Бірюков Д.С.,
кандидат технічних наук, головний консультант відділу енергетичної та техногенної безпеки Національного інституту стратегічних досліджень

ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ: ВІД НАУКОВОГО ОСМИСЛЕННЯ ДО РОЗРОБКИ ЗАСАД ПОЛІТИКИ

Стаття представляє досвід опрацювання концепції захисту критичної інфраструктури в Україні та пропонує авторське бачення пріоритетних напрямів впровадження такої концепції в систему забезпечення національної безпеки України

The paper presents the experience of working out the concept of protection of critical infrastructure in Ukraine and provides the author's vision on priorities of implementation of this concept into national security system of Ukraine

Вступ. Прикметник "критичний" у різному роді, відмінку чи числі нині з'являється у вітчизняних офіційних документах та нормативно-законодавчих актах в переважній більшості випадків в поєднанні із такими поняттями як "стан", "ситуація" та "зношеність основних фондів". Деякою мірою таке положення справ може змінити впровадження в Україні системи захисту критичної інфраструктури. Причому йдеться в першу чергу не про зміну статистики результатів пошукових запитів, а про впровадження низки нововведень нормативного та організаційного характеру в систему забезпечення національної безпеки нашої країни.

З середини 90-х років XX століття поняття "критична інфраструктура" було введено в нормативно-правові документи та практику міжнародного спілкування на дипломатичному рівні, в науковому та діловому колах. Терміном "критична інфраструктура", зазвичай, охоплюються ті об'єкти, порушення функціонування або руйнування яких призведе до найсерйозніших наслідків для соціальної та

економічної сфери держави, негативно вплине на рівень її обороноздатності та національної безпеки, а також підтримування життєво важливих функцій в суспільстві. Як правило, до критичної інфраструктури відносять енергетичні та транспортні магістральні мережі, нафто- та газопроводи, морські порти, канали швидкісного та урядового зв'язку, системи життєзабезпечення (водо- та теплопостачання) мегаполісів, утилізації відходів, служби екстреної допомоги населенню та служби реагування на надзвичайні ситуації, високотехнологічні підприємства та підприємства військово-промислового комплексу, а також центральні органи влади. Хоча в Сполучених Штатах до нещодавно критичну інфраструктуру розглядали у більш широкому розумінні, включаючи до неї національні символи.

Як і в інших країнах, в Україні існують такі об'єкти. 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 врегульовують окремі питання в цій сфері. Проте, в Україні й досі відсутній системний підхід на національному рівні до управління захистом та безпекою усього комплексу таких систем, з врахуванням їх взаємопов'язаності.

Також необхідно підкреслити відсутність механізму попередження можливих кризових ситуацій, що пов'язані із функціонуванням критичної інфраструктури. Впровадження такого механізму потребує ґрунтовного переосмислення існуючої практики забезпечення захисту об'єктів критичної інфраструктури в Україні (що нині базується на відомчому підході), аналізу взаємодії та координації дій відповідальних державних органів, способів і практики залучення приватних суб'єктів господарства до підвищення безпеки та стабільності функціонування критичної інфраструктури.

В якості ще одного аргументу в підтвердження необхідності впровадження в Україні такого підходу є поступова модернізація сектору безпеки і оборони в нашій державі, приведення його до стандартів країн учасниць трансатлантичного Альянсу.

Мета статті – розкрити досвід опрацювання концепції захисту критичної інфраструктури в Україні та представити авторське бачення принципів впровадження такої концепції в систему забезпечення національної безпеки та моделі організації взаємодії органів державної влади.

Виклад основного матеріалу. Впровадження захисту критичної інфраструктури в країні є амбіційним завданням, вирішення якого потребує як матеріальних ресурсів, так і ґрунтовної науково-технічної та експертної підтримки, кадрових ресурсів, і мабуть ключовий момент – політичної волі. Відносно останнього потрібно сказати, що країна, яка виявиться нездатною організувати ефективно захист власної критичної інфраструктури не тільки закриває собі шлях розвитку, а приречена на загибель. На щастя в нашій державі є значний науковий потенціал, здатний забезпечити науково-технологічне, методологічне та кадрове забезпечення системи захисту критичної інфраструктури.

Без сумніву захист критичної інфраструктури може розглядатися як комплексна наукова проблема. Результати досліджень мають забезпечити вирішення питань нормативно-правового, організаційного, методологічного, технологічного, інженерного, кадрового забезпечення.

В даній роботі ми розглянемо два пов'язаних аспекти захисту критичної інфраструктури, перший стосується виокремлення цього напряму в державній політиці в сфері національної безпеки, а другий – організації самої системи захисту критичної інфраструктури в Україні. Названі питання починаючи з 2011 року були в полі зору Національного інституту стратегічних досліджень (НІСД), який взяв на себе активну роль з ініціювання в Україні огляду проблем в цій сфері, зокрема в рамках утвореної міжвідомчої експертної робочої групи.

В липні 2012 р. НІСД організував круглий стіл та оприлюднив аналітичну доповідь з питань захисту критичної інфраструктури. На той час проблема відсутності комплексного захисту критичної інфраструктури була визначена таким чином [1, с.46-47]:

– “заходи … здійснюються низкою відомств в межах їх завдань і компетенції, і мають фрагментарний характер, що відбивається в паралельному функціонуванні систем, призначених для захисту об’єктів та населення від окремих типів загроз”;

– “категоризація критично важливих об’єктів … здійснюється на основі галузевих (відомчих) підходів”;

– наявна “невідповідність національної нормативно-правової бази положенням міжнародних документів … на фоні декларування курсу на євроінтеграцію”;

– залишається “обмеженість механізмів обміну інформацією та інформаційного забезпечення про загрози об’єктам критичної інфраструктури та відсутність механізмів надвідомчого управління та інвентаризації ресурсів”;

– “відсутність нормативних документів, вимог, методологій для оцінки загроз об’єктам, що є критичними для життєдіяльності держави; загальної методології оцінки ризиків для критично важливих об’єктів та інфраструктури, не зважаючи на щільну взаємозалежність критично важливих об’єктів (насамперед інформаційними, енергетичними і транспортними мережами), що створює небезпеку виникнення каскадних аварій”;

– “відсутність ефективної практики державно-приватного партнерства в сфері безпеки, що вимагає вдосконалення організаційних та правових основ такого партнерства”.

Наступним кроком в опрацюванні концепції захисту критичної інфраструктури як методологічного складника основ національної безпеки можна назвати міжнародну конференцію, проведену НІСД в листопаді 2013 року [2].

В ході конференції розглядалися в тому числі питання організації захисту критичної інфраструктури в країнах-членах ЄС, зокрема, Польщі та Угорщині [2, с.49-61]. Запрошеними іноземними експертами було звернено увагу на те, що в концепції захисту критичної інфраструктури здійснено фокусування на стійкості суспільства, пріоритеті надання життєво необхідних для суспільства функцій та товарів [2, с.41-49]. Останнє зайняло важливе місце в

рекомендаціях апарату Європейської Комісії в 2013 р. [3], і відобразилося в офіційному визначенні терміну. яке було введено в Директиві 2008/114 Європейської Комісії в такому виді [4]: “критична інфраструктура – об’єкти, системи чи їх частини, розташовані в країнах-членах ЄС, 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”. Схоже визначення містяться в нормативно-правових актах Сполучених Штатів [5]: “системи та об'єкти, фізичні чи віртуальні, настільки життєво важливі для держави, що недієздатність або знищення таких систем або об'єктів підриває національну безпеку, економіку, здоров‘я або безпеку населення, або має своїм результатом будь-яку комбінацію з переліченого вище”.

Декілька слів потрібно сказати відносно використання терміну “критична інфраструктура” у вітчизняних офіційних документах. Перше згадування про нього (з точки зору інформаційних мереж) прозвучало у 2006 р. в тексті Рекомендацій парламентських слухань з питання розвитку інформаційного суспільства [6], однак, на жаль, робота з впровадження цих рекомендацій, у т. ч. стосовно захисту критичної інфраструктури від широкого кола загроз, у подальшому припинилася. В Стратегії національної безпеки “Україна у 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.

Спроба ввести термін "критичний об'єкт національної інформаційної інфраструктури" були здійснена в Законі України від 16 січня 2014 року № 721-VII, що втратив чинність вже на початку лютого 2014 р. Раніше в проекті Закону України "Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України" (був зареєстрований під №11125 від 31.08.2012р., відкликаний 12.12.2012р.) передбачалось внесення змін до Закону України "Про основи національної безпеки України", і, зокрема, введення терміну "об'єкти критичної інформаційної інфраструктури".

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".

В 2014-2015 рр. Інститутом за сприяння Офісу зв'язку НАТО в Україні було проведено низку експертних нарад із запрошеними зарубіжними експертами, на яких обговорювався зміст Зеленої книги з питань захисту критичної інфраструктури в Україні (у вересні 2014 р., листопаді 2014 р. та лютому 2015 р.). Остаточна редакція Зеленої книги була оприлюднена на сайті Інституту на початку жовтня 2015 р. [7].

В Зеленій книзі зазначається, що мета захисту критичної інфраструктури в Україні полягає в забезпеченні постачання населенню, суспільству, бізнесу і державі життєво важливих товарів та послуг [7, с.14]. Для цього 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. Саме виходячи з пріоритету надання функцій та послуг життєво необхідних для суспільства, людини та держави і дається таке визначення [7, с.8]: "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".

Разом із визначенням терміну "критична інфраструктура" потрібно уточнити й поняття "захист критичної інфраструктури" [7, с.8]:. "це комплекс заходів, реалізований в нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури". Потрібно зазначити, що в даному контексті поняття "захист" вживається в широкому розумінні, і не в якому випадку не має ототожнюватися із поняттям фізичного захисту об'єктів (тобто їх захищеності). Також, поняття "безпека", яке використано у визначенні, включає як фізичну безпеку (фізичний захист), так й експлуатаційну безпеку. Окремо слід пояснити термін "стійкість" (аналог англомовного терміну Resilience), який широко вживається в офіційних та нормативних документах Європейської Комісії. 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.

В Зеленій книзі були представлені основні принципи формування (побудови) захисту критичної інфраструктури в Україні [7, с.17-18]. Слід зупинитися на них більш детально.

Першим названий принцип координованості. Він увібрав в себе цілу низку ідей, пов'язаних із необхідністю узгодженості як процесів планування безпеки на національному рівні, узгодження розвитку нормативно-правових, організаційних та науково-технологічних інструментів, призначених для виконання завдань захисту критичної інфраструктури, так і діяльності суб'єктів захисту критичної інфраструктури.

Напевне ключовою проблемою є 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.

Координація процесу побудови захисту критичної інфраструктур повинна, за думкою розробників Зеленої книги, відобразитися і при плануванні та визначенні пріоритетів соціально-економічного розвитку країни. Надійне функціонування критичної інфраструктури є передумовою стабільного економічного зростання країни та соціально-економічного благополуччя населення [1, с.77].

Через різноманітність загроз та типів об'єктів критичної інфраструктури потрібним є створення 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. Причому така комплексна оцінка ризиків має здійснюватися в мережі ситуаційних центрів.

Пов'язаною задачею є запровадження національної проектної загрози для критичної інфраструктури та окремих її елементів на основі оцінки загроз національній безпеці.

Другим названий принцип єдності методологічних засад. Відповідно до цього принципу запровадження 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).

Принцип єдності вказує на необхідність побудови таких підходів до захисту критичної інфраструктури, що враховують разом елементи певних груп (категорії) особливостей, а саме: урахуванням та оцінки всього комплексу загроз; 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.

Окремо підкреслюється важливість принципу державно-приватного партнерства, тобто залучення всіх зацікавлених у функціонуванні критичної інфраструктури сторін та розмежування відповідальності між ними (держава – власник; влада – суспільство; регулятор – оператор). Основними завданнями реалізації даного принципу є:

- партнерський розподіл і чітке розмежування відповідальності за забезпечення захищеності, безпеки та стійкості критичної інфраструктури між оператором і державою;
- організація обміну інформацією між державними органами, приватним сектором, населенням і окремими громадянами стосовно ризиків;
- використання ресурсів як держави, так й приватного сектору для досягнення цілей забезпечення захисту критичної інфраструктури;
- залучення громадськості та експертного співтовариства, використання консультаційних (дорадчих) рад при визначенні вимог до захищеності, безпеки та стійкості критичної інфраструктури.

Окремо названий принцип забезпечення конфіденційності, який 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.

Оскільки критична інфраструктура в Україні має і транскордонне значення, впливає на безпеку наших європейських сусідів, а Україна рішуче здійснює кроки з євроінтеграції, то при побудові захисту критичної інфраструктури потрібно слідувати принципу міжнародного співробітництва. Цей принцип 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.

Робота із опрацювання Зеленої книги, зокрема обговорення питань із залученими до роботи зарубіжними експертами, дозволила чітко окреслити структуру та характеристики бажаної майбутньої системи захисту критичної інфраструктури в Україні. Не можна сказати, що вирішенню деяких окремих завдань (як-то реагування на надзвичайні ситуації чи боротьба з тероризмом) захисту критичної інфраструктури бракує нормативного або організаційного забезпечення, тут можна говорити лише про вдосконалення відповідних інструментів, а здебільшого про ресурсне забезпечення відповідної діяльності. Проте треба звернути увагу на задачі не об'єктового а системного рівня. Саме недосконаліть заходів із комплексного управління захистом критичної інфраструктури в Україні спричиняє необхідність вдосконалювати нормативні, організаційні та технологічні інструменти задля забезпечення безпеки та стійкості критичної інфраструктури.

Спираючись на досвід країн-членів ЄС та НАТО, зокрема, посилаючись на досвід успішного функціонування Урядового центру з питань безпеки [8] (Республіка Польща), в Зеленій книзі в якості однієї з основних рекомендацій вказується на необхідність визначення органу, який буде відповідати за

виконання завдань координації в системі захисту критичної інфраструктури. Крім того такому органу будуть делеговані функції аналітичного та прогностичного характеру, завдання із організації підтримки прийняття стратегічних рішень щодо захисту критичної інфраструктури. Слід підкреслити, що такий орган не має входити в організаційну структуру будь-якого з відомств, що задіяні до вирішення завдань захисту критичної інфраструктури. Зважаючи на це, вважаємо за доцільне утворення Центру захисту критичної інфраструктури (Центр).

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"[1] 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"[2]. 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

[1] 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"

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

розумінні, в якому він використовується в даній Зеленій книзі [7, с.21]:

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 Центру 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.

Оскільки не передбачається наділити Центр правом прямого управління суб'єктами системи захисту критичної інфраструктури, то його пропозиції мають враховуватися шляхом затвердження в нормативно-правових документах. Одним із способів такого затвердження є винесення пропозиції на розгляд Державної надзвичайної комісії у формі проекту рішення.

На основі досвіду впровадження захисту критичної інфраструктури в країнах-членах ЄС та НАТО в Зеленій книзі

запропонований перелік "секторів" критичної інфраструктури [7, с.30]. Фахівцями НІСД аналізувалися категорії об'єктів, які знайшли відображення у вітчизняній нормативно-правовій базі та можуть (певна частина з них) бути віднесені до об'єктів критичної інфраструктури в Україні [1, с.31-34]. В кожному із секторів критичної інфраструктури, як правило, визначається відповідальне відомство, на яке буде покладено низку функцій (часто на практиці ці функції вже виконуються відомством) щодо захисту відповідних об'єктів критичної інфраструктури.

До суб'єктів системи захисту критичної інфраструктури мають бути віднесені: Центр захисту критичної інфраструктури (при його утворенні); суб'єкти Єдиної державної системи цивільного захисту; суб'єкти Єдиної системи запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків; оператори об'єктів критичної інфраструктури; органи місцевої влади.

Окрім виконання функцій захисту об'єктів критичної інфраструктури, що були визначені законодавством та покладені на відповідальні відомства в рамках існуючих державних систем, що є елементами загальної системи забезпечення національної безпеки України, передбачається доручити їм такі специфічні функції як:

– підготовка (узагальнення) пропозицій щодо переліку об'єктів критичної інфраструктури, що віднесені до сфери своєї компетенції;

– формування (узагальнення) пропозицій щодо вдосконалення нормативно-правової бази в сферах національної безпеки і оборони, пов'язаних із захистом об'єктів критичної інфраструктури (за сектором або загрозою);

– взаємодія через "секторальний" ситуаційний центр із відповідним підрозділом Центру захисту критичної інфраструктури; аналіз та оцінка загроз об'єктам (та на об'єктах) критичної інфраструктури в секторі;

– участь в роботі та стимулювання роботи галузевих (або орієнтованих на розгляд певних типів загроз) експертних/консультативних рад з питань захисту критичної інфраструктури;

– формування пропозицій щодо проекту державної

цільової програми в сфері захисту критичної інфраструктури;

– здійснення перевірок забезпечення захисту критичної інфраструктури;

– участь у розробці та впровадженні стандартів, норм та регламентів захисту критичної інфраструктури.

Безумовно створення системи захисту критичної інфраструктури потребуватиме внесення в вітчизняне законодавство відповідних нововведень. В Зеленій книзі запропоновано здійснити це шляхом прийняття окремого Закону України "Про захист критичної інфраструктури", яким врегулювати такі питання.

– щодо утворення Центру з питань захисту критичної інфраструктури;

– щодо визначення секторів та відомств, що відповідають за кожен сектор;

– щодо процедури включення об'єктів до переліку критичної інфраструктури (організація процесу включення об'єктів до переліку та загальні критерії віднесення об'єктів до критичної інфраструктури);

– щодо запровадження порядку зміни режимів функціонування системи захисту критичної інфраструктури в залежності від визначеного рівня загроз;

– щодо формування Національного плану дій із захисту критичної інфраструктури та його періодичного перегляду.

Причому Кабінет Міністрів України своїми постановами має затверджувати: Положення про Центр з питань захисту критичної інфраструктури; перелік секторів критичної інфраструктури України та відомств, що визначаються відповідальними за кожен сектор; процедуру включення об'єктів до переліку критичної інфраструктури.

Висновки. 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.

Нині ми можемо спостерігати поступове усвідомлення концепції захисту критичної інфраструктури в середовищі вітчизняних експертів. Зелена книга, яка в силу жанру, мала підняти питання та ініціювати широку дискусію, без сумніву виконала своє завдання. Крім того низка аналітичних матеріалів та публікації, експертних семінарів та конференцій з даної тематики, які передували виходу Зеленої книги, надали підґрунтя для роботи.

Треба відмітити, що захист критичної інфраструктури – це не просто оновлення термінів в чинному законодавстві, це впровадження нового підходу. Основними його складниками є створення безпекового партнерства між всіма заінтересованими сторонами, організація комплексної оцінки загроз критичній інфраструктурі та їх впливу на рівень національної безпеки в окремих її складових, створення механізму моніторингу та попередження кризових ситуацій, що пов'язані із функціонуванням критичної інфраструктури.

Переваги концептуального підходу, основаного на понятті – "критична інфраструктура", що дозволяє системно вирішувати питання захисту критично важливих для життєдіяльності держави, безпеки її громадян та довкілля систем і об'єктів та регіональної безпеки, створює можливості для більш ефективного управління ризиками на глобальному, регіональному та національному рівнях.

Список використаної літератури

1. Бірюков Д.С., Кондратов С.І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. – К.: НІСД, 2012. – 96 с.

2. Концепція захисту критичної інфраструктури: стан, проблеми та перспективи її впровадження в Україні : зб. матеріалів міжнар. наук.-практ. конф. (7-8 листопада 2013 р., Київ – Вишгород) / упоряд. Д. С. Бірюков, С. І. Кондратов.– К. : НІСД, 2014. – 148 с.

3. SWD(2013) 318 final "On a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure". – [Електронний ресурс]. – Режим доступу:

http://ec.europa.eu/energy/infrastructure/doc/critical/20130828_epcip_commission_staff_working_document.pdf

4. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/NOT/?uri=CELEX:32008L0114

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

6. Про Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні : Постанова Верховної Ради України // ВВР. – 2006. – № 15. – ст.131.

7. Зелена книга з питань захисту критичної інфраструктури в Україні [Електронний ресурс]. – НІСД, 2015. – Режим доступу: http://www.niss.gov.ua/public/File/2015_table/Green%20Paper%20on%20CIP_ua.pdf

8. Порядок організації і режиму роботи Урядового центру з безпеки (Польською мовою) http://isap.sejm.gov.pl/DetailsServlet?id=WDU20110860471