ЗЕЛЕНА КНИГА З ПИТАНЬ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

(друга версія проекту документа)

Національний інститут стратегічних досліджень

Підготовлено у Національному інституті стратегічних досліджень із залученням українських та зарубіжних експертів і за підтримки Офісу зв'язку НАТО в Україні

Київ - 2014

Передмова

Останніми роками в діяльності експертів як на національному, так і на міжнародному рівнях все більшої популярності набуває такий інструмент стимулювання і організації професійних дискусій як видання «зелених книг» за конкретною проблематикою з подальшим широким обговоренням питань, піднятих у них для досягнення певного консенсусу. Зелені книги не мають чітко визначеного і загально прийнятого формату, але у політичній сфері вони, зазвичай, презентують певні варіанти діяльності держави або об'єднання держав (наприклад, ЄС), які виносяться на широке обговорення і не містять зобов'язань щодо вжиття конкретних заходів. У багатьох випадках видання «зеленої книги» з конкретної проблематики передує наступному етапу – розробці та виданню «білої книги» або іншого офіційного документу, де офіційно формулюються пропозиції щодо розв'язання певної проблеми.

З початку XXI століття у світі відбулися глобальні безпекові зміни, які стали наслідками, серед іншого, кризи сучасних систем управління. Не зважаючи на стрімкий розвиток передових технологій, зокрема в ІТ-сфері, управління складними системами відбувається в умовах скорочення горизонту або навіть неспроможності прогнозування малоймовірних надзвичайних ситуацій комплексного характеру. До непередбачуваних за своїми наслідками та масштабами катастрофічних подій слід віднести, наприклад, такі різнопланові події, як терористичні атаки 11 вересня 2001 р. у США, ураган «Катрина» 2005 р. у США, світова фінансова криза 2008 р., руйнівні землетрус і цунамі, які викликали важку ядерну кризу на АЕС «Фукусіма» в Японії у 2011 р., події так званої «арабської весни» 2011 р. та сучасна криза навколо України.

Аналіз цих та інших масштабних надзвичайних ситуацій комплексного характеру, винесені з них уроки з усією очевидністю висувають на порядок денний проблему забезпечення захисту критично важливих для існування цивілізованої держави об'єктів, систем та ресурсів (критичної інфраструктури) від усіх видів загроз і загроз комплексного характеру. Цей безпековий напрям, започаткований у США ще у період *холодної війни*, став активно розвиватися у провідних країнах світу на початку нинішнього століття, як відповідь на різке зростання терористичних загроз. Захист критичної інфраструктури 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 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 у листопаді 2005 р. випустила *Зелену книгу щодо Європейської програми захисту критичної інфраструктури*[1], а згодом, у 2006 р., коли завершився етап консультацій між членами ЄС, була запущена в дію *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 оцінку потреб у підвищенні рівня їхнього захисту (грудень 2008)[4]. Захист критичної інфраструктури енергопостачання Декларацією Чиказького саміту (20 травня 2012 р.) було віднесено до числа пріоритетних напрямів забезпечення енергетичної безпеки для держав-членів НАТО та самого Альянсу.

Вважаємо, що з огляду на ті драматичні події, що відбуваються на Сході України, під час яких не тільки гинуть люди, а й руйнуються критично важливі для життєдіяльності регіону, а також усієї країни об'єкти та системи, закладення основ для створення системи захисту критичної інфраструктури в Україні та гармонізації відповідних підходів з тими, що активно запроваджуються в ЄС та НАТО, є актуальним завданням, виконання якого сприятиме удосконаленню механізмів забезпечення національної безпеки та посилюватиме 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, робочою групою українських експертів, створеною при Національному інституті стратегічних досліджень (далі – НІСД), за сприяння Офісу зв'язку НАТО в Україні, а також за участі експертів з країн-членів Альянсу, було підготовлено проект Зеленої книги з питань захисту критичної інфраструктури в України (далі – Зелена книга). Після погодження тексту Зеленої книги її буде опубліковано на сайті НІСД, а також розіслано усім заінтересованим державним органам, підприємствам, науковим і науково-дослідним інститутам та іншим організаціям для широкого обговорення окресленої у публікації проблематики. За результатами обговорення будуть розроблені рекомендації щодо подальших кроків у напрямі забезпечення захисту критичної інфраструктури в Україні.

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 фактори у теперішніх умовах роблять особливо актуальною проблему 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 існує такі системи, об'єкти та ресурси, знищення або пошкодження яких матиме суттєвий 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 визначає повноваження та компетенцію державних органів у цій сфері, встановлює 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, які прийнято відносити до критичної інфраструктури. В результаті чого спостерігається домінування відомчих підходів, низький рівень взаємодії, координації дій та управління ресурсами, особливо, у випадку надзвичайних державного рівня.

Дана Зелена книга розроблена з метою сприяння експертному обговоренню на національному рівні основних проблем запровадження концептуального підходу «захист критичної інфраструктури» в Україні та можливих напрямів їх розв'язання. Реалізація такого підходу в нашій країні зробила б вагомий внесок у процес системного реформування усього сектору безпеки держави, наблизивши його структуру і функції до тих, що вже існують у державах-членах ЄС та НАТО.

При підготовці 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, 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».

Розробка Зеленої книги з питань захисту критичної інфраструктури в Україні здійснювалася за підтримки Офісу зв'язку НАТО в Україні у рамках виконання щорічного Плану дій Україна-НАТО на 2014 рік. Робота над Зеленою книга була виконана у НІСД за активної участі залучених вітчизняних і зарубіжних експертів (список експертів представлений в Додатку А).

2. Ціль, принципи побудови та основні завдання захисту критичної інфраструктури

Під захистом критичної інфраструктури розуміють увесь комплекс заходів, реалізований в нормативно-правових, організаційних, техніко-технологічних інструментах запобігання загроз, зниження ризиків та усунення вразливостей, мінімізації наслідків та відновлення критичної інфраструктури у випадку надзвичайних ситуацій (збоїв, аварій тощо), які спрямовані на забезпечення захищеності (охорони), безпеки та належного функціонування усіх її елементів - об'єктів, систем, мереж (далі скорочено – об'єктів) - в умовах мирного часу.

2.1. *Ціль захисту критичної інфраструктури* полягає в недопущенні руйнування чи завдання невиправної шкоди, припинення функціонування або втрати контролю над об'єктами критичної інфраструктури внаслідок дії чинників техногенного, природного, соціально-політичного та воєнного характеру, або їх комбінації.

2.2. *Основні принципи побудови системи захисту критичної інфраструктури* 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 перелічене нижче.

Принцип координованості зусиль, що означає:

- узгоджений розвиток нормативно-правових, організаційних та науково-технологічних інструментів, призначених для виконання завдань захисту критичної інфраструктури;
- планування безпеки на національному рівні, виходячи із захисту національних інтересів, шляхом створення механізмів впливу на стан захищеності критичної інфраструктури;
- урахування необхідності забезпечення захищеності критичної інфраструктури при плануванні, визначенні пріоритетів та оцінці соціально-економічного розвитку країни;
- функціонування єдиного центру оцінки стану захищеності критичної інфраструктури, прогнозування загроз та оцінки ризиків для 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.

Принцип компліментарного розвитку, відповідно до якого запровадження концепції захисту критичної інфраструктури має здійснюватися шляхом:

- поступового впровадження нормативно-правових, організаційних та науково-технологічних інструментів, на основі яких повинні вдосконалюватися засоби та заходи із забезпечення захисту та безпеки критичної інфраструктури;
- розробки методології ідентифікації об'єктів критичної інфраструктури (визначення переліку) на основі наявних даних;
- періодичної оцінки загроз, ризиків та уразливостей об'єктів критичної інфраструктури з використанням відповідного досвіду, набутого, насамперед, в ядерній галузі та у банківському секторі економіки;
- впровадження результатів вже виконаних науково-прикладних досліджень та перспективного планування науково-технічних досліджень щодо безпеки критичної інфраструктури, застосування високотехнологічних рішень;
- планування розвитку кадрового забезпечення з урахуванням наявних можливостей спеціалізованих учбових закладів.

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:

- використання ресурсів як держави, так й приватного сектору для досягнення цілей забезпечення захисту критичної інфраструктури;
- декларування безпеки об'єкту власником (оператором), ведення паспортизації об'єктів критичної інфраструктури;
- залучення громадськості та експертного співтовариства, використання консультаційних (дорадчих) рад при визначенні вимог до безпеки об'єктів критичної інфраструктури.

Принцип побудови комплексного захисту, згідно з яким формування захисту критичної інфраструктури здійснюється на основі:

- використання єдиної понятійної та методологічної бази для аналізу загроз критичній інфраструктурі;
- урахування та оцінки комплексу загроз об'єктам критичної інфраструктури, спричинених дією чинників техногенного, природного, соціально-політичного та воєнного характеру;
- урахування особливостей функціонування захисту критичної інфраструктури в мирний час (як в умовах повсякденного функціонування, так й в умовах надзвичайної ситуації та режиму надзвичайного стану);
- надання пріоритету заходам з попередження загроз надзвичайних ситуацій перед заходами з підвищення готовності до реагування і ліквідації наслідків, таких ситуацій, використання ризик-орієнтованих методів аналізу та прогнозування.

Принцип забезпечення конфіденційності означає, що інформація про вразливості та конкретні характеристики систем фізичного захисту об'єктів, 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.

2.3. Виходячи з цілі та принципів побудови захисту критичної інфраструктури, можна сформулювати такі *основні завдання:*

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

- підготовку 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 зовнішніх факторів природного та соціально-політичного характеру, техногенних чинників, оцінки ризиків як на рівні окремих об'єктів, так і для регіонів та держави в цілому;
- підготовку національної програми захисту критичної інфраструктури;
- підтримку функціонування мережі ситуаційних центрів;
- підтримку та узгодження роботи експертних та консультаційних рад різних рівнів з питань розробки та впровадження нормативних, організаційних та технологічних інструментів забезпечення захисту критичної інфраструктури;
- підготовка бази даних критичної інфраструктури;
- розроблення планів реагування на надзвичайні ситуації;
- формування комплексної науково-дослідної програми з питань захисту критичної інфраструктури;
- здійснення взаємодії зі структурами ЄС та державними органами країн-членів ЄС.

2) Забезпечення готовності до дій у надзвичайних ситуаціях, запобігання загрозам, реагування на надзвичайні ситуації, пов'язані з функціонуванням критичної інфраструктури; забезпечення умов для відновлення функціонування об'єктів критичної інфраструктури, а також для мінімізації та ліквідації наслідків надзвичайних ситуацій на цих об'єктах або об'єктах, пов'язаних з її функціонуванням, що включає:

- мінімізацію ризиків для функціонування критичної інфраструктури, зокрема, локалізація та нейтралізація загроз на ранніх етапах їх зародження
- забезпечення безпеки населення та територій від найбільш небезпечних радіологічних, хімічних, бактеріологічних чинників, що пов'язані із можливими надзвичайними ситуаціями на об'єктах критичної інфраструктури;
- забезпечення фізичного захисту об'єктів критичної інфраструктури,

запобігання несанкціонованим діям (в т.ч. терористичних актів) 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;

- розроблення та впровадження інженерно-технічних заходів цивільного захисту;
- 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;
- формування матеріальних резервів, оцінка та інвентаризація ресурсів;
- забезпечення стабільного функціонування критичної інфраструктури в умовах надзвичайних ситуацій.

3) Підтримка прийняття рішень щодо захисту критичної інфраструктури, включаючи

- ідентифікацію об’єктів критичної інфраструктури; ведення автоматизованого реєстру критичної інфраструктури; збір, узагальнення та аналіз даних щодо об’єктів критичної інфраструктури та їх функціонування;
- здійснення постійного моніторингу, аналізу та прогнозування загроз об’єктам критичної інфраструктури;
- ідентифікацію природних, техногенних і соціально-політичних чинників виникнення надзвичайних ситуацій, пов’язаних із функціонуванням критичної інфраструктури;
- визначення необхідних ресурсів для забезпечення захисту критичної інфраструктури, населення та територій від надзвичайних ситуацій, пов’язаних з функціонуванням критичної інфраструктури;
- підтримку прийняття рішень щодо реагування на надзвичайні ситуації (в т.ч. евакуації населення);
- аналіз ефективності організаційно-технічних засобів стосовно зниження ризиків життєдіяльності в умовах можливих і реальних надзвичайних ситуацій спричинених порушенням функціонування 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;
- запровадження автоматизованих систем раннього виявлення надзвичайних ситуацій та оповіщення про них;
- розробку та впровадження стандартів, норм та регламентів захисту критичної інфраструктури;
- формування паспортів об’єктів критичної інфраструктури, а також

паспортів ризику адміністративно-територіальних одиниць;

– здійснення перевірок та оцінки захищеності критичної інфраструктури.

5) Міжнародне співробітництво в сферах цивільного захисту, протидії тероризму та кіберзагрозам.

Слід відмітити, що заходи, згадані у наведеному вище переліку завдань, значною мірою охоплюються рамками існуючих в Україні систем з протидії надзвичайним ситуаціям, тероризму, кіберзагрозам, забезпечення обороноздатності держави.

Проте особливістю підходу до захисту критичної інфраструктури є те, що він має бути побудований із урахуванням усіх видів систем, мереж і об'єктів, комплексної оцінки їх взаємовпливів — взаємозалежностей (каскадних ефектів), включаючи й ті, що не пов'язані з об'єктами підвищеної небезпеки, проте відіграють важливу роль в тому числі при реагуванні на надзвичайні ситуації (наприклад, важливі мости на залізниці та автошляхах).

Питання для обговорення:

1. Чи правильно, як на Вашу думку, сформульована ціль захисту критичної інфраструктури?
2. Чи може (має) будуватися захист критичної інфраструктури для умов особливого періоду, враховуючи особливості мобілізації чи режиму воєнного стану?
3. Чи може (має) будуватися захист критичної інфраструктури для умов відбудовного періоду?
4. Чи має захист критичної інфраструктури бути розширений та включати завдання щодо протидії економічним загрозам?
5. Які б могли бути додаткові завдання для захисту критичної інфраструктури?

3. Визначення об'єктів критичної інфраструктури в Україні

3.1. Визначення терміну «критична інфраструктура»

Термін «критична інфраструктура» неодноразово використовувався в нормативно-правових документах в Україні, проте його дефініція й досі відсутня 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, у подальшому активна робота у цьому важливому напрямі припинилася.

В Стратегії національної безпеки «Україні у світі, що змінюється» в четвертому розділі «Стратегічні цілі та основні завдання політики національної безпеки» серед ключових завдань політики національної безпеки у внутрішній сфері одним із шляхів зміцнення енергетичної безпеки названий: «дієвий захист критичної інфраструктури паливно-енергетичного комплексу від еколого-техногенних впливів та зловмисних дій», а одним із напрямів забезпечення інформаційної безпеки — «забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури».

Нині відсутність терміну «критична інфраструктура» в українському законодавстві, і як наслідок, відсутність переліку об'єктів, які слід віднести до неї, створюють перешкоду для ефективного виконання 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 02.03.2014р.), на виконання якого Міністерству внутрішніх справ України наказується забезпечити «посилену охорону об'єктів енергетики та критичної інфраструктури».

Зважаючи на викладені вище міркування і враховуючи, що саме США є лідером у розробці підходів до забезпечення національної безпеки на основі фундаментального терміну «критична інфраструктура», пропонуємо використати «американську формулу» і визначити цей термін таким чином:

Критична інфраструктура України – це системи та ресурси, фізичні чи віртуальні, настільки життєво важливі для країни, що їх недієздатність або знищення підриває національну безпеку, національну економіку, здоров'я або безпеку населення, або має своїм результатом будь-яку комбінацію з переліченого вище.

3.2. Категорії об'єктів, які повністю або частково можуть бути включені до переліку об'єктів критичної інфраструктури

Як вже відзначалося, 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 внутрішньовідомчий характер.

Дійсно, 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];
- об'єкти, які включені до Державного реєстру потенційно небезпечних об'єктів[6];
- об'єкти підвищеної небезпеки[7] (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[8]);
- об'єкти, які віднесені до категорій з цивільного захисту;
- важливі державні об'єкти[9];
- об'єкти, що підлягають обов'язковій охороні підрозділами Державної служби охорони за договорами[10];
- об'єкти, які підлягають охороні і обороні в умовах надзвичайних ситуацій і в особливий період[11];
- особливо важливі об'єкти електроенергетики[12;
- особливо важливі об'єкти нафтогазової галузі[13];
- Національна система конфіденційного зв'язку[14];

- платіжні системи[15];
- чергово-диспетчерська система екстреної допомоги населенню за єдиним безкоштовним телефонним номером виклику екстрених служб 112[16];
- аварійно-рятувальні служби;
- нерухомі об’єкти культурної спадщини[17].

Нині 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 № 11від 9 січня 2014 р.[18]). 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.

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[19]).

Питання для обговорення:
1. Які інші існуючі категорії об’єктів, на Вашу думку, можуть бути віднесені (повністю чи частково) до критичної інфраструктури в Україні? Якщо такі категорії не названі, то вкажіть для них, якими нормативними актами регулюється:
- механізм (процедура) визначення даної категорії об’єктів;
- порядок доступу (чи є перелік об’єктів даної категорії загальнодоступним);
- суб’єкти, що здійснюють захист даної категорії об’єктів;
- механізми захисту, охорони, забезпечення безпеки даних об’єктів тощо;
- координація суб’єктів забезпечення захисту та безпеки функціонування об’єктів даної категорії.
2. Чи всі об’єкти даної категорії мають на Вашу думку бути включені до переліку об’єктів критичної інфраструктури?

3.3. Ідентифікація елементів критичної інфраструктури

При визначенні елементів критичної інфраструктури (віднесенні об’єктів до критичної інфраструктури) враховують 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:

a) економічна безпека (вплив на ВВП, розмір економічних втрат як прямих, так і непрямих, частки продукції на ринку, чисельності зайнятих співробітників, податкових надходжень у бюджет);
b) 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);
c) внутрішньополітична й державна безпека (втрата впевненості в дієздатності влади, авторитету держави, порушення керованості державою);
d) обороноздатність (зниження боєздатності збройних сил, розголошення таємної інформації);
e) 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 може бути здійснений в декілька ітерацій. Початковий перелік може бути складений з об'єктів, зазначених в категоріях попереднього підпункту. Далі може бути побудована модель взаємозв'язків між об'єктами критичної інфраструктури та оцінені наслідки можливого припинення їх функціонування (аварії тощо) на довготривалий період.

Потрібно також сказати, що проблема ідентифікації об'єктів критичної інфраструктури в Україні неодноразово піднімалася з огляду на необхідність захисту від окремих загроз. Наприклад, у Концепції боротьби з тероризмом (квітень 2013р.[20]) вказується про «наявність на території України потенційно-небезпечних та уразливих у терористичному плані об'єктів...» та необхідність «розроблення та затвердження критеріїв віднесення об'єктів (незалежно від форм власності) до переліку об'єктів можливих посягань».

Питання для обговорення:
1. Які показники для існуючих категорій об'єктів можна використовувати, на Вашу думку, для ідентифікації об'єктів критичної інфраструктури?
2. Як встановлювати граничні значення для показників, за якими будуть відносити ти, чи інші об'єкти до критичної інфраструктури?

4. Основні загрози критичній інфраструктурі

Відповідно до характеру походження загрози критичній інфраструктурі можна умовно поділити на такі категорії: техногенні, природного характеру, соціально-політичного характеру (включаючи терористичні), комбіновані загрози (являють собою якусь комбінацію з перелічених вище), а також воєнні, розгляд яких виходить за рамки даного документу. Очевидно, що комбіновані загрози та загрози, реалізація яких може призвести до катастрофічних і різноманітних каскадних ефектів внаслідок взаємозалежності елементів критичної інфраструктури, потребують особливої уваги.

4.1. Розглядаючи *загрози техногенного походження*, слід відмітити, що в Україні через високий рівень зношеності основних фондів[i] існує загроза виникнення аварій на об’єктах підвищеної небезпеки, об’єктах електроенергетики та мережах життєзабезпечення. За даними ДСНС[ii] аварії на 955 об'єктах, що внесені до Державного реєстру об’єктів підвищеної небезпеки, можуть призвести до виникнення надзвичайних ситуацій державного або регіонального рівня.

Приклад 1. У промисловому комплексі України функціонує біля тисячі об’єктів, на яких зберігається або використовується у виробничій діяльності понад 300 тис. т хімічно небезпечних речовин, а у зонах можливого хімічного забруднення мешкає близько 9,34 млн осіб (20,6% населення країни).

Приклад 2. За оцінками експертів, 14% залізничних мостів мають незадовільний технічний стан. Серед мостів загального користування, що підпорядковані Укравтодору, не відповідають вимогам експлуатації та безпеки руху 46%.

Приклад 3. Близько 5 тис. км (14%) лінійної частини магістральних газопроводів побудовані в 60-70 роки і відпрацювали свій амортизаційний термін.

Приклад 4. За даними ДСНС в аварійному та ветхому стані знаходяться 38,2% протяжності водопровідних мереж та 36,4% протяжності каналізаційних мереж[iii].

Заслуговує на серйозну увагу й 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.

Приклад 5. У жовтні 2013 р. мало місце незаконне втручання в роботу автоматизованих систем та комп'ютерних мереж Мін’юсту.

Приклад 6. У березні 2014 р. DDoS-атаки перешкоджали роботі Апарату РНБОУ.

4.2. До *загроз природного характеру* можна віднести такі їх види:

– метеорологічні (снігопади, ожеледь, хуртовини, зливи, градобій, заморозки, засухи);
– гідрологічні (повені, селі, паводки, підтоплення);
– геологічні (небезпечні екзогенні геологічні процеси - зсуви, просідання та карст);
– геліофізичні (пожежі).

Серед перелічених видів загроз слід виділити метеорологічні, частота яких значно підвищилася останніми десятиліттями.

Приклад 7. У листопаді 2000 р. внаслідок обледеніння було пошкоджено понад 20 тис. ліній електропередач, понад 307 тис. залізобетонних опор ЛЕП, стали

[i] *Примітка:* в т.ч. через "зношеність основних фондів, зокрема об'єктів підвищеної небезпеки, комунальної інфраструктури населених пунктів, очисних споруд підприємств", що зазначено як загроза в Стратегії національної безпеки України «Україна у світі, що змінюється» (п.3.2.6. "Наявність небезпечних екологічних і техногенних викликів і загроз").

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

[iii] *Примітка:* там само, стор.146, 148.

непридатними для подальшої експлуатації понад 34 тис. т дроту, відключено понад 2000 сільських телефонних станцій і т.д.

Приклад 8. В останній декаді січня 2014 р. внаслідок сильного снігу, снігопаду з дощем, поривів вітру зі швидкістю понад 25 м/с сталося обледеніння та пошкодження повітряних ЛЕП, спрацювання систем автоматичного захисту ЛЕП, було знеструмлено 1605 населених пунктів, на автошляхах України через снігові замети було ускладнено або повністю припинено рух автотранспорту на багатьох територіях.

Серед гідрологічних загроз за серйозністю наслідків для критичної інфраструктури слід 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 загрожує екологічній безпеці в районах розміщення об’єктів підвищеної небезпеки, захисних гребель і дамб шламосховищ і ставків-відстійників, ускладнення інженерно-геологічних умов експлуатації промислових споруд та інженерних мереж промислово-міських агломерацій.

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

За час проведення антитерористичної операції в східних регіонах держави значно зросла ймовірність аварій на об’єктах підвищеної небезпеки через дії терористів. Наведемо тільки окремі приклади.

Приклад 9. Загорання сухої сірки, що сталося на території колишнього заводу підприємства “Хімпром” у м. Слов’янську (5 червня 2014 р.).

Приклад 10. В результаті бойових дій на Донецькій, Придніпровській і Південній залізницях пошкоджено понад 190 об'єктів залізничної інфраструктури, з яких, зокрема, 49 об’єктів колійного господарства, 74 – електропостачання, 30 – автоматики та зв'язку, 11 – будівель та цивільних споруд, що забезпечують функціонування пасажирського господарства тощо.

Безумовно, найсерйознішою є 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.

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.

Питання для обговорення:
1. Від яких загроз потрібно захищати критичну інфраструктуру?
2. Які комплексні оцінки загроз для об’єктів, що прийнято відносити до критичної інфраструктури, Вам відомі?
3. Чи правильно визначені пріоритети захисту (впорядковані загрози за їх значимістю), які суттєві загрози не згадуються, або згадані непропорційно їхній значимості?
4. Чи повинні воєнні загрози розглядатися разом з іншими невоєнними загрозами критичній інфраструктурі?
5. Чи потрібно розглядати також економічний блок загроз, виходячи з міркування про одноманіття наслідків загроз в незалежності від їхнього характеру?

5. Напрями розвитку механізмів захисту критичної інфраструктури в Україні

5.1. 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 їхніх національних критичних інфраструктур, відповідних підходів, які застосовуються в ЄС, та НАТО, з однієї сторони, а також аналізу ситуації щодо захисту таких інфраструктур в Україні, з іншої сторони, пропонуємо такі ключові напрями розвитку механізмів захисту критичної інфраструктури в нашій державі:

– удосконалення нормативно-правових та організаційних механізмів захисту критичної інфраструктури;
– визначення пріоритетних секторів критичної інфраструктури та органів державної влади, які відповідають за формування та реалізацію державної політики щодо забезпечення захисту відповідних об’єктів критичної інфраструктури (див. додаток Б);
– 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 та запобігання виникненню на них надзвичайних ситуацій;
– удосконалення механізмів державно-приватного партнерства;
– 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;
– 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 протидії тероризму);
- розвиток міжнародного співробітництва з питань захисту критичної інфраструктури.

5.2. Для запровадження загального підходу до захисту критичної інфраструктури в Україні першочерговими кроками можна вважати таке:

a) *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;
   - врегулювання порядку обміну інформацією, збору даних про об’єкти критичної інфраструктури, загрози та ризики, пов’язані із функціонуванням об’єктів критичної інфраструктури тощо.

b) *Інституційне 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;
   - аналіз та оцінка 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);

c) *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 поверхні Землі, систем прогнозування і підтримки прийняття рішень в умовах надзвичайних ситуацій;
   - удосконалення систем моніторингу, включаючи дистанційне зондування поверхні Землі, систем прогнозування і підтримки прийняття рішень в умовах надзвичайних ситуацій;

– 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.

а) 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;
– сприяння активізації 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.

Питання для обговорення:
1. Який орган, на Вашу думку, повинен координувати зусилля із захисту критичної інфраструктури?
2. Яким має бути статус національного ситуаційного центру із захисту критичної інфраструктури? Самостійний орган? Підпорядкований Президенту? У складі Апарату РНБОУ? Підпорядкований Уряду?
3. Які механізми інформаційної взаємодії можуть слугувати прикладом «найкращої практики» в Україні?
4. Які перешкоди існують для інформаційного обміну щодо загроз критичній інфраструктурі?

5.3. Слід значно активізувати зусилля, спрямовані на вирішення 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.

Питання для обговорення:
1. Чи вважаєте Ви, що необхідно проаналізувати стан виконання завдань щодо створення Урядової інформаційно-аналітичної системи з питань надзвичайних

ситуацій (УІАСНС); визначити місце і роль існуючих елементів УІАСНС у системі моніторингу і прогнозування надзвичайних ситуацій[iv]?
2. Як би Ви оцінили рівень взаємодії між окремими ситуаційним центрами в Україні?
3. На Вашу думку, чи буде доцільним перенесення досвіду забезпечення фізичної безпеки ядерних об'єктів, зокрема, впровадження національної проектної загрози, на захист об'єктів критичної інфраструктури в інших секторах?

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

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[v], 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 2004 р. ЄК оприлюднила офіційне повідомлення[21], 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 згаданому повідомленні зазначається, що через значну кількість об'єктів, які потенційно можуть бути віднесені до критичної інфраструктури ЄС, забезпечити їх захист на загальноєвропейському рівні неможливо, тому, слідуючи принципу субсидіарності, загальноєвропейським інституціям потрібно сконцентрувати зусилля на захисті тих об'єктів, припинення функціонування яких буде мати транскордонний вплив, залишивши за країнами ЄС відповідальність за решту об'єктів. При цьому, як наголошується в даному повідомленні, 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).

[iv] Див. постанову Кабінету Міністрів України від 9 січня 2014 р. №11 «Про затвердження Положення про єдину державну систему цивільного захисту» (стаття25).

[v] Повна офіційна назва угоди: Угода про асоціацію між Україною, з однієї сторони, та Європейським союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони.

В офіційному повідомленні №786 за 2006р.[22] ЄК рекомендувала всім країнам ЄС вжити заходів, зазначених в ЄПЗКІ, а саме:

- розробити національну програму захисту КІ 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.

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. Через високі технічні вимоги та унікальність даної інформаційної системи підтримка її функціонування оцінюється сумою понад 600 тис. євро щорічно[23].

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.

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

- загальних принципів захисту критичної інфраструктури;
- тлумачення основних термінів (див. додаток Г);

- визначення "контактного пункту"[vi].
- узгодженості щодо пріоритетності захисту критичної інфраструктури (вибору пріоритетних секторів та відповідних підсекторів критичної інфраструктури;
- методологій порівняння та визначення пріоритетних об'єктів в різних секторах;
- 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, зокрема[vii]:

- Директива №2005/89/ЄС щодо заходів з забезпечення безпеки постачання електроенергії та інвестицій в інфраструктуру [viii];
- Директива №2004/67/ЄС стосовно заходів щодо забезпечення безперервного постачання природного газу [ix];
- Директива №2005/65/ЄС Європейського Парламенту та Ради від 26 жовтня 2005 року про посилення безпеки портів [x]
- Регламент (ЄС) №725/2004 Європейського Парламенту та Ради від 31 березня 2004 року про посилення безпеки суден та портових споруд [xi];
- Директива 2004/49/ЄС Європейського Парламенту та Ради від 29 квітня 2004 року про безпеку залізниць у Співтоваристві, яка вносить зміни до Директиви Ради 96/18/ЄС про ліцензування підприємств залізничного транспорту та до Директиви 2001/14/ЄС про розділення пропускної здатності залізничних інфраструктур та стягнення платежів за використання залізничної інфраструктури та про сертифікацію безпеки (Директива про безпеку на залізницях)[xii];
- Регламент (ЄС) №336/2006 Європейського Парламенту та Ради від 15 лютого 2006 року про імплементацію Міжнародного кодексу з управління

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

[vii] Див. Додаток XXVII до Угоди про асоціацію

[viii] Directive 2005/89/EC concerning measures to safeguard security of electricity supply and infrastructure investment

[ix] Directive 2004/67/EC concerning measures to safeguard security of natural gas supply

[x] Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32005L0065

[xi] Regulation (EC) 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security

[xii] 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)

безпекою в рамках Співтовариства та скасування Регламенту Ради (ЄС) №3051/95[xiii].

Питання для обговорення:
1. На Вашу думку, які інші кроки потрібно зробити у цьому напрямі?
2. З якими міжнародними угодами пов'язаний захист критичної інфраструктури?
3. Які існуючі механізми співробітництва України з ЄС та окремими країнами-членами ЄС, пов’язані із захистом критичної інфраструктури?

[xiii] 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

Додаток А

Список учасників робочої групи щодо розробки Зеленої книги

№	ІМ'Я	ПРЕДСТАВЛЯЄ
1.	**Келдер** Керсті	**Офіс зв'язку НАТО в Україні** Керівник програм професійної підготовки
2.	**Ратчев** Валерій	**Женевський Центр демократичного контролю над збройними силами (DCAF)** (Болгарія), експерт
3.	**Атоєв** Костянтин Леонович	**Інститут кібернетики НАН України** Старший науковий співробітник
4.	**Білоконь** Володимир Миколайович	**Інститут проблем математичних машин і систем НАН України,** Старший науковий співробітник відділу обробки та відображення візуальної інформації
5.	**Бірюков** Дмитро Сергійович	**Національний інституту стратегічних досліджень** Головний консультант
6.	**Груздєв** Олексій Володимирович	**ПАТ «Укртранснафта»** Начальник управління охорони праці та промислової безпеки
7.	**Євдін** Олександр Миколайович	**УкрНДІ цивільного захисту ДСНС України** Перший заступник директора
8.	**Жилін** Артем Вікторович	**Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ»** Співробітник
9.	**Мохор** Володимир Володимирович	**Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ»** Начальник кафедри
10.	**Заславський** Володимир Анатолійович	**Київський національний університет ім. Т.Г. Шевченка** Начальник управління міжнародного науково-технічного співробітництва та інноваційних технологій
11.	**Іванюта** Сергій Петрович	**Національний інституту стратегічних досліджень** Головний консультант
12.	**Кондратов** Сергій Іванович	**Національний інституту стратегічних досліджень** Старший науковий співробітник
13.	**Куницький** Ігор Миколайович	**ДП НАЕК «ЕНЕРГОАТОМ»** Начальник відділу протидії актам ЯТ, СП та ООЖ ДФЗ ядерних установок та ядерних матеріалів дирекції з фізичного захисту і спеціальної безпеки
14.	**Мороз** Оксана В'ячеславівна	**Міненерговугілля України** Головний спеціаліст Департаменту стратегії розвитку ПЕК
15.	**Насвіт** Олег Іліодорович	**Національний інституту стратегічних досліджень** Завідувач сектору екологічної та техногенної безпеки

16.	**Фаль** Олексій Михайлович	**Інститут кібернетики НАН України** Провідний науковий співробітник

Додаток Б

Перелік секторів, які пропонується віднести до критичної інфраструктури України

I. Паливно-енергетичний комплекс
- а) електроенергетика
- б) паливна промисловість
- в) вугільна промисловість

II. Транспорт
- а) залізничний та автомобільний
- б) повітряний
- в) морський та річковий
- г) трубопровідний транспорт

III. Фінансово-банківський сектор
- а) платіжні системи
- б) фондова біржа
- в) виготовлення цінних державних паперів

IV. Телекомунікації та зв'язок
- а) урядовий зв'язок та е-урядування
- б) мобільний, фіксований зв'язок та широкосмуговий доступ
- в) телерадіомовлення
- г) поштовий зв'язок

V. Хімічна промисловість

VI. Харчова промисловість та агропромисловий комплекс

VII. Мережі життєзабезпечення

а) об'єкти комунального господарства та забезпечення життєдіяльності великих міст

б) метрополітен

VIII. Органи влади, правосуддя та правопорядку

а) органи виконавчої влади

б) органи правосуддя

в) установи кримінально-виконавчої системи

г) дипломатичні установи України за кордоном, дипломатичні та консульські представництва інших держав в Україні

IX. Служби екстреної допомоги та реагування на надзвичайні ситуації

а) чергово-диспетчерська система екстреної допомоги населенню за єдиним безкоштовним телефонним номером виклику екстрених служб 112 (Система екстреної допомоги - «112»)

б) сили цивільного захисту

в) органи внутрішніх справ

г) системи оповіщення

д) Державна служба медицини катастроф

X. Охорона здоров’я населення та природного середовища

а) управління відходами та небезпечні матеріали (ХБРЯ)

XI. Культурна спадщина та місця проведення масових культурних та спортивних подій

а) нерухомі пам’ятки культурної спадщини

б) стадіони, концертні та спортивні зали тощо.

XII. Воєнна сфера

а) оборонно-промисловий комплекс

б) логістичне забезпечення військових формувань і правоохоронних органів України

в) об’єкти підвищеної небезпеки.

Додаток В

Довідкова інформація до розділу 5

1. 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 1992 р. 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. Остання спроба у цьому напрямі була зроблена в Апараті РНБОУ у період 2010–2013 рр.

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 1996 р., 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.

Необхідність у створенні національного ситуаційного центру знайшла своє певне відображення у затвердженому в 2012 р. 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)[27].

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»[28].

Ситуаційні центри створюються і розвиваються в окремих крупних корпораціях, зокрема, в ядерній енергетиці. Наприклад, НАЕК «Енергоатом» планує запровадити нову систему радіаційного моніторингу 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.

2. Попередження можливих кризових ситуацій

Потрібно зазначити, що ефективне попередження загроз критичній інфраструктурі можливе лише при наявності інструментів та механізмів для визначення надзвичайних ситуацій та їх недопущення (пом'якшення) з тим, щоб вони не переростали у кризові ситуацій державного рівня.

Нині в системі забезпечення національної безпеки України відсутній дієвий механізм моніторингу та формування рішень щодо попередження можливих «кризових ситуацій». Дане питання залишилося невирішеним як в організаційному, так й в нормативно-правовому аспектах. Дійсно, на відміну від термінів «надзвичайний стан» та «надзвичайна ситуація», для яких в чинному законодавстві чітко прописані механізми введення режиму надзвичайного стану та оголошення надзвичайної ситуації (державного, регіонального чи місцевого рівня), термін «кризова ситуація» визначений лише у вузькопрофільних нормативних документах (цивільна авіація, фінансовий ринок, фізичний захист ядерних матеріалів та установок). Крім того, за винятком економічної та продовольчої безпеки, відсутні індикатори та їх порогові значення, за якими можна було б визначати перехід системи забезпечення національної безпеки у стан «кризової ситуації», чи наближення до неї за окремими показниками.

Додаток Г

Таблиця В.1.

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

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 КІ 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.

Додаток Д

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 29.08.2002 р. № 1288 «Про затвердження Положення про Державний реєстр потенційно небезпечних об'єктів»

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

[8] *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

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

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

[11] *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»

[12] *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»

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

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

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

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

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

[18] *Постанова* Кабінету Міністрів України від 09.01.2014 № 11 "Про затвердження Положення про єдину державну систему цивільного захисту" http://zakon4.rada.gov.ua/laws/show/11-2014-%D0%BF

[19] *Рішення* Ради національної безпеки і оборони України від 28 серпня 2014 року "Про невідкладні заходи щодо захисту України та зміцнення її обороноздатності" http://president.gov.ua/documents/18125.html

[20] *Указ* Президента України від 25.04.2013 р. № 230/2013 «Про Концепцію боротьби з тероризмом» [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/230/2013

[21] *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/

[22] *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/

[23] *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/

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

[28] 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