичної інфраструктури в Україні, що нині характеризується домінування відомчих підходів, аналізу взаємодії та координації дій відповідальних державних органів, способів і практики залучення суб’єктів господарства до підвищення безпеки та стабільності функціонування критичної інфраструктури.

Дана Зелена книга розроблена з метою сприяння експертному обговоренню на національному рівні основних проблем та напрямів їх вирішення щодо створення системи захисту критичної інфраструктури в Україні, що зробить вагомий внесок у процес системного реформування усього сектору безпеки держави, наблизивши його структуру і функції до тих, що вже існують у країнах-членах ЄС та НАТО.

2. Що таке критична інфраструктура

Для стабільного і безпечного існування сучасне суспільство та його члени мають надійно отримувати цілу низку самих різноманітних продуктів і послуг, мати доступ до ряду важливих ресурсів тощо. Для цього створюються і використовуються певні об’єкти, мережі та системи, фізичні або віртуальні.

Останніми десятиліттями бурхливий розвиток технологій, особливо в ІТ-сфері, призвів до значних, а іноді й до революційних, змін у підвищенні ступеню взаємозв’язку, взаємопроникнення і взаємозалежності різноманітних мереж і систем, виробничих, фінансових, торговельних та інших процесів у всіх сферах життя більшості країн світу. Це суттєво збільшує вразливість таких систем і об’єктів, значно ускладнює забезпечення їх надійного захисту та безпеки. Водночас згадані процеси відбувалися на тлі різкого загострення загроз тероризму, насамперед міжнародного, зростання кількості техногенних катастроф, у т.ч. викликаних

людським фактором, збільшення кількості природних катастроф, обумовлених, зокрема, глобальними кліматичними змінами. Усі ці чинники обумовили ту увагу, яку провідні країни світу стали приділяти захисту найбільш важливих для безпеки своїх громадян, суспільства і держави об'єктів, систем і ресурсів.

2.1. Визначення терміну «критична інфраструктура»

Зважаючи на величезну кількість чинників, від яких у той чи інший спосіб залежить життя сучасної людини, суспільства та держави, вкрай важливо достатньо чітко окреслити коло саме тих систем, мереж і об'єктів, завдяки функціонуванню яких населенню, суспільству та державі надаються критично важливі для їх існування послуги і здійснюються необхідні функції. Саме це завдання має виконувати визначення терміну «критична інфраструктура».

Слід зазначити, що при всій близькості визначень цього терміну в законодавстві провідних країн та міжнародних організацій, існують і певні відмінності, які, очевидно, відображають національну або організаційну (у випадках ЄС і НАТО) специфіку сфери застосування терміну, особливості їх нормативно-правових систем.

У законодавстві США, країни-лідера у розвитку цього безпекового напряму, під критичною інфраструктурою розуміються «*системи та засоби, фізичні чи віртуальні, настільки життєво важливі для Сполучених Штатів, що недієздатність або знищення таких систем або ресурсів підриває національну безпеку, національну економіку, здоров'я або безпеку населення, або має своїм результатом будь-яку комбінацію з переліченого*» (*Patriot Act*, 2001).

У Німеччині до критичної інфраструктури відносять «*організаційні та фізичні структури і об'єкти настільки життєво важливі для суспільства та економіки країни, що їх вихід з ладу або погіршення функціонування будуть мати своїм результатом стійкі зриви постачання, значний підрив державної безпеки або інші драматичні наслідки*».

Велика Британія визначила елементами критичної інфраструктури «*ті установки, системи, об'єкти та мережі, необхідні для функціонування країни та надання важливих послуг, від яких залежить повсякденне життя Великої Британії*». У Нідерландах при визначенні терміну до критичної інфраструктури віднесли «*продукцію, послуги та пов'язані з ними процеси*». Існують й інші приклади деяких відмінностей у визначенні цього терміну в національних законодавствах.

На наш погляд, важливим є те, що у деяких національних законодавствах вже при визначенні терміну «критична інфраструктура» акцент дещо зміщено з фізичного виміру тобто особливо важливих систем, об'єктів і ресурсів, на функції та послуги, якими вони забезпечують. Саме функції та послуги, якими забезпечують суспільство, бізнес та державу об'єкти та системи критичної інфраструктури, лежать в основі визначення їх критичності, що надає ефективні методологічні можливості для встановлення критеріїв відбору елементів критичної інфраструктури та пріоритетності їх захисту[ii].

Зрозуміло, що визначення цього ключового для даної проблематики терміну в українському законодавстві, залишаючись у рамках загальновизнаних у світі підходів, має у повній мірі відобразити специфіку безпекових умов, в яких перебуває Україна.

В Україні термін «критична інфраструктура» неодноразово використовувався в нормативно-правових документах, проте його визначення й досі відсутнє в чинному законодавстві. Вперше в офіційних документах термін «критична інфраструктура» з'явився у 2006 р. у тексті Рекомендацій парламентських слухань з питання розвитку інформаційного суспільства, на жаль, без подальшого розвитку. В Стратегії національної безпеки «Україна у

[ii]Наприклад, енергетичний сектор у всіх країнах і в таких міжнародних об'єднаннях, як ЄС і НАТО, відносять до критичної інфраструктури. Основна функція (послуга) цього сектора полягає у забезпеченні потреб населення, суспільства і держави в енергії. Якщо акцент робиться на енергетичних об'єктах і системах, то при такому підході без належного аналізу до критичної 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 показує світовий досвід, найтяжчі наслідки для забезпечення електроенергією суспільства виникають внаслідок аварій у системах передачі та розподілення електроенергії, а не у випадку виходу із ладу одного чи кількох об'єктів генерації.

світі, що змінюється» (2012 р.) цей термін згадувався при визначенні шляхів зміцнення енергетичної безпеки та напрямів забезпечення інформаційної безпеки.

В новій Стратегії національної безпеки України (2015 р.) термін «критична інфраструктура» використовується більш деталізовано. Вперше з-поміж «актуальних загроз національній безпеці» виокремлюються загрози критичній інфраструктурі, крім того окремо в підрозділі «Загрози кібербезпеці і безпеці інформаційних ресурсів» згадується вразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак. Також вперше з-поміж «основних напрямів державної політики в сфері національної безпеки» названо забезпечення безпеки критичної інфраструктури та визначені пріоритети такого напряму.

Відсутність визначення терміну «критична інфраструктура» в українському законодавстві, і як наслідок, відсутність переліку об'єктів, які слід віднести до неї, неодноразово створювали перешкоду для ефективного виконання першочергових безпекових завдань, таких як п.6 рішення Ради національної безпеки і оборони України від 1 березня 2014 року «Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України» (введеного в дію указом Президента України №189/2014 від 02.03.2014 р.), на виконання якого Міністерству внутрішніх справ України наказується забезпечити «посилену охорону об'єктів енергетики та критичної інфраструктури».

Зважаючи на викладене вище і враховуючи, отриманий досвід провідних країн світу з розробки підходів до забезпечення національної безпеки на основі застосування концепції «критична інфраструктура», пропонуємо використати в Україні таке визначення даного терміну:

> *Критична інфраструктура України* – це системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки.

Хоча у наведеному визначенні не наголошується на взаємозв'язку/взаємовпливі між окремими елементами критичної інфраструктури, саме ця особливість вливає на рівень наслідків. Відповідно управління безпекою окремих об'єктів повинно здійснюватися виходячи із загальносистемних функцій всієї критичної інфраструктури.

Потрібно надати також тлумачення поняття «захист критичної інфраструктури»:

> *Захист критичної інфраструктури України* – це комплекс заходів, реалізований в нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури.

Під *стійкістю критичної інфраструктури* будемо розуміти її здатність надійно функціонувати у нормальному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після аварій та технічних збоїв, зловмисних дій, природних лих та небезпечних природних явищ[iii]. Також слід підкреслити, що поняття «безпека», яке використано у визначенні «захист критичної інфраструктури», включає як фізичну (фізичний захист), експлуатаційну, так й операційну безпеку.

2.2. Сектори, об'єкти, системи та ресурси, що можуть бути віднесені до критичної інфраструктури

Переліки секторів, які у різних країнах відносять до критичної інфраструктури, також в

[iii] Таке тлумачення відповідає змісту терміну «стійкість» (англ., - Resilience) при його вживанні в офіційних документах як Європейської Комісії, так й низки розвинених країн, зокрема, в Директиві Президента США №21 (лютий 2013 р.)

основному збігаються, адже розвиток сучасного суспільства відбувається за єдиними законами. Існуючі відмінності, обумовлені, насамперед, національною специфікою, традиціями і особливостями безпекової політики тієї чи іншої країни або міжнародної структури.

Звертаючись до досвіду Сполучених Штатів у цій сфері, відзначимо, що перелік секторів, включених до національної критичної інфраструктури цієї країни, є, очевидно, найбільш повним і включає 16 пунктів:

- Хімічний сектор (Chemical);
- Комерційні об'єкти (Commercial facilities);
- Зв'язок (Communications);
- Критичне виробництво (Critical manufacturing);
- Дамби та інші гідротехнічні споруди (Dams);
- Оборонно-промислова база (Defense industrial base);
- Служби екстреної допомоги населенню, реагування на надзвичайні ситуації (Emergency services);
- Енергетичний сектор (Energy);
- Банки та фінанси (Banking and finance);
- Продукти харчування та сільське господарство (Food and agriculture);
- Урядові об'єкти (Government facilities);
- Охорону здоров'я та медицину (Healthcare and public health);
- Інформаційні технології (Information technology);
- Ядерні реактори, матеріали та відходи (Nuclear reactors, materials and waste);
- Транспортні системи (Transportation systems);
- Водні ресурси, системи водопостачання і стічних вод (Water and wastewater systems).

У Німеччині критична інфраструктура розділена на дві групи секторів, які фактично об'єднують дев'ять секторів – *життєво важливу (абсолютно необхідну) базову технічну інфраструктуру* (забезпечення енергією, інформаційні та комунікаційні технології, транспорт, водопостачання і видалення побутових відходів) та *життєво важливу (абсолютно необхідну) інфраструктуру надання соціально-економічних послуг* (охорона здоров'я і забезпечення продуктами; служби невідкладної допомоги, рятувальні служби, управління у надзвичайних ситуаціях; парламент, уряд, державні органи управління, правоохоронні органи; фінансовий сектор та страхові компанії; ЗМІ та об'єкти культурної спадщини). Причому відмічається значна взаємозалежність цих двох груп, оскільки практично всі служби надання соціально-економічних послуг значною мірою покладаються на необмежений доступ до базової технічної інфраструктури, а базова технічна інфраструктура, в свою чергу, залежить від надання соціально-економічних послуг, таких як постійна юридична служба або служби першої допомоги і реагування у надзвичайних ситуаціях.

Зрозуміло, що для України, яка знаходиться у жорстких безпекових та фінансово-економічних умовах, при формуванні переліку секторів критичної інфраструктури слід виходити, насамперед, із наявних ресурсів і потреб підтримання і захисту базових функцій, без чого неможливе безпечне існування населення, суспільства та функціонування економіки й держави, належний захист національних інтересів.

Примірний перелік секторів критичної інфраструктури України наведений у Додатку А.

Наступним кроком, після визначення секторів критичної інфраструктури, має стати складання переліку конкретних об'єктів, систем та ресурсів (елементів) критичної інфраструктури. Такий перелік може налічувати від кількох десятків пунктів для невеликих країн до багатьох тисяч (наприклад, для США). Виходячи з того, що кожна країна може виділити на захист національної інфраструктури лише обмежені ресурси, національне законодавство повинно встановити критерії віднесення тих чи інших об'єктів та систем до критичної інфраструктури, спираючись на затверджені методи оцінки загроз та ризиків сталому її функціонуванню. Такі переліки використовуються при плануванні відповідних заходів та у процесі прийняття рішень. Вони, як правило, підлягають перегляду, періодичному або при значних змінах у безпековому середовищі та при внесенні істотних змін у національне законодавство тощо.

У зв'язку з викладеним заслуговує на увагу визначення критичності, наведене у Національній стратегії захисту критичної інфраструктури Німеччини: *критичність – це відносна міра важливості даної інфраструктури, що враховує вплив раптового припинення її функціонування, або функціонального збою на безпеку постачання, тобто забезпечення суспільства важливими товарами і послугами.*

Аналіз існуючих підходів до визначення переліку елементів критичної інфраструктури (віднесення об'єктів до критичної інфраструктури) засвідчує, що можуть враховуватися, зокрема, такі характеристики:

- масштаб (географічне охоплення території, для якої втрата елементу критичної інфраструктури викликає значну шкоду);
- взаємозв'язок між елементами критичної інфраструктури;
- тривалість впливу (як саме і коли проявлятимуться шкода, пов'язана із втратою чи відмовою, виходом з ладу або порушенням функціонування об'єктів критичної інфраструктури;
- вразливість об'єкту до впливу небезпечних чинників;
- важкість можливих наслідків за показниками в таких основних групах:
    - економічна безпека (вплив на ВВП, розмір економічних втрат як прямих, так і непрямих, частки продукції на ринку, чисельності зайнятих співробітників, податкових надходжень у бюджет);
    - безпека життєдіяльності та здоров'я населення (число постраждалих,загиблих, осіб, які отримали серйозні травми, а також чисельність евакуйованого населення, забезпечення роботи аварійно-рятувальних служб, екстреної допомоги населенню);
    - внутрішньополітична й державна безпека (втрата впевненості в дієздатності влади, авторитету держави, порушення управління державою);
    - обороноздатність (зниження боєздатності збройних сил, розголошення таємної інформації);
    - екологічна безпека (вплив на навколишнє природне середовище).

Деталізація показників, за якими визначається важкість наслідків, значною мірою залежить від сектору критичної інфраструктури.

Процес ідентифікації елементів критичної інфраструктури має включати аналіз взаємозв'язків між елементами критичної інфраструктури та оцінені наслідки можливого припинення їх функціонування (аварії тощо) на довготривалий період.

2.3. Категорії об'єктів у нормативно-правовому полі України, близькі за змістом до об'єктів критичної інфраструктури

Українське законодавство щодо захисту об'єктів, які, згідно зі світовою практикою, відносять до критичної інфраструктури, є достатньо розгалуженим і включає численні нормативно-правові акти, які, проте, носять переважно відомчий характер.

Чинне законодавство визначає такі категорії об'єктів, для яких встановлюються особливі умови забезпечення їх захисту та функціонування:

- підприємства, які мають стратегічне значення для економіки та безпеки держави[5];
- особливо важливі об'єкти електроенергетики[6;]
- особливо важливі об'єкти нафтогазової галузі[7];
- важливі державні об'єкти, у тому числі пункти управління органів державної влади та органів місцевого самоврядування[8];
- об'єкти можливих терористичних посягань[9];
- об'єкти, які підлягають охороні і обороні в умовах надзвичайних ситуацій і в особливий період[10];
- об'єкти, що підлягають обов'язковій охороні підрозділами Державної служби охорони за договорами[11];
- об'єкти підвищеної небезпеки[12] (в т.ч. Перелік особливо небезпечних підприємств, припинення діяльності яких потребує проведення спеціальних заходів щодо запобігання

заподіянню шкоди життю та здоров'ю громадян, майну, спорудам, навколишньому природному середовищу[13]);

- об'єкти, які включені до Державного реєстру потенційно небезпечних об'єктів[14];
- радіаційно небезпечні об'єкти, для яких розробляється об'єктова проектна загроза[15];
- об'єкти, які віднесені до категорій з цивільного захисту[16];
- об'єкти, що належать суб'єктам господарювання, проектування яких здійснюється з урахуванням вимог інженерно-технічних заходів цивільного захисту[17];
- чергово-диспетчерська система екстреної допомоги населенню за єдиним безкоштовним телефонним номером виклику екстрених служб 112[18];
- аварійно-рятувальні служби;
- Національна система конфіденційного зв'язку[19];
- платіжні системи[20];
- нерухомі об'єкти культурної спадщини[21].

Деякі із зазначених категорій об'єктів, частково або повністю, після виконання відповідного аналізу, можуть бути віднесеними до об'єктів критичної інфраструктури.

3. Основні загрози критичній інфраструктурі

У провідних країнах світу, які після терактів 11 вересня 2001 року поставили захист критичної інфраструктури та підвищення рівня її стійкості до числа найбільш пріоритетних завдань у сфері безпеки, виходять із необхідності забезпечення її захисту від усіх видів загроз (*all hazards approach*).

Як правило, у національних законодавствах провідних країн світу загрози критичній інфраструктурі розділяють на три основні категорії, виходячи з характеру їх походження. Але й тут існують деякі відмінності. Наприклад, у США і Канаді до спектру загроз критичній інфраструктурі прийнято відносити *зловмисні дії* (зловмисні дії груп або окремих осіб, таких як терористи і злочинці), *природні небезпеки* (урагани, торнадо, землетруси, цунамі, повені, надзвичайні погодні умови і т. ін.) і *техногенні надзвичайні ситуації* (авіаційні катастрофи, ядерні аварії, пожежі, аварії у системах енергозабезпечення, викиди небезпечних речовин тощо). У Німеччині категорії загроз мають такий вигляд: *небезпечні природні явища* (надзвичайні погодні умови, лісові та степові пожежі, сейсмічні явища, епідемії та пандемії, космічні явища); *технічні аварії/людські помилки* (відмови систем, аварії та надзвичайні події, недбалість, організаційні помилки тощо); *тероризм, злочинність, війна* (тероризм, диверсії, злочинність, громадянські війни, війни).

Загрози кожної з перелічених вище категорій у випадку їх реалізації можуть викликати такі негативні наслідки, які, у свою чергу, стають ініціюючими подіями для реалізації загроз інших категорій і на інших елементах критичної інфраструктури. У такому разі говорять про так звані «ефект доміно» та/або каскадний ефект.

Що стосується спектру загроз критичній інфраструктурі в Україні, то його специфіка обумовлюється, насамперед, особливістю тієї безпекової ситуації, в якій перебуває наша країна. Бойові дії у рамках антитерористичної операції (АТО) на території Донбасу, яка і до теперішньої кризи характеризувалася високою зношеністю основних фондів, серйозними проблемами із забезпеченням екологічної та техногенної безпеки, різко збільшує загрози виникнення аварій на об'єктах підвищеної небезпеки, шахтах, об'єктах електроенергетики, хімічних і металургійних підприємствах і мережах життєзабезпечення, як внаслідок їх випадкового пошкодження або втрати контролю над технологічними процесами, так і в результаті терористичних актів і диверсій.

При цьому слід підкреслити, що Зелена книга з питань захисту критичної інфраструктури в Україні не розглядає захист критичної інфраструктури під час ведення бойових дій або воєнного стану, що має бути предметом розгляду інших документів.

Без сумніву, розвиток ситуації на Сході України буде значною мірою впливати на загрози національній критичній інфраструктурі. Зокрема, слід очікувати, що, одним із наслідків теперішньої кризи стане ймовірне збереження упродовж доволі тривалого часу високого рівня терористичних, диверсійних і кримінальних загроз для критичної інфраструктури.

В існуючому нормативно-правовому полі України, що регулює правовідносини у питаннях близьких до питань захисту критичної інфраструктури, класифікуються не загрози, а надзвичайні ситуації, зокрема, за їх походженням. Статтею 5 Кодексу цивільного захисту України визначається, що залежно від характеру походження подій, що можуть зумовити виникнення надзвичайних ситуацій на території України, визначаються такі види надзвичайних ситуацій: 1) техногенного характеру; 2) природного характеру; 3) соціальні; 4) воєнні. На наш погляд така класифікація не може бути без змін перенесена на загрози критичній інфраструктурі, оскільки має певні методологічні обмеження, і не дозволяє реалізувати всі переваги, які створює запровадження концепції захисту критичної інфраструктури.

Доцільним є виділення наступних категорій загроз, на які має бути налаштований захист критичної інфраструктури:

аварії та технічні збої, зокрема, авіаційні катастрофи, ядерні аварії, пожежі, аварії у системах енергозабезпечення, викиди небезпечних речовин, відмови систем, аварії та надзвичайні події обумовлені недбалістю, організаційними помилками тощо;

небезпечні природні явища, зокрема, надзвичайні погодні умови, лісові, степові та торф'яні пожежі, сейсмічні явища, епідемії та пандемії, космічні явища, урагани, торнадо, землетруси, цунамі, повені і т. ін.;

зловмисні дії, зокрема, зловмисні дії груп або окремих осіб, таких як терористи, злочинці і диверсанти, а також військові дії в умовах війни.

Особливо небезпечними є комбіновані загрози та загрози, реалізація яких може призвести до катастрофічних і різноманітних каскадних ефектів внаслідок взаємозалежності елементів критичної інфраструктури.

Аварії та технічні збої

Розглядаючи *аварії та технічні збої*, слід відмітити, що в Україні через високий рівень зношеності основних фондів існує загроза виникнення аварій на об'єктах підвищеної небезпеки, об'єктах електроенергетики та мережах життєзабезпечення. Значний ризик техногенних аварій пов'язаний із наявністю на території України великої кількості об'єктів віднесених до категорії потенційно небезпечних (понад 24 тис.), причому понад чверть з них ідентифіковані як об'єкти підвищеної небезпеки[iv]. За даними ДСНС[v] аварії на 955 об'єктах, що внесені до Державного реєстру об'єктів підвищеної небезпеки, можуть призвести до виникнення надзвичайних ситуацій державного або регіонального рівня, що також може загрожувати критичної інфраструктури, зокрема що стосується функціонування об'єктів паливно-енергетичного комплексу, мостів та доріг, комунальної інфраструктури тощо.

Природні лиха та небезпечні природні явища

До *природних лих та небезпечних природних явищ* можна віднести такі їх види:

- метеорологічні або надзвичайні погодні умови (снігопади, ожеледь, хуртовини, зливи, градобій, заморозки, посухи, спека, урагани, шквали, смерчі);
- гідрологічні (повені, селі, паводки, підтоплення, цунамі);
- сейсмічні (землетруси);
- геологічні (небезпечні екзогенні геологічні процеси - зсуви, просідання та карст);
- геліофізичні (геомагнітні сонячні бурі);
- лісові, степові й торф'яні пожежі;
- епідемії та пандемії, епізоотії, епіфітотії.

Серед перелічених видів загроз слід виділити метеорологічні, частота яких в Україні значно підвищилася останніми десятиліттями, зокрема таких як обледеніння, підтоплення, посухи тощо.

[iv] *Примітка:* дані опубліковані в Національній доповіді про стан техногенної та природної безпеки в Україні у 2014 році (стор.212).

[v] *Примітка:* дані опубліковані в Національній доповіді про стан техногенної та природної безпеки в Україні у 2013 році.

Серед гідрологічних загроз за наслідками для критичної інфраструктури найнебезпечнішими слід вважати паводки. Зокрема, найбільш масштабний за останні роки паводок в Україні у 2008 р. спричинив пошкодження понад 500 автомобільних мостів, розмивання 1660 км автомобільних доріг різного значення тощо.

Значну загрозу для функціонування та безпеки критичної інфраструктури становлять небезпечні екзогенні геологічні процеси (підтоплення, просідання, карст, зсуви). Так, до 20% залізничних колій знаходяться під впливом регіонального підтоплення земель, близько 40% - перебувають у зонах карстових загроз, до 11% - на територіях можливої активізації зсувних процесів. До 59% магістральних газопроводів перебувають в умовах можливого прояву карсту, до 21% - у зонах прояву регіонального підтоплення земель. Активізація небезпечних екзогенних геологічних процесів спричинює ускладнення інженерно-геологічних умов експлуатації промислових споруд та інженерних мереж промислово-міських агломерацій.

Зловмисні дії

Напружена воєнно-політична ситуація, в умовах якої наша держава відстоює власну територіальну цілісність та суверенітет, характеризується значним зростанням рівня *загроз зловмисних дій* - вчинення терористичних актів та диверсійних операцій на території України, спрямованих на об’єкти критичної інфраструктури.

Безумовно, найсерйознішою може бути потенційна загроза використання з терористичною метою об’єктів ядерної енергетики. При цьому слід відзначити, що на даний момент на українських АЕС забезпечується рівень фізичного захисту, адекватний поточним загрозам.

Відзначається значне зростання інтенсивності кібератак, що здійснюються на інформаційно-телекомунікаційну інфраструктуру в Україні. Кібератак через мережу Інтернет зазнають сервери державних установ, великих компаній, фінансових установ, політичних партій та ЗМІ, а останнім часом й інформаційно-телекомунікаційна інфраструктура воєнних об'єктів.

На окрему увагу заслуговує проблема забезпечення безпеки функціонування державних органів влади, збройних сил, правоохоронних органів та спецслужб (будівель, належної інфраструктури тощо) у кризових ситуаціях. Відповідні інфраструктурні об’єкти у розвинутих країнах світу, як правило, також відносять до критичної інфраструктури.

Загрози критичній інфраструктурі можна також розглядати не тільки з точки зору характеру їх походження, але і виділення елементів критичній інфраструктурі, 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 персонал, який безпосередньо забезпечує функціонування критичної інфраструктури у реальному часі.

Виділення спрямованості дії загроз методологічно дозволяє більш системно підійти до формування державної політики і організації системи захисту критичної інфраструктури. В планах захисту критичної інфраструктури, розроблених операторами, погоджених і схвалених відповідними державними органами, мають бути докладно описані заходи протидії загрозам за наступними напрямами захисту:

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 і живучості систем, функціональне резервування;

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

інформаційні технології – захист інформації, систем зв’язку і управління;

юридичний – врегулювання питань реагування персоналу та функціонування інфраструктури у кризових ситуаціях, закріплення розподілу відповідальності у нормативних і

правових документах, розробка керівництв і інструкцій для персоналу, в тому числі щодо взаємодії в умовах кризової ситуації;

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

4. Державна політика захисту критичної інфраструктури

4.1. Мета захисту критичної інфраструктури в Україні

Одним із пріоритетних напрямів безпекової політики України повинно стати підвищення безпеки та стійкості національної критичної інфраструктури по відношенню до усього спектру загроз і ризиків, оскільки саме критична інфраструктура забезпечує життєво важливі для населення, суспільства та держави послуги та функції, без яких неможливі їх безпечне існування та благополуччя, а також належний рівень національної безпеки.

Мета захисту критичної інфраструктури в Україні випливає із визначення критичної інфраструктури і полягає в забезпеченні постачання населенню, суспільству, бізнесу і державі життєво важливих товарів та послуг. Для виконання зазначеної функції критичної інфраструктури, необхідно гарантувати безперебійне стале функціонування об’єктів критичної інфраструктури у визначених режимах, мати спроможність запобігати руйнуванню чи завданню невиправної шкоди, припиненню функціонування або втраті контролю над об’єктами критичної інфраструктури внаслідок дії всіх чинників, та забезпечувати швидке відновлення їх функціонування, у разі, якщо воно було перерване.

4.2. Стратегічні цілі державної політики захисту критичної інфраструктури

Критична інфраструктура сучасної держави являє собою надскладний комплекс різноманітних за своїм характером елементів, який включає низку організаційних структур, різні управлінські моделі, залежні та взаємозалежні функції та системи як у фізичному, так і у віртуальному просторах. В управлінні критичної інфраструктури беруть участь державні структури на усіх рівнях, з різними сферами відповідальності та повноваженнями, а також власники та оператори об’єктів та систем, що входять до критичної інфраструктури. В умовах глобалізації національна безпека, виробництво, економіка і фінанси кожної країни знаходяться у значній залежності від чинників, які визначають стан безпеки в інших країнах та у глобальному вимірі.

У теперішній час відбувається розвиток нової філософії забезпечення безпеки, в основу якої покладені спільні зусилля громадянина, суспільства, бізнесу і держави. Відбувається формування «культури управління ризиками», яка має складати основу політики у сфері захисту критичної інфраструктури і включає таке:

- відкритий обмін інформацією між державними органами, приватним сектором, населенням і окремими громадянами стосовно ризиків, враховуючи необхідність захисту певної (чутливої) інформації;
- співробітництво між усіма суб’єктами процесу захисту критичної інфраструктури у запобіганні інцидентам та у реагуванні на них;
- підвищення рівня самозахисту, самопомочі, власних можливостей громадян та організацій, уразливих до припинення або погіршення послуг, які забезпечує критична інфраструктура[vi];
- активне міжнародне співробітництво щодо захисту критичної інфраструктури з огляду на процеси глобалізації та зростання залежності безпекових, економічних, виробничих, фінансових і т.ін. процесів у багатьох країнах від постачання послуг та ресурсів, які здійснюються міжнародними мережами, системами, компаніями тощо.

Викладене вище обумовлює першу стратегічну ціль політики щодо захисту критичної

[vi]Наприклад, у Канаді населення повинно бути готовим до того, щоб у випадку надзвичайної ситуації упродовж щонайменше перших 72 годин самостійно забезпечувати першочергові власні потреби.

інфраструктури: *розбудова безпекового партнерства для підвищення безпеки та забезпечення стійкості національної критичної інфраструктури.*

У більшості країн світу і, враховуючи економічні реформи, в Україні очевидним є те, що об'єкти критичної інфраструктури будуть знаходитись переважно у приватній власності. Саме приватним операторам належить як більшість об'єктів критичної інфраструктури, так і лідерство у розробці новітніх технологій виробництва та технологій їх захисту.

Зауважимо, що у більшості розвинутих країн світу основна відповідальність за безпеку об'єктів/систем критичної інфраструктури покладається на їх власників/операторів. Вони мають забезпечувати надійність, живучість і стійкість своїх об'єктів/систем. Держава ж має забезпечувати належне інформування власників/операторів, створення адекватної нормативно-правової бази і стимулів для інвестування в безпеку критичної інфраструктури, а також умов для збереження конкурентоспроможності бізнесу, що робить належні інвестиції в безпеку критичної інфраструктури.

Тому ефективне державно-приватне партнерство (ДПП) є ключовим елементом дієвої сталої політики, спрямованої на підтримання належного рівня безпеки та стійкості критичної інфраструктури. В США і Німеччині необхідною умовою для розбудови такого партнерства визнають формування довіри[vii]між партнерами та стимулів для співпраці. Політика країн має стимулювати як приватних власників, так і органи державного управління на всіх рівнях створити таку систему захисту інфраструктури життєзабезпечення суспільства, яка була б спроможною переборювати надзвичайні ситуації, знижувати ризики та наслідки виникнення таких ситуацій. Обов'язковим елементом такого партнерства є створення стимулів для інвестування в безпеку критичної інфраструктури, а також умов для збереження конкурентоспроможності бізнесу, який робить належні інвестиції в безпеку критичної інфраструктури.

Таким чином, механізм ДПП створює фундамент для стимулювання інвестицій у захист критичної інфраструктури шляхом адекватного інформування бізнесу щодо загроз та ризиків для елементів критичної інфраструктури при одночасному врахуванні того, що витрати бізнесу на відповідні заходи мають бути збалансованими і такими, що не підривають його конкурентоспроможності і спроможності надавати критично-важливі для населення, суспільства і держави послуги.

Що стосується України, то до 2014 року ДПП здійснювалося, головним чином, в сфері економіки в рамках Закону України «Про державно-приватне партнерство» від 01.07.2010 № 2404-VI, норми якого не охоплюють діяльність у сфері захисту критичної інфраструктури. У той же час події 2014-2015 років вказали на важливість залучення громадськості до захисту національних інтересів України і, зокрема, до захисту критичної інфраструктури.

Для України необхідне законодавче врегулювання питання державно-приватного партнерства з забезпечення захисту критичної інфраструктури. Необхідна також розробка нормативно правової-бази щодо врегулювання питань взаємних зобов'язань держави та суб'єктів недержавної форми власності у діяльності із захисту критичної інфраструктури, запровадження у діяльність суб'єктів господарювання практики аналізу ризиків та реагування на загрози (contingency planning), механізмів та інструментів взаємодії та узгодження дій державних та недержавних суб'єктів господарювання, громадськості, механізму розподілу відповідальності та зобов'язань (у т.ч. фінансових).

Потрібно відмітити те, що здійснення заходів з підвищення надійності, живучості та стійкості об'єктів/систем вимагатимуть від операторів додаткових фінансових витрат, що може призвести до підвищення собівартості послуг/товарів, які надають відповідні об'єкти/системи. Як наслідок, при ринковому ціноутворенні підвищаться ціни на відповідні послуги/товари. Ця соціально-економічна сторона захисту критичної інфраструктури має бути врахована як при визначенні об'єктів критичної інфраструктури, так і при встановленні вимог до їх захисту. Причому ініціювання з боку держави вимог щодо підсилення захисту критичної інфраструктури має бути усвідомленим кроком з огляду на зазначений соціально-економічний зміст. До того ж,

[vii]U.S. Department of Homeland Security, National Infrastructure Protection Plan, NIPP 2013 Partnering for Critical Infrastructure Security and Resilience, //www.dhs.gov/national-infrastructure-protection-plan

для деяких секторів критичної інфраструктури держава, в особі відповідних регулюючих органів, можливо повинна буде переглянути тарифи на послуги/товари (як електроенергія).

Одним із найбільш важливих інструментів формування довіри між державними і приватними партнерами, як у США, так і в інших розвинутих країнах світу, вважають обмін відповідною інформацією.

У зв'язку з цим другу стратегічну ціль політики щодо національної критичної інфраструктури у загальному вигляді формулюють як *налагодження обміну інформацією*, що включає збір, аналіз та усвідомлення інформації щодо загроз та ризиків для критичної інфраструктури, вразливостей та характеристик систем захисту елементів критичної інфраструктури, механізмів та процедур реагування тощо.

У сучасному світі елементи критичної інфраструктури мають складні вертикальні та горизонтальні взаємозв'язки, що обумовлює можливість каскадних та віддалених у просторі й часі негативних наслідків відмови окремого елемента критичної інфраструктури. Як зазначалось, у більшості розвинутих країн світу основна відповідальність за безпеку об'єктів/систем критичної інфраструктури покладається на їх операторів. Однак керівництво приватних компаній часто не має ані адекватного усвідомлення необхідності захисту критичної інфраструктури, ані мотивації для цього, виходячи з інтересів лише своєї компанії.

Достатньо повними даними та інформацією щодо ризиків та загроз як усій критичній інфраструктурі, так і окремим її елементам, можуть володіти лише уповноважені державою органи, які однак потребують детальної інформації та співпраці з боку приватного сектору. У зв'язку з цим важливим аспектом є створення адекватної нормативно-правової бази щодо обміну інформацією, яка стосується безпеки функціонування критичної інфраструктури чи захищених систем. При досягненні цієї цілі між партнерами відповідно до встановлених процедур здійснюється ефективний обмін інформацією (у т.ч. розвідувальною) щодо різних аспектів захисту критичної інфраструктури (у т.ч. про найкращу практику), забезпечується захист чутливої інформації (у тому числі комерційної інформації), яка може бути використана у зловмисних цілях.

Українська держава має забезпечувати належне врегулювання питання обміну інформацією, зокрема через формування загальних стандартів обміну інформацією, регламентації діяльності відповідальних зі сторони операторів за забезпечення інформаційного обміну, методології обробки та аналізу інформації, інформування операторів інфраструктури щодо потенційних та реальних загроз, встановлення вимог й обмежень щодо використання чутливої інформації для недопущення зловживань.

У більшості розвинутих країн світу до стратегічних цілей відносять також побудову системи захисту критичної інфраструктури та підвищення її стійкості на основі *підходу до управління ризиками, пов'язаними з усіма видами загроз.*

Виходячи із зарубіжного досвіду, першим кроком на шляху до цієї цілі є основана на всебічному аналізі ідентифікація усіх загроз і ризиків для критичної інфраструктури України. У процесі управління ризиками для їх зниження доцільно включати такі заходи[viii]:

- підвищення стійкості критичної інфраструктури до ідентифікованих загроз і небезпек;
- запобігання загрозам, пов'язаним із зловмисними діями (тероризм, злочинність тощо);
- планування своєчасного реагування на збої у функціонуванні критичної інфраструктури з метою зменшення їх негативного впливу на здоров'я та безпеку населення, економіку та базові функції держави;
- планування швидкого ремонту та відновлення функціонування критичної інфраструктури для випадку надзвичайних ситуацій, яким не можна запобігти.

Незважаючи на критичну важливість заходів з підвищення рівня захищеності та стійкості критичної інфраструктури, їх планування у будь-якій країні здійснюється у рамках бюджетних і ресурсних обмежень. У зв'язку з цим ще однією стратегічною ціллю політики у цій сфері має бути *максимально ефективне використання ресурсів для захисту критичної інфраструктури.* Розбудоване партнерство як на національному, так і на міжнародному рівнях, координація дій та

[viii] U.S. Department of Homeland Security, National Infrastructure Protection Plan, 2006, http://www.naruc.org/publications/nipp_plan4.pdf

обмін інформацією між партнерами створюють передумови для досягнення такої цілі, в результаті чого виключаються дублювання функцій, а також розпорошення ресурсів серед окремих суб'єктів процесу забезпечення захисту критичної інфраструктури.

З огляду на важкі соціально-політичні та фінансово-економічні умови, в яких наразі перебуває Україна, встановлення такої цілі є особливо актуальним.

Україна має забезпечити формування загальнодержавної системи оцінки ризиків та загроз критичній інфраструктурі, належну координацію органів державної влади та узгодження дій різних залучених осіб, що потребуватиме визначення відповідального державного органу та надання йому відповідних повноважень.

Очевидно, що стратегічні цілі державної політики України в сфері захисту критичної інфраструктури мають бути зафіксовані ц вітчизняному законодавстві. Так, доцільним бачиться розробка окремого Закону України, пропозиції щодо його структурних елементів наведені в Додатку Б.

4.3. Основні принципи формування захисту критичної інфраструктури в Україні

Пріоритети політики захисту критичної інфраструктури в Україні сформульовані, виходячи із значущості захисту критичної інфраструктури для забезпечення національної безпеки сучасної держави. Принципи, на яких повинен будуватися такий захист, мають стратегічний безпековий контекст.

На наш погляд, до основних принципів формування (побудови) захисту критичної інфраструктури в Україні слід віднести наступні.

Принцип координованості, що означає

- планування безпеки на національному рівні, узгодження розвитку нормативно-правових, організаційних та науково-технологічних інструментів, призначених для виконання завдань захисту критичної інфраструктури;
- урахування необхідності забезпечення захищеності критичної інфраструктури при плануванні, визначенні пріоритетів та оцінці соціально-економічного розвитку країни;
- створення механізмів впливу на стан захищеності критичної інфраструктури;
- функціонування єдиного центру оцінки стану захищеності критичної інфраструктури, прогнозування загроз та оцінки ризиків для об'єктів, критичної інфраструктури, координації дій всіх зацікавлених сторін із захисту критичної інфраструктури;
- створення механізмів координації зусиль всіх зацікавлених сторін – влади, бізнесу і суспільства, щодо захисту критичної інфраструктури, включно з горизонтальною координацією операторів взаємозалежних і однотипних об'єктів критичної інфраструктури;
- управління усіма наявними в державі ресурсами з метою їх раціонального використання;
- запровадження національної проектної загрози для критичної інфраструктури та окремих її елементів на основі оцінки загроз національній безпеці;
- планування розвитку кадрового забезпечення з урахуванням наявних можливостей спеціалізованих учбових закладів.

Принцип єдності методологічних засад захисту критичної інфраструктури, відповідно до якого запровадження концепції захисту критичної інфраструктури має здійснюватися шляхом:

- використання єдиної понятійної та методологічної бази для аналізу загроз критичній інфраструктурі;
- розробки методології ідентифікації об'єктів критичної інфраструктури (визначення переліку) на основі оцінки важливості надання ними товарів та послуг (оцінки критичності);
- урахування та оцінки всього комплексу загроз об'єктам критичної інфраструктури, використання ризик-орієнтованих методів аналізу та прогнозування ризиків і загроз;
- періодичної оцінки загроз, ризиків та уразливостей об'єктів критичної інфраструктури з використанням відповідного досвіду;

- встановлення особливостей функціонування захисту критичної інфраструктури в мирний час (як в умовах повсякденного функціонування, так й в умовах надзвичайної ситуації та режиму надзвичайного стану) та особливий період (враховуючи особливості періоду мобілізації, режиму воєнного стану та відбудовного періоду);
- надання рівної уваги заходам з попередження загроз надзвичайних ситуацій, підвищення готовності до реагування і ліквідації наслідків таких ситуацій;
- поєднання заходів фізичного захисту із заходами забезпечення надійності, живучості й здатності до швидкого відновлення;
- забезпечення багатоешелонованості і різноманітності бар'єрів захисту;
- поступового впровадження нормативно-правових, організаційних та науково-технологічних інструментів, на основі яких повинні вдосконалюватися засоби та заходи із забезпечення захисту та безпеки критичної інфраструктури.

Принцип державно-приватного партнерства, під яким розуміється залучення всіх зацікавлених у функціонуванні критичної інфраструктури сторін та розмежування відповідальності між ними (держава – власник; влада – суспільство; регулятор – оператор).

Реалізація цього принципу має включати:

- обмін інформацією між державними органами, приватним сектором, населенням і окремими громадянами стосовно ризиків, враховуючи необхідність захисту певної (чутливої) інформації;
- використання ресурсів як держави, так й приватного сектору для досягнення цілей забезпечення захисту критичної інфраструктури;
- декларування безпеки об'єкту власником (оператором);
- паспортизація об'єктів критичної інфраструктури;
- партнерський розподіл і чітке розмежування відповідальності за забезпечення захищеності, безпеки та стійкості критичної інфраструктури між оператором і державою;
- створення стимулів для інвестування у безпеку критичної інфраструктури, створення умов для забезпечення конкурентоспроможності бізнесу, що робить належні інвестиції в безпеку об'єктів/систем критичної інфраструктури;
- залучення громадськості та експертного співтовариства, використання консультаційних (дорадчих) рад при визначенні вимог до захищеності, безпеки та стійкості критичної інфраструктури.

Принцип забезпечення конфіденційності означає, що чутлива інформація про вразливості та конкретні характеристики систем захисту об'єктів чи комерційна інформація, за виключенням випадків, передбачених чинним законодавством, не повинна розголошуватися, оскільки може бути використана у зловмисних цілях.

Принцип міжнародного співробітництва означає врахування трансграничних впливів функціонування критичної інфраструктури, міжнародних зобов'язань України щодо функціонування та безпеки критичної інфраструктури, а також участь України в європейських механізмах цивільного захисту, кібербезпеки та протидії тероризму.

5. Система захисту критичної інфраструктури в Україні

5.1. Основні завдання системи захисту критичної інфраструктури в Україні

Виходячи з цілей та принципів побудови системи захисту критичної інфраструктури, можна сформулювати такі *основні завдання* цієї системи.

1) Загальна координація захисту критичної інфраструктури в Україні, що, зокрема, включає:

- створення та підтримка функціонування національного центру з управління в кризових ситуаціях та захисту критичної інфраструктури;
- формування пропозицій щодо вдосконалення нормативно-правової бази в сферах національної безпеки і оборони (зокрема, щодо цивільного захисту, боротьби з тероризмом, протидії кіберзагрозам), пов'язаних із захистом критичної інфраструктури;

- здійснення оцінки загроз критичній інфраструктурі на національному рівні із врахуванням взаємозв'язків окремих об'єктів та секторів інфраструктури, впливу всіх видів загроз, оцінки ризиків як на рівні окремих регіонів, так і держави в цілому;
- прийняття рішення та оповіщення щодо зміни режиму функціонування системи захисту критичної інфраструктури в залежності від рівня загроз, зміни правового стану (мирний час, надзвичайна ситуація, особливий період);
- підготовку національного плану захисту критичної інфраструктури;
- підготовку національної проектної загрози для критичної інфраструктури;
- координацію зусиль всіх зацікавлених сторін (державних органів та місцевої влади, бізнесу і суспільства), щодо захисту критичної інфраструктури, включно з горизонтальною координацією операторів взаємозалежних і однотипних об'єктів;
- взаємодію та обмін інформацією із мережею ситуаційних (інформаційно-аналітичних) центрів в сфері безпеки і оборони;
- підготовку державної цільової програми в сфері захисту критичної інфраструктури;
- формування комплексної науково-дослідної програми з питань захисту критичної інфраструктури;
- здійснення взаємодії (контактна-точка) зі структурами ЄС та державними органами країн-членів ЄС.

2) Попередження кризових ситуацій, забезпечення готовності до дій у кризових ситуаціях, управління в умовах надзвичайних ситуацій, пов'язаних з функціонуванням критичної інфраструктури (об'єктами критичної інфраструктури), забезпечення відновлення функціонування критичної інфраструктури, що включає:

- застосування існуючих та формування нових заходів із попередження можливих кризових ситуацій, що пов'язані із функціонуванням критичної інфраструктури (її окремих секторів чи об'єктів);
- забезпечення готовності критичної інфраструктури, її здатності функціонувати в умовах кризової ситуації;
- створення нових та вдосконалення існуючих інструментів (нормативно-регламентуючих, організаційних, технологічних) попередження та управління в кризових ситуаціях, пов'язаних із функціонуванням критичної інфраструктури (її окремих секторів чи об'єктів);
- підготовка в рамках національного плану захисту критичної інфраструктури планів попередження кризових ситуацій, пов'язаних із функціонуванням критичної інфраструктури;
- забезпечення фізичного захисту об'єктів критичної інфраструктури, запобігання несанкціонованим діям (в т.ч. терористичним актам) по відношенню до об'єктів критичної інфраструктури, пом'якшення негативних наслідків та відновлення функціонування об'єктів критичної інфраструктури, якщо несанкціоновані дії все ж таки мали місце;
- забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак, забезпечення захисту даних та технічної інформації, що містяться в системах управління технологічними процесами на об'єктах критичної інфраструктури, від несанкціонованого блокування та модифікації;
- забезпечення необхідного рівня експлуатаційної безпеки на об'єктах критичної інфраструктури, розроблення та впровадження інженерно-технічних заходів підвищення безпеки критичної інфраструктури;
- забезпечення стабільного функціонування критичної інфраструктури в умовах надзвичайних ситуацій та особливий період;
- формування матеріальних резервів, оцінка та інвентаризація ресурсів;
- забезпечення конфіденційності інформації, відповідно до встановлених законодавством вимог, при обробці даних про об'єкти критичної інфраструктури;

- забезпечення відновлення функціонування критичної інфраструктури в разі виникнення аварій/збоїв, вчинення зловмисних дій, що зашкодили її функціонуванню, або впливу природних явищ.

3) Підтримка прийняття рішень щодо захисту критичної інфраструктури, включаючи:

- моніторинг та виявлення можливих кризових ситуацій, пов'язаних із функціонуванням критичної інфраструктури;
- формування пропозицій щодо попередження загроз критичній інфраструктурі;
- встановлення та перегляд вимог до захисту об'єктів критичної інфраструктури в різних режимах функціонування;
- ідентифікацію об'єктів критичної інфраструктури; ведення автоматизованого реєстру критичної інфраструктури; збір, узагальнення та аналіз даних щодо об'єктів критичної інфраструктури та їх функціонування;
- забезпечення функціонування системи обміну інформацією, здійснення постійного моніторингу, аналізу та прогнозування загроз об'єктам критичної інфраструктури;
- виявлення та оцінка взаємозалежності між об'єктами критичної інфраструктури;
- визначення та прогнозування об'ємів необхідних ресурсів для забезпечення захисту критичної інфраструктури;
- підтримку прийняття рішень щодо реагування на надзвичайні ситуації, що пов'язані із безпекою та стійкістю критичної інфраструктури;
- аналіз ефективності організаційно-технічних засобів стосовно зниження ризиків життєдіяльності в умовах можливих і реальних загроз функціонуванню критичної інфраструктури.

4) Застосування механізмів регулювання та контролю за функціонуванням критичної інфраструктури, включаючи:

- здійснення раннього оповіщення (попередження про загрози) операторів об'єктів критичної інфраструктури та надання інформаційної, консультативної, експертної, технологічної допомоги операторам критичної інфраструктури, користувачам їх послуг (населенню) задля попередження, реагування, мінімізації можливого впливу загроз;
- зміна режимів функціонування системи захисту критичної інфраструктури в залежності від рівня загроз та правового стану;
- запровадження автоматизованих систем раннього виявлення надзвичайних ситуацій та оповіщення про них;
- розробку та впровадження стандартів, норм та регламентів захисту критичної інфраструктури;
- здійснення перевірок та оцінки захищеності об'єктів критичної інфраструктури;
- здійснення перевірок та оцінки інформаційної безпеки на об'єктах критичної інфраструктури;
- формування, облік та оновлення паспортів об'єктів критичної інфраструктури, а також карт ризику адміністративно-територіальних одиниць.

5) Міжнародне співробітництво в сферах захисту критичної інфраструктури:

- забезпечення оцінки транскордонних впливів функціонування критичної інфраструктури та трансграничних загроз;
- обмін інформацією та кращим досвідом з питань захисту критичної інфраструктури;
- участь України в європейських механізмах захисту критичної інфраструктури;
- аналіз вимог нормативних документів ЄС та їх можливої імплементації в Україні.

Слід відмітити, що деякі завдання, згадані у наведеному вище переліку, частково охоплюються рамками існуючих в Україні систем цивільного захисту, боротьби з тероризмом, протидії кіберзагрозам, забезпечення обороноздатності держави. Проте більшість завдань є принципово новими і пов'язані із принципами побудови захисту критичної інфраструктури, що в свою чергу відображають стратегічні цілі державної політики в цій сфері.

Потрібно окремо зупинитися на деяких наведених вище завданнях системи захисту критичної інфраструктури. Перша група завдань щодо загальної координації включає пункт про

створення та підтримку функціонування *національного центру з управління в кризових ситуаціях та захисту критичної інфраструктури* (Центр). Таке інституціональне нововведення має вирішити задачу організаційного забезпечення роботи системи захисту критичної інфраструктури. Центр може бути утворений як окремий орган, або як структурна частина в межах органу влади, який буде визначений як відповідальний за координацію діяльності із захисту критичної інфраструктури. До функцій такого Центру мають бути віднесені всі ті функції, здійснення яких спрямоване на вирішення тих завдань системи захисту критичної інфраструктури, що не враховані у існуючих державних системах (цивільного захисту, боротьби з тероризмом, протидії кіберзагрозам тощо), зокрема, функції, пов'язані з вирішенням завдань координації (всіх завдань даної групи), підтримки прийняття рішень (більшості завдань), міжнародного співробітництва, а також із частиною функцій двох інших груп.

Завдання захисту критичної інфраструктури зміщують фокус уваги на попередження кризових ситуацій, пов'язаних із функціонуванням критичної інфраструктури в Україні. Потрібно зауважити, що поняття кризова ситуація не є однозначно визначеним у вітчизняному законодавстві, це поняття вживається як в широкому розумінні: «крайнє загострення протиріч, гостра дестабілізація становища в будь-якій сфері діяльності, регіоні, країні»[ix] або як синонім воєнно-політичної кризи: «стан, що характеризується граничним загостренням регіональної або міжнародної воєнно-політичної обстановки, за якої вичерпуються можливості врегулювання спірних питань мирними засобами і наростає реальна загроза застосування воєнної сили», так і в вузькому (галузевому) розумінні, наприклад, для системи фізичного захисту ядерних установок та ядерних матеріалів: «ситуація, що склалася або може скластися внаслідок вчинення або загрози вчинення диверсії, крадіжки або будь-якого іншого незаконного вилучення ядерних матеріалів»[x]. Поняття кризової ситуації для критичної інфраструктури має проміжний характер, і враховує як вплив зовнішніх факторів безпекового середовища, так і фактори функціонування самих об'єктів критичної інфраструктури. Для уникнення неоднозначності надамо визначення цього терміну в тому розумінні, в якому він використовується в даній Зеленій книзі.

Кризова ситуація, що пов'язана із функціонуванням критичної інфраструктури – це ситуація, при якій виникають чи загострюються чинники, змінюються умови чи характеристики безпекового середовища, або змінюється стан функціонування окремих об'єктів критичної інфраструктури таким чином, що це становить загрозу забезпеченню безпеки та/або стійкості критичної інфраструктури (окремого сектору чи його частини).

Таким чином, саме попередження кризових ситуацій має стати ключовою складовою роботи *національного центру з управління в кризових ситуаціях та захисту критичної інфраструктури*. При цьому має здійснюватися постійний моніторинг та виявлення можливих кризових ситуацій, пов'язаних із функціонуванням критичної інфраструктури. Виконання останнього можливе лише за умов створення підрозділу (відділу) в структурі Центру, який буде виконувати функції притаманні ситуаційним центрам, оперативно, в цілодобовому режимі – «24/7» здійснювати функції, пов'язанні із задачами із підтримки прийняття рішень в системі забезпечення захисту критичної інфраструктури. Зокрема, такий підрозділ Центру має взаємодіяти (стане невід'ємною частиною) із мережею відомчих та корпоративних ситуаційних центрів (кризових/інформаційно-аналітичних тощо). Зважаючи на високі здобутки вітчизняних вчених в галузі інформаційних технологій, досить оптимістично сприймається задача технологічного, методологічного та кадрового оснащення такого підрозділу із функціями ситуаційного центру.

Наступним нововведенням, закладеним у перелік завдань захисту критичної інфраструктури є поняття «режим функціонування» даної системи. Треба зазначити, що на сьогодні передбачені виокремленні режими функціонування в державних системах цивільного захисту (повсякденного функціонування, підвищеної готовності, надзвичайної ситуації, надзвичайного стану), «боротьби з тероризмом» (за рівнями терористичної загрози: нормальний, підвищений, високий, критичний), фізичного захисту (нормальне функціонування, підвищена

[ix] З примітки в тексті Закону України «Про внесення змін до Закону України «Про Раду національної безпеки і оборони України» щодо вдосконалення координації і контролю у сфері національної безпеки і оборони»

[x] Згідно визначень нормативних галузевих документів, затверджених наказами Держатомрегулювання від 28.08.2008 №156 та від 15.09.2011 №501/1001

готовність, функціонування у кризовій ситуації, відновлення нормального функціонування). Не викликає сумніву, що режими функціонування цих систем пов'язані із станом захисту критичної інфраструктури. Проте, такі режими не співвідносяться із завданнями захисту критичної інфраструктури, і не можуть бути зведені разом у єдину шкалу для побудови режимів функціонування системи захисту критичної інфраструктури. Також потрібно враховувати особливості правових режимів надзвичайного стану[xi] та зони надзвичайної екологічної ситуації[xii], воєнного стану[xiii], які теж тісно пов'язані із функціонуванням захисту критичної інфраструктури.

Виходячи з вищесказаного та зважаючи на пріоритет завдання попередження кризових ситуацій для системи захисту критичної інфраструктури виокремимо такі режими її (системи) функціонування:

- попередження кризових ситуацій (однієї чи комплексу);
- управління в умовах кризової ситуації;
- функціонування в режимі надзвичайного стану;
- функціонування в режимі воєнного стану.

В цій класифікації нормальний режим функціонування критичної інфраструктури є режимом моніторингу та оцінки ризиків виникнення кризових ситуація, по суті покликаний забезпечити неперервне попередження кризових ситуацій. Якщо ж не вдається уникнути кризової ситуації, то система захисту критичної інфраструктури повинна перейти в наступний режим функціонування – управління в умовах кризової ситуації. Треба відмітити, що кризова ситуація може настати в окремому секторі критичної інфраструктури, проте через взаємозв'язки секторів (взаємозв'язків/впливів об'єктів із різних секторів), така криза може розповсюдитися на всю критичну інфраструктуру та мати найсерйозніші наслідки для соціально-економічного розвитку, обороноздатності чи національної безпеки країни.

Режим управління в умовах кризової ситуації означає необхідність залучення надзвичайних заходів задля стримування чинників, покращення умов та характеристик безпекового середовища, чи покращення стану функціонування окремих об'єктів критичної інфраструктури тощо. Цей самий режим застосовується при відновленні критичної інфраструктури після здійснення зловмисних дій, виникнення аварій та збоїв, значного впливу небезпечних природних явищ.

Перехід в режим функціонування в режимах надзвичайного та воєнного стану відбувається із проголошенням відповідних правових режимів.

Важливою умовою функціонування критичної інфраструктури та елементом управління в різних режимах має стати визначення принципів економічних взаємовідносин та їх змін при зміні режимів функціонування. Оператори та держава мають чітко розуміти економічні наслідки та відповідальність за реалізацію заходів захисту критичної інфраструктури у кожному з режимів її функціонування. Проте, слід відмітити, що в чинному законодавстві не врегульовані в повній мірі питання фінансування витрат операторів критичної інфраструктури, що можуть додатково виникати в умовах кризових ситуацій. Відсутність чітко прописаних зобов'язань щодо підсилення безпеки об'єктів критичної інфраструктури має бути усунена шляхом розвитку відповідних нормативних документів.

Третім нововведенням є «*національний план захисту критичної інфраструктури*» (План). Метою такого документу є детальний огляд системи захисту критичної інфраструктури, що містить як визначення шляхів розвитку системи, так і загальний опис конкретних механізмів досягнення завдань системи. Особливу увагу в Плані слід приділити *діям з попередження кризових ситуацій*[xiv] з метою визначення механізмів виявлення та пом'якшення загроз критичній інфраструктурі (її секторам).

[xi] Закон України від 16.03.2000 № 1550-III «Про правовий режим надзвичайного стану»

[xii] Закон України від 13.07.2000 № 1908-III «Про зону надзвичайної екологічної ситуації»

[xiii] Закон України «Про правовий режим воєнного стану» (в редакції від 11.06.2015)

[xiv] Наприклад, в Великій Британії урядом розроблений План превентивних дій (National Preventive Action Plan: Gas) для сектору газопостачання в енергетиці (див. https://www.gov.uk/government/publications/national-preventive-action-plan-gas), який узгоджується із загальноєвропейськими нормами, що введені Директивою №2004/67/ЄС стосовно заходів щодо забезпечення безперервного постачання природного газу.

Наступна особливість завдань системи захисту критичної інфраструктури, на яку слід звернути увагу, є підготовка «*національної проектної загрози для критичної інфраструктури*». На сьогодні в Україні в державній системі фізичного захисту передбачено розробку та періодичне уточнення проектної загрози, що фактично визначає перелік тих загроз (та їх характеристики), на які повинен бути розрахований фізичний захист об'єктів. Хоча система фізичного захисту спрямована на захист лише окремої категорії об'єктів (ядерних матеріалів, ядерних установок, радіоактивних відходів, інших джерел іонізуючого випромінювання), механізм визначення проектної загрози є важливим з точки зору визначення вимог до систем фізичного захисту, відповідно, обов'язків оператора із забезпечення безпеки об'єктів. На нашу думку, досвід ядерної галузі щодо розробки проектної загрози можна поширити, внісши відповідні корективи, й на інші сектори критичної інфраструктури.

5.2. Суб'єкти системи захисту критичної інфраструктури

Звичайно, ключову роль у діяльності, спрямованій на забезпечення безпеки критичної інфраструктури, має відігравати держава в особі уповноважених нею органів. Це, насамперед, стосується створення відповідної нормативно-правової бази. Роль державних органів є також очевидною для випадків, коли елементи критичної інфраструктури знаходяться або повністю, або частково у державній власності.

Разом з тим, у багатьох країнах світу саме у приватній власності знаходиться значна, а подекуди, й основна частина об'єктів критичної інфраструктури. Тому, наприклад, у Національній стратегії (безпеки) критичної інфраструктури Канади підкреслюється, що «головна відповідальність за підвищення стійкості/здатності до швидкого відновлення (*resilience*) критичної інфраструктури залишається за власниками та операторами». У зв'язку з цим, ефективне державно-приватне партнерство (ДПП) у сфері безпеки в цілому і щодо захисту критичної інфраструктури зокрема є чи не найважливішою складовою здійснення державної політики у цьому напрямі.

Що стосується відповідальності за захист критичної інфраструктури в державі та координації відповідної діяльності, то зарубіжна практика свідчить про можливість різноманітних організаційних підходів.

У США, наприклад, за безпеку критичної інфраструктури відповідає створене одразу ж після терористичних актів 11 вересня 2001 р. Міністерство внутрішньої безпеки (*Department of Homeland Security, DHS*). Схожий з американським підхід використовується у Канаді, де аналогічні функції, за виключенням питань безпеки на морі, виконує Міністерство суспільної безпеки та готовності до надзвичайних ситуацій Канади (*Ministry of Public Safety and Emergency Preparedness of Canada*).

У Німеччині координація дій щодо захисту критичної інфраструктури на національному рівні покладена на Федеральне міністерство внутрішніх справ (*Federal Ministry of the Interior*), у системі якого відповідні організації та установи здійснюють оцінку загроз критичній інфраструктурі, аналізують поточні безпекові умови та розробляють концепції захисту критичної інфраструктури.

У Великій Британії урядова установа Центр захисту національної інфраструктури (*Centre for the Protection of National Infrastructure, CPNI), підпорядкована Генеральному директору Служби безпеки (MI5*), надає консультативні послуги приватним компаніям та організаціям щодо фізичної безпеки національної інфраструктури.

У Польщі завдання координації заходів щодо захисту критичної інфраструктури покладено на Урядовий центр безпеки (*Government Centre for Security*), який є надміністерською організацією, підпорядкованою безпосередньо Прем'єр-Міністру. Цим центром було розроблено Національну програму захисту критичної інфраструктури. В Україні відсутнє визначення критичної інфраструктури на законодавчому рівні, тому відсутнє і поняття суб'єкта захисту критичної інфраструктури. В нашій державі сьогодні паралельно функціонують Єдина система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків (Положення затверджене Постановою Кабінету Міністрів України № 1051 від 15.08.2007 р.), Єдина державна система цивільного захисту (Положення затверджене Постановою Кабінету Міністрів України №

11 від 9 січня 2014 р.), Державна система фізичного захисту (Порядок функціонування затверджений Постановою Кабінету Міністрів України №1337 від 21 грудня 2011 р.).

Названі системи створені, в тому числі, для захисту життєво важливих для держави об'єктів від окремих видів загроз, у зв'язку з чим створюється ситуація, що характеризується домінуванням відомчих підходів до розв'язання безпекових проблем національного масштабу.

Потребує вирішення також питання створення єдиної державної системи виявлення та попередження кібератак на об'єкти критичної інформаційної інфраструктури держави, оцінки рівня захищеності її елементів, створення сил та засобів виявлення і попередження кібератак, а також органів управління та координації різних рівнів, до повноваження яких віднесено в т.ч. забезпечення безпеки автоматизованих систем управління об'єктів критичної інфраструктури.

Через об'єктивну необхідність забезпечення захисту від кіберзагроз, активізувалася робота щодо створення національного центру кіберзахисту та протидії кіберзагрозам, а також національного центру оперативно-технічного управління мережами телекомунікацій України для забезпечення потреб обороноздатності держави в особливий період (відповідне завдання згадується у рішенні РНБОУ[xv]).

В січні 2015 р. Постановою № 18 Кабінет Міністрів України затвердив Положення про Державну комісію з питань техногенно-екологічної безпеки та надзвичайних ситуацій (далі – Положення) і її склад. Згідно з Положенням Державна комісія з питань техногенно-екологічної безпеки та надзвичайних ситуацій (далі - Державна надзвичайна комісія) є постійно діючим органом, який забезпечує координацію діяльності центральних і місцевих органів виконавчої влади, пов'язаної із забезпеченням техногенно-екологічної безпеки, захисту населення і територій від наслідків надзвичайних ситуацій, організаційних заходів протидії терористичній діяльності та воєнній загрозі, запобігання виникненню надзвичайних ситуацій і реагування на них.

Серед основних завдань Державної надзвичайної комісії зазначені і такі, що є близькими за змістом до завдань захисту критичної інфраструктури, а саме:

1) координація діяльності центральних і місцевих органів виконавчої влади щодо

- забезпеченням живучості об'єктів національної економіки та державного управління *під час реагування на надзвичайну ситуацію*;
- забезпеченням стабільного функціонування паливно-енергетичного комплексу *під час виникнення надзвичайної ситуації*, злагодженої роботи підприємств, установ та організацій для забезпечення сталої і безперебійної роботи Єдиної газотранспортної та об'єднаної енергетичної систем України;
- забезпеченням безпеки та сталої роботи транспортної інфраструктури, послуг поштового зв'язку та всіх видів електричного зв'язку;

2) визначення шляхів та способів вирішення проблемних питань, що виникають під час порушення умов належного функціонування об'єктів інфраструктури та безпеки життєдіяльності населення, зокрема у сферах національної безпеки і оборони, енергетики, фінансів, соціального захисту, охорони здоров'я та навколишнього природного середовища.

Прийняття зазначеної постанови, формально, частково вирішує питання координації дій щодо захисту критичної інфраструктури, проте обмежується лише рамками надзвичайних ситуацій в розумінні системи цивільного захисту. Системне комплексне вирішення питань захисту критичної інфраструктури неможливе в рамках існуючої системи цивільного захисту в силу методологічних обмежень.

Вибір тієї чи іншої організаційної моделі захисту критичної інфраструктури для України потребує ретельного вивчення зарубіжного досвіду, але попередній аналіз вказує на прийнятність для України того організаційного підходу, який застосований у сусідній Польщі й у рамках якого можна було б використати деякі українські напрацювання у створенні ситуаційних центрів національного і галузевого рівнів для побудови національної мережі розподілених ситуаційних центрів, однією із ключових функцій якої має бути інформаційно-аналітична підтримка національного ситуаційного/кризового центру.

[xv] *Рішення* Ради національної безпеки і оборони України від 28 серпня 2014 року «Про невідкладні заходи щодо захисту України та зміцнення її обороноздатності»

5.3. Розвиток механізмів захисту критичної інфраструктури в Україні

Захист критичної інфраструктури – це складне комплексне завдання для кожної держави, якими б великими не були її ресурси. На основі аналізу досвіду провідних країн світу щодо захисту національних критичних інфраструктур, а також аналізу ситуації щодо захисту таких інфраструктур в Україні, пропонуємо такі ключові напрями розвитку механізмів захисту критичної інфраструктури в нашій державі:

- створення нормативно-правових та організаційних механізмів захисту критичної інфраструктури;
- визначення пріоритетних секторів критичної інфраструктури;
- визначення органів державної влади, які відповідають за формування та реалізацію державної політики щодо захисту критичної інфраструктури, чіткий розподіл відповідальності між усіма учасниками процесів/заходів із захисту критичної інфраструктури;
- розроблення та затвердження критеріїв та методології віднесення об'єктів (незалежно від їх форми власності) до переліку критичної інфраструктури;
- удосконалення системи моніторингу стану об’єктів критичної інфраструктури, аналізу та прогнозування загроз критичній інфраструктурі, визначення шляхів та способів зменшення ризиків, пов’язаних з функціонуванням критичної інфраструктури, підвищення надійності, живучості та стійкості об’єктів критичної інфраструктури, запобігання виникненню на них надзвичайних ситуацій;
- удосконалення механізмів державно-приватного партнерства, визначення джерел фінансування захисту критичної інфраструктури;
- впровадження інноваційних розробок та удосконалення існуючих засобів забезпечення безпеки та захисту об’єктів критичної інфраструктури;
- розроблення та впровадження стандартів, правил, технічних умов захищеності об'єктів критичної інфраструктури;
- впровадження в систему управління діяльністю операторів «культури управління ризиками»;
- удосконалення систем та режимів охорони об’єктів критичної інфраструктури;
- залучення експертного співтовариства, громадськості, поширення інформації та передових досягнень, підготовка кадрів, проведення тренувань та навчань;
- усунення джерел загроз, зменшення рівня загроз шляхом застосування комплексних безпекових заходів (наприклад, в рамках системи боротьби з тероризмом);
- розвиток міжнародного співробітництва з питань захисту критичної інфраструктури.

Для запровадження загального підходу до захисту критичної інфраструктури в Україні першочерговими можна вважати такі кроки.

а) *Щодо забезпечення нормативно-правового регулювання захисту критичної інфраструктури*:

- визначення основних термінів ("критична інфраструктура", "захист критичної інфраструктури", "регулятор" та "оператор" критичної інфраструктури тощо);
- запровадження порядку ідентифікації (визначення переліку) об’єктів критичної інфраструктури;
- запровадження порядку зміни режимів функціонування системи захисту критичної інфраструктури в залежності від визначеного рівня загроз;
- врегулювання порядку обміну інформацією, збору даних про об’єкти критичної інфраструктури, загрози та ризики для цих об’єктів.

б) Щодо інституційного забезпечення відповідних заходів:

- створення або визначення державного органу, на який будуть покладені обов’язки зі створення, забезпечення організаційно-технічної та наукової підтримки функціонування національного ситуаційного центру з питань захисту критичної інфраструктури (далі – національного ситуаційного центру), а також створення та забезпечення функціонування державної (національної) системи (мережі) розподілених ситуаційних центрів на основі

єдиних регламентів взаємодії та уніфікованих методологічних та організаційних підходів;

- проведення аналізу та оцінки функціонування існуючих галузевих ситуаційних центрів (у т.ч. їх апаратного, методологічного, кадрового забезпечення) з метою створення національної мережі розподілених ситуаційних центрів, однією із ключових функцій якої має бути інформаційно-аналітична підтримка національного ситуаційного центру (див. довідкову інформацію в Додатку В);

в) Щодо організаційно-технічного, методологічного та кадрового забезпечення:

- розробка методології віднесення об’єктів до критичної інфраструктури;
- розробка методології визначення стану об’єктів критичної інфраструктури, а також оцінки ефективності реагування на надзвичайні ситуації на таких об'єктах;
- удосконалення систем моніторингу, включаючи дистанційне зондування, систем прогнозування і підтримки прийняття рішень;
- розробка та впровадження системи підтримки прийняття рішень для національного ситуаційного центру;
- розробка рекомендацій щодо започаткування цільових комплексних програм наукових досліджень та більш активного залучення приватного сектору до фінансування досліджень за тематикою захисту критичної інфраструктури;
- підготовка та перепідготовка кадрів за тематикою захисту критичної інфраструктури, організація спеціалізованих тренувань та учбових курсів на базі вже існуючих учбових центрів у ядерній галузі, у сфері цивільного захисту тощо.

г) Щодо залучення бізнесу та громадськості до вирішення проблем забезпечення захисту критичної інфраструктури:

- інформування населення щодо основних цілей захисту об'єктів критичної інфраструктури, а також з метою стримування потенційних порушників;
- організація державно-приватного партнерства в сфері безпеки;
- створення умов/стимулів участі компаній-операторів (власників) у забезпеченні захисту критичної інфраструктури;
- підтримка національних виробників на ринку безпекових послуг (зокрема в сфері кібербезпеки);
- утворення та підтримка функціонування відповідних консультаційних, дорадчих груп тощо.

6. Критична інфраструктура в аспекті євроінтеграційного курсу України та міжнародне співробітництво

В силу свого географічного розташування Україна має особливо тісні зв'язки із енергетичною та транспортною інфраструктурою країн-членів ЄС. Україна є невід'ємною частиною глобального кіберпростору. Тому потрібно усвідомлювати, враховуючи сучасні геополітичні реалії, що, наприклад, газотранспортна система України може розглядатися європейськими та трансатлантичними партнерами як елемент критичної інфраструктури загальноєвропейського значення.

Підписання 21 березня 2014 р. політичної частини та згодом 27 червня 2014 р. економічної частини Угоди про асоціацію[xvi], подальша її ратифікація Україною та низкою країн-членів ЄС обумовлюють необхідність визначення першочергових кроків, які повинна зробити Україна з метою приведення своїх підходів у цій сфері у відповідність до підходів, які застосовуються в ЄС у сфері захисту критичної інфраструктури.

В ЄС створення правових та організаційних механізмів захисту критичної інфраструктури було ініційовано в 2004 р. у зверненні Європейської Ради до Європейської Комісії (ЄК), в якому ЄК доручалося підготувати загальну стратегію захисту критичної інфраструктури. В жовтні

[xvi] Угода про асоціацію між Україною, з однієї сторони, та Європейським союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони.

2004 р. ЄК оприлюднила офіційне повідомлення[22], в якому містився як огляд дій ЄК в цій сфері, так і пропозиції щодо додаткових заходів заради вдосконалення європейської системи запобігання, готовності та реагування стосовно терористичних атак, спрямованих проти елементів критичної інфраструктури ЄС. У повідомленні наголошується, що підхід до захисту критичної інфраструктури у всіх країнах ЄС повинен бути методологічно близьким. Забезпечити впровадження та реалізацію такого загального підходу мають Європейська програма захисту критичної інфраструктури (ЄПЗКІ) та Європейська інформаційна мережа попередження загроз критичній інфраструктурі (*European Critical Infrastructure Warning Information Network*, CIWIN).

В офіційному повідомленні № 786 за 2006 р.[23] ЄК рекомендувала всім країнам ЄС вжити заходів, зазначених в ЄПЗКІ, а саме:

- розробити національну програму (план) захисту критичної інфраструктури як документ, що має правову силу;
- задовольнити такий рівень охорони здоров'я, технологічної безпеки, соціально-економічного благополуччя, який би гарантував «стійкість» нації до загроз;
- уніфікувати зусилля, спрямовані на захист критичної інфраструктури, надавши єдиному державному органу, що звітує з цього питання, функції координації дій державних органів влади, які спеціалізуються і мають тісні відносини з галузями промисловості, до яких належать об'єкти критичної інфраструктури;
- визначити органи державної влади, відповідальні за сектори критичної інфраструктури, та відповідні приватні компанії;
- створити умови для ефективної взаємодії та обміну інформацією, даними і досвідом між країнами-членами ЄС, урядовими структурами та приватним сектором;
- зробити внесок у створення гармонізованої методології на рівні ЄС та загальноєвропейської системи аналізу ризиків.

Пропозиції щодо процедури та критеріїв визначення об'єктів критичної інфраструктури на загальноєвропейському рівні були представлені в Зеленій книзі (2005 р.)[24]. В ній розглянуто 11 секторів критичної інфраструктури, які охоплюють 37 підсекторів. Надалі, при підготовці проекту директиви, було визначено 11 секторів з 29 підсекторами[25], а вже в ухваленій директиві ЄК[26] згадується тільки два сектори Європейської критичної інфраструктури, що складаються з восьми підсекторів:

- енергетика (електромережі та об'єкти із генерування та передачі електроенергії; нафтопереробна та нафтовидобувна промисловість, нафтопроводи та сховища; газовидобувна промисловість, газопроводи, термінали зрідженого газу);
- транспорт (автомобільний транспорт; залізничний транспорт; авіаційний транспорт; річковий флот; океанічний і морський флот та порти).

Водночас директива не забороняє визначати національні критичні інфраструктури в інших секторах.

Щодо CIWIN, то основним завданням цієї мережі є створення інструментів координації та інформаційного обміну щодо критичної інфраструктури на загальноєвропейському рівні. CIWIN характеризується високими вимогами до забезпечення інформаційної безпеки, оскільки в мережі обробляється інформація, яка є чутливою щодо забезпечення безпеки об'єктів критичної інфраструктури[27].

Отже, при розробці системи захисту критичної інфраструктури в Україні, враховуючи євроінтеграційний курс нашої держави, необхідно спрямувати зусилля на досягнення узгодженості національного законодавства з нормативними актами ЄС щодо:

- загальних принципів захисту критичної інфраструктури;
- тлумачення основних термінів (див. Додаток Г);
- визначення «контактного пункту»[xvii].
- узгодженості щодо пріоритетності захисту критичної інфраструктури (вибору пріоритетних секторів та відповідних підсекторів критичної інфраструктури;
- методологій порівняння та визначення пріоритетних об'єктів в різних секторах;

[xvii] Примітка: англ. термін "Point of contact".

- впровадження діючих в ЄС стандартів захисту критичної інфраструктури.

Необхідно також відмітити, що у процесі розбудови системи захисту критичної інфраструктури в Україні слід враховувати той факт, що у відповідності до Угоди про асоціацію в Україні вже створено «Механізм раннього попередження», призначений для ранньої оцінки потенційних ризиків та проблем, пов'язаних з попитом та пропозицією на природний газ, нафту чи електричну енергію та попередження і швидку реакцію у випадку надзвичайної ситуації чи загрози надзвичайної ситуації.

Особливу увагу в процесі розвитку національної нормативно-правової бази у сфері захисту критичної інфраструктури слід приділити документам, призначеним максимально наблизити вимоги національного законодавства до вимог до функціонування та захисту критичної інфраструктури в галузі енергетики та транспорту, що визначені в директивах ЄС і вказані в Угоді про асоціації між Україною та ЄС[xviii]:

- Директива №2005/89/ЄС щодо заходів з забезпечення безпеки постачання електроенергії та інвестицій в інфраструктуру;
- Директива №2004/67/ЄС стосовно заходів щодо забезпечення безперервного постачання природного газу;
- Директива №2005/65/ЄС Європейського Парламенту та Ради від 26 жовтня 2005 року про посилення безпеки портів
- Регламент (ЄС) №725/2004 від 31 березня 2004 року про посилення безпеки суден та портових споруд;
- Директива 2004/49/ЄС Європейського Парламенту та Ради від 29 квітня 2004 року про безпеку залізниць у Співтоваристві[xix];
- Регламент (ЄС) №336/2006 Європейського Парламенту та Ради від 15 лютого 2006 року про імплементацію Міжнародного кодексу з управління безпекою в рамках Співтовариства[xx].

Слід відзначити важливість формування міжнародних рамкових угод щодо захисту критичної інфраструктури на глобальному рівні. У даному контексті підготовка групою експертів ООН проекту Меморандуму про ненапад на об'єкти критичної інфраструктури з використанням інформаційних технологій може слугувати прикладом такої ініціативи. Україна також має брати активну участь у таких форм співробітництва.

7. Основні висновки

Зелена книга окреслила широкий спектр питань, пов'язаних із захистом критичної інфраструктури. В ній поєднаний як аналіз ситуації в Україні щодо вирішення задач захисту окремих груп об'єктів критичної інфраструктури, так і аналіз досвіду побудови системи захисту критичної інфраструктури в провідних країнах світу. Не відкидаючи інших питань, хочемо сфокусувати увагу на таких питаннях, що в першу чергу пов'язані із формуванням державної політики в цій сфері та створенням в майбутньому системи захисту критичної інфраструктури в Україні.

а) Нині захист критичної інфраструктури є складовою безпекової політики як на національному рівні окремих країн-членів ЄС та НАТО, так і на міжнародному – в рамках названого міждержавного об'єднання та воєнно-політичного блоку. Для України, зважаючи на тяжку безпекову ситуацію, завдання створення системи захисту критичної інфраструктури може здатися занадто амбіційним. Проте його поступове втілення у життя дозволить зміцнити систему

[xviii] Див. Додаток XXVII до Угоди про асоціацію

[xix] Directive 2004/49/EC of the European Parliament and of the Council of 29 April 2004 on safety on the Community's railways and amending Council Directive 95/18/EC on the licensing of railway undertakings and Directive 2001/14/EC on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification (Railway Safety Directive)

[xx] Regulation (EC) No 336/2006 of the European Parliament and of the Council of 15 February 2006 on the implementation of the International Safety Management Code within the Community and repealing Council Regulation (EC) No 3051/95

захисту національної безпеки, посиливши її здатність до попередження кризових ситуацій, пов'язаних із функціонуванням критичної інфраструктури. Разом з тим, запровадження системи захисту критичної інфраструктури ще більше наблизить вітчизняні механізми управління в сфері національної безпеки до тих, що впроваджені в країнах-членах ЄС та НАТО. Захист критичної інфраструктури в Україні має стати невід'ємною частиною загальноєвропейського механізму в сфері безпеки.

б) В даній Зеленій книзі визначені *стратегічні цілі державної політики* в сфері захисту критичної інфраструктури, а відповідно до них – *завдання системи захисту* критичної інфраструктури та *принципи побудови* захисту критичної інфраструктури. В свою чергу завдання системи обумовлюватимуть *функції суб'єктів захисту* критичної інфраструктури. Для створення державної системи захисту критичної інфраструктури в Україні необхідним є здійснення певних змін у національному законодавстві. Доречним бачиться прийняття окремого *Закону України*, який визначає принципи державної політики в сфері захисту критичної інфраструктури в Україні, суб'єкти, завдання та структуру системи захисту критичної інфраструктури в Україні, встановлює відповідальність органів державної влади щодо визначення особливостей функціонування цієї системи.

в) Політика захисту критичної інфраструктури має будуватись на фундаменті співробітництва між державним та приватним сектором. Тому формування й розвиток системи державно-приватного партнерства є наріжним каменем державної політики з питань захисту критичної інфраструктури та має знайти законодавче врегулювання, методологічне та організаційно-технічне забезпечення узгоджених дій. Зокрема, взаємовідносини між оператором і державою як в частині забезпечення функціонування системи захисту критичної інфраструктури, так і в частині обміну інформацією відповідно до встановлених вимог потребують нормативного, організаційного, та технічного врегулювання в рамках функціонування державної системи захисту критичної інфраструктури.

Партнерство означає високий рівень зобов'язань оператора об'єктів критичної інфраструктури щодо забезпечення безпеки об'єктів, а також спроможність регулятора ефективно діяти та забезпечувати стійкість всієї критичної інфраструктури, зокрема в умовах виникнення надзвичайних ситуацій на окремих об'єктах.

Окремим питанням, що має бути вирішено, є врегулювання в повній мірі питання фінансування витрат операторів критичної інфраструктури, що можуть додатково виникати в умовах кризових ситуацій.

г) Особливості завдань захисту критичної інфраструктури, що відрізняють її від існуючих державних систем цивільного захисту, боротьби з тероризмом, протидії кіберзагрозам, тощо, обумовлюють необхідність організаційних нововведень, а саме: *утворення центру з питань захисту критичної інфраструктури* як окремого органу, або як структурної частини в межах органу влади, який буде визначений як відповідальний за координацію діяльності із захисту критичної інфраструктури. Такий Центр має координувати розробку правових, організаційних, технологічних та ін. інструментів захисту критичної інфраструктури, організовувати та залучати до роботи із їхньої розробки всіх зацікавлених сторін (операторів, регуляторів, органи місцевого самоврядування, громадськість тощо). Уточнення завдань системи захисту критичної інфраструктури, визначення функцій її суб'єктів потребує подальшого обговорення цієї проблематики в експертному співтоваристві, серед державних службовців, співробітників правоохоронних органів і спецслужб та представників приватного сектору, до сфери компетенції та інтересів яких входить зазначена проблематика.

д) Хоча в Зеленій книзі запропоновано *перелік секторів* критичної інфраструктури, а також наведено загальну структуру *критеріїв віднесення об'єктів* до переліку критичної інфраструктури, процес їх ідентифікації потребуватиме нормативно-законодавчого, організаційно та методологічного забезпечення. Слід відмітити те, що жодна з існуючих на даний час категорій об'єктів, для яких встановлюються особливі умови забезпечення їх захисту та функціонування, не має підстав бути віднесеною у повному складі, без додаткового аналізу до критичної інфраструктури.

Таким чином дана Зелена книга є кроком до осмислення цілісної державної політики в сфері захисту критичної інфраструктури на шляху її формування в Україні.

Додаток А

Пропозиції щодо переліку секторів критичної інфраструктури та відповідальних відомств[xxi]

Таблиця А.1

Сектор критичної інфраструктури	**Основні відомства, що відповідають за забезпечення безпеки, захищеності та функціонування об'єктів сектору**
1. Паливно-енергетичний комплекс	Міненерговугілля, СБУ[xxii], МВС[xxiii], Держспецзв'язок[xxiv]
2. Транспорт	Мінінфраструктури, СБУ[xxi], МВС[xxii]
3. Мережі життєзабезпечення	Мінрегіон, ДСНС[xxv]
4. Телекомунікації та зв'язок	Держспецзв'язок, МВС[xxii]
5. Фінансово-банківський сектор	НБУ, Мінфін, СБУ[xxi], Держспецзв'язок[xxiii]
6. Органи влади та правопорядку	СБУ[xxi], МВС[xxii], ДСО[xxii]
7. Сектор безпеки і оборони	МО, МВС[xxii], СБУ[xxi]
8. Хімічна промисловість	Держпраці, ДСНС[xxiv], СБУ[xxi]
9. Служби екстреної допомоги та цивільного захисту	ДСНС, МОЗ
10. Харчова промисловість та агропромисловий комплекс	Мінагрополітики

Примітки:

[xxi] відповідальні відомства при прийнятті нормативно-законодавчих актів з регулювання захисту критичної інфраструктури мають бути уточнені.

[xxii] в межах завдань боротьби з тероризмом.

[xxiii] щодо забезпечення охорони об'єктів

[xxiv] щодо протидії кібер-загрозам

[xxv] в межах завдань цивільного захисту.

Додаток Б

Структура Проекту Закону України «Про критичну інфраструктуру»

I. Загальні положення
1. Сфера дії Закону
2. Визначення

II. Державна політика захисту критичної інфраструктури
3. Принципи державної політики у сфері захисту критичної інфраструктури
4. Цілі державної політики захисту критичної інфраструктури
5. Об’єкти захисту критичної інфраструктури
6. Суб’єкти захисту критичної інфраструктури

III. Система захисту критичної інфраструктури
7. Цілі та завдання системи захисту критичної інфраструктури
8. Повноваження і завдання органів державної влади у сфері захисту критичної інфраструктури
9. Взаємодія з іншими системами захисту у сфері національної безпеки
10. Організація взаємодії у сфері захисту критичної інфраструктури
11. Обмін інформацією у сфері захисту критичної інфраструктури
12. Зміна режимів функціонування систем захисту критичної інфраструктури в залежності від рівня загроз та правового стану
13. Участь громадськості у захисті критичної інфраструктури

IV. Механізми реалізації політики захисту критичної інфраструктури
14. Критерії та методологія віднесення об'єктів до переліку критичної інфраструктури
15. Система моніторингу стану об’єктів критичної інфраструктури, аналізу та прогнозування загроз критичній інфраструктурі
16. Визначення та оповіщення щодо рівня загроз критичній інфраструктурі
17. Національна програма захисту критичної інфраструктури
18. Національна система ситуаційних центрів
19. Плани реагування на надзвичайні ситуації

V. Державно-приватне партнерство у сфері захисту критичної інфраструктури
20. Завдання та відповідальність органів державної влади
21. Повноваження та завдання операторів критичної інфраструктури
22. Відповідальність операторів критичної інфраструктури
23. Фінансування заходів у сфері захисту критичної інфраструктури

VI. Міжнародне співробітництво у сфері захисту критичної інфраструктури
24. Набуття міжнародних зобов’язань у сфері захисту критичної інфраструктури
25. Укладання угод у сфері захисту критичної інфраструктури
26. Участь у міжнародних організаціях у сфері захисту критичної інфраструктури

VII. Перехідні положення
27. Внесення змін до Законів України
28. Розробка нормативно-правових актів

Додаток В

Довідкова інформація до розділу 5

Нині проблема підтримки прийняття рішень, оперативного реагування на загрози національній безпеці шляхом швидкого формування обґрунтованих рішень на найвищому рівні державного управління є вкрай актуальною.

Потреба у створенні мережі кризових, інформаційно-аналітичних і ситуаційних центрів в сфері національної безпеки стає все більш очевидною. Захист критичної інфраструктури слід віднести до стратегічного рівня заходів, спрямованих на забезпечення національної безпеки. У цьому контексті доцільно згадати, що за роки незалежності в Україні було зроблено кілька спроб створення ситуаційного центру стратегічного рівня. Дійсно, першу спроба створення Ситуаційного центру при Президентові України датується ще 1992р. Розпорядженням Президента України від 14 липня 1992 р. №128/92-рп були затверджені склад науково-технічної ради по його створенню та схвалена Концепція такого центру.

У теперішній час в Україні існує декілька центрів та систем, які виконують або мали виконувати ті чи інші функції ситуаційних центрів в окремих секторах національної безпеки і оборони. До них слід віднести, зокрема, такі:

Антитерористичний центр при Службі безпеки України, що здійснює координацію діяльності суб'єктів боротьби з тероризмом щодо запобігання, попередження та припинення терористичних актів (в т.ч. на об’єктах підвищеної небезпеки);

Ситуаційний центр Головного командного центру Збройних Сил України (ГКЦ ЗСУ), до функцій якого належить, зокрема, здійснення аналізу та узагальнення інформації про надзвичайні ситуації, організація накопичення інформації про потенційно небезпечні об’єкти Міністерства оборони України;

Урядова інформаційно-аналітична система з питань надзвичайних ситуацій (УІАС НС), програма створення якої була ухвалена ще у 1996р., а її виконання було затверджене на період 2000-2002 рр. На жаль, за ряду причин, головною з яких можна вважати неефективність державного апарату, ця система так і не була повністю запроваджена в експлуатацію.

Остання спроба у цьому напрямі була зроблена в Апараті РНБОУ у період 2010 – 2013 рр., а саме розпорядженням Секретаря Ради національної безпеки і оборони України від 6 листопада 2013 р. № 70 «Про затвердження концепції створення ситуаційного центру інформаційно-аналітичної підтримки Апарату Ради національної безпеки і оборони України» було затверджено концепцію та відповідно до першого етапу робіт створено програмно-технічний комплекс вказаного ситуаційного центру. Необхідність у створенні національного ситуаційного центру знайшла своє певне відображення у затвердженому в 2012р. Кодексі цивільного захисту України. В ньому згадується державний центр управління в надзвичайних ситуаціях, на який покладені функції щодо здійснення управління у режимі повсякденного функціонування суб’єктами забезпечення цивільного захисту, координації дій органів управління та сил цивільного захисту, здійснення цілодобового чергування та забезпечення функціонування системи збору, оброблення, узагальнення та аналізу інформації про обстановку в районах надзвичайних ситуацій «цілодобового» (ст.73.п.1)[28].

У теперішній час робота окремих підсистем єдиної державної системи цивільного захисту здійснюється із залученням відомчих структурних підрозділів, що виконують частину функцій, притаманних ситуаційному центру. Наприклад, в структурі Держатомрегулювання функціонує Інформаційно-кризовий центр, який є ключовим елементом підсистеми «Безпека об’єктів ядерної енергетики»[29].

Ситуаційні центри створюються і розвиваються в окремих крупних корпораціях, зокрема, в ядерній енергетиці. Наприклад, НАЕК «Енергоатом» планує запровадити нову систему підтримки прийняття рішень при радіаційних аваріях РОДОС (*RODOS – Real-time On-line Decision Support System*), яка вже діє в ряді країн-членів ЄС, створити Центр прогнозування наслідків радіаційних аварій, автоматичну метеорологічну станцію і спеціалізований обчислювальний центр.

Наявність цілої низки галузевих і, навіть, корпоративних ситуаційних центрів в Україні, тенденція до їх подальшого розвитку, а також наявний зарубіжний досвід свідчать про те, що завдання створення національної мережі ситуаційних центрів і національного ситуаційного центру, які мають відігравати ключову роль у захисті критичної інфраструктури України, слід віднести до категорії пріоритетних у сфері національної безпеки.

Додаток Г

Основні визначення в сфері захисту критичної інфраструктури, прийняті в нормативно-правових актах ЄС (за Директивою ЄК 2008/114) та США

Переклад українською мовою	Визначення англійською мовою, опубліковане в офіційному джерелі Європейської Комісії
критична інфраструктура – об'єкти (*матеріальні ресурси, основні фонди)*, системи чи їх частини, розташовані в країнах-членах, які є суттєвими для підтримки життєво важливих функцій суспільства, здоров'я, безпеки, захищеності, економічного та соціального благополуччя людей, порушення їхнього функціонування або знищення матимуть значний вплив у країні-члені ЄС та призведуть до нездатності забезпечувати вказані функції.	**'critical infrastructure'** means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions
Європейська критична інфраструктура – критична інфраструктура, розміщена на території країн-членів ЄС порушення функціонування якої або знищення матиме значний вплив щонайменше для двох країн-членів ЄС. Значимість впливу є бути оцінена в термінах між секторальних критеріїв. Це включає впливи спричинені між секторальними взаємозв'язками із іншими типами інфраструктури.	**'European critical infrastructure'** or 'ECI' means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure
Аналіз ризику – розгляд відповідних сценаріїв загроз задля оцінки вразливості та потенційного впливу порушення функціонування або знищення критичної інфраструктури.	**'risk analysis'** means consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure
Чутлива інформація, пов'язана із захистом критичної інфраструктури – факти (дані) про критичну інфраструктуру, які в разі їх розкриття можуть бути використані для планування та здійснення діяльності спрямованої на порушення функціонування або знищення об'єктів критичної інфраструктури.	**'sensitive critical infrastructure protection related information'** means facts about a critical infrastructure, which if disclosed could be used to plan and act with a view to causing disruption or destruction of critical infrastructure installations
Захист – всі види діяльності, спрямовані на забезпечення функціональності, безперервності та цілісності критичної інфраструктури з метою недопущення, пом'якшення та нейтралізації загроз, ризиків та вразливостей.	'protection' means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability
Власники/оператори – особи відповідальні за інвестиції та/або щоденне функціонування окремого об'єкту, системи або її частини, що визначені як Європейська критична інфраструктура згідно з Директивою Європейської Комісії 2008/114.	'owners/operators' means those entities responsible for investments in, and/or day-to-day operation of, a particular asset, system or part thereof designated as an European Critical Infrastructure under this Directive 2008/114/EC.

Список посилань

[1]GREEN PAPER ON A EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION, http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf

[2]Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection, http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf

[3]A Communication on Protecting Europe's Critical Energy and Transport Infrastructure (цей документ містить чутливу інформацію, і тому не підлягає публікації)

[4]COUNCIL DIRECTIVE 2008/114/EC of 8 December on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[5]*Постанова* Кабінету Міністрів України від 23.12.2004 № 1734 «Про затвердження переліку підприємств, які мають стратегічне значення для економіки та безпеки держави»

[6]*Постанова* Кабінету Міністрів України від 28.07.2003 № 1170 «Про затвердження переліку особливо важливих об'єктів електроенергетики, які підлягають охороні відомчою воєнізованою охороною у взаємодії із спеціалізованими підрозділами інших центральних органів виконавчої влади»

[7]*Розпорядження* Кабінету Міністрів України від 27.05.2009 № 578-р «Про затвердження переліку особливо важливих об'єктів нафтогазової галузі»

[8]*Постанова* Кабінету Міністрів України № 1051 від 15.08.2007 (для службового користування)

[9] *Положення* про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків (затверджене Постановою Кабінету Міністрів України № 1051 від 15.08.2007 р.)

[10]*Постанова* Кабінету Міністрів України від 24.04.99 року №675-019 «Щодо затвердження Переліку об’єктів, які підлягають охороні і обороні в умовах надзвичайних ситуацій і в особливий період»

[11]*Постанова* Кабінету Міністрів України від 10 серпня 1993 р. №615 «Про заходи щодо вдосконалення охорони об'єктів державної та інших форм власності» (із змінами)

[12]*Закон* України від 18.01.2001 № 2245-III «Про об’єкти підвищеної небезпеки»

[13]*Перелік* особливо небезпечних підприємств, припинення діяльності яких потребує проведення спеціальних заходів щодо запобігання заподіянню шкоди життю та здоров'ю громадян, майну, спорудам, навколишньому природному середовищу / Затв. Постановою Кабінету Міністрів України від 06.05.2000 №765

[14]*Постанова* Кабінету Міністрів України від 29.08.2002 р. № 1288 «Про затвердження Положення про Державний реєстр потенційно небезпечних об'єктів»

[15] *Наказ* Держатомрегулювання від 17.12.2012 № 238 «Про затвердження Переліку радіаційно небезпечних об’єктів в Україні, для яких розробляється об’єктова проектна загроза»

[16] відповідно до порядку, затвердженого постановою Кабінету Міністрів України від 02.03.2010 № 227 дск (із змінами згідно постанови Кабінету Міністрів України від 24.07.2014 № 545 дск)

[17] затверджених постановою Кабінету Міністрів України від 09.01.2014 № 6

[18]*Закон* України від 13.03.2012 №4499-VI «Про систему екстреної допомоги населенню за єдиним телефонним номером 112»

[19]*Закон* України від 10.01.2002 № 2919-III «Про Національну систему конфіденційного зв'язку» (із змінами)

[20]*Закон* України від 05.04.2001 №2346-III «Про платіжні системи та переказ коштів в Україні»

[21]*Закон* України від 08.06.2000 № 1805-III «Про охорону культурної спадщини»

[22]*Communication* from the Commission to the Council and the European Parliament of 20 October 2004 – Critical infrastructure protection in the fight against terrorism (COM/2004/702 final). – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

[23]*Communication* from the Commission on a European Programme for Critical Infrastructure Protection (COM/2006/786 final). – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

[24]*Green paper* on a European programme for critical infrastructure protection (COM/2005/576 final). – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

[25]*Proposal*for a Directive of the Council on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection (COM/2006/787 final). – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

[26]*Council* Directive 2008/114/EC “On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection”. – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

[27]*Commission* staff working document – Accompanying document to the proposal for a Council decision on creating a Critical Infrastructure Warning Information Network (CIWIN) – Impact assessment (SEC/2008/2702). – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

[28] Кодекс цивільного захисту України http://zakon1.rada.gov.ua/laws/show/5403-17/page4

[29]Положення про функціональну підсистему єдиної державної системи запобігання і реагування на надзвичайні ситуації техногенного та природного характеру «Безпека об’єктів ядерної енергетики» http://www.snrc.gov.ua/nuclear/uk/publish/article/140508