НАЦІОНАЛЬНИЙ ІНСТИТУТ СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ
NATIONAL INSTITUTE FOR STRATEGIC STUDIES

ЗЕЛЕНА КНИГА З ПИТАНЬ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

Збірник матеріалів міжнародних експертних нарад

GREEN PAPER ON CRITICAL INFRASTRUCTURE PROTECTION IN UKRAINE

Proceedings of International Expert Meetings

Київ 2016

УДК 32.1, 323.285, 519.8
З—48

Упорядники:
Д. С. Бірюков, к. т. н.; *С. І. Кондратов*

За загальною редакцією доктора наук з державного управління, професора *О. М. Суходолі*

Зелена книга з питань захисту критичної інфраструктури в Україні : зб. мат-лів міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С.І. Кондратов; за заг. ред. О. М. Суходолі. – К. : НІСД, 2015. – 176 с.

ISBN 978-966-554-258-2

Представлено низку аналітичних матеріалів з питань захисту критичної інфраструктури в Україні, висвітлено актуальні питання створення нормативних, організаційних і методологічних основ у цьому безпековому напрямі. У частині І видання представлено Зелену книгу з питань захисту критичної інфраструктури в Україні, підготовлену в НІСД із залученням вітчизняних та іноземних експертів у зазначеній сфері. До частини ІІ видання увійшли окремі доповіді та повідомлення учасників міжнародних експертних нарад із питань захисту критичної інфраструктури, організовані НІСД протягом 2014–2015 рр., а також створеної при Національному інституті стратегічних досліджень 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.

Розраховано на представників органів державної влади, співробітників правоохоронних органів і спецслужб, представників промисловості, науковців, експертів, а також на широке коло читачів, які цікавляться відповідною проблематикою.

Volume editors: *D. Biriukov, S. Kondratov,*
General editor: *O. Sukhodolia,* Doctor of Public Administration, Professor

Greeen paper on Critical Infrastructure Protection in Ukraine: Proceedings of International Expert Meetings / vol. edt.: D. Biriukov, S. Kondratov; general edt. O. Sukhodolia. – Kyiv: NISS, 2015. – 176 p.

This volume presents analytical papers on Critical Infrastructure protection in Ukraine. Urgent issues of the establishment of legal, organizational and methodological foundations for ensuring security in this field are emphasized. In the Part I of this volume the Green Paper on Critical Infrastructure protection in Ukraine is presented. This document was prepared by the NISS under involvement of domestic and foreign experts in this field. Part II of this volume includes reports presented by participants of several international expert meetings on critical infrastructure protection, held by NISS in 2014-2015, as well as reports made by participants of the Interagency Expert Working Group on non-proliferation of WMD, counter-terrorism and critical infrastructure protection issues established by National Institute for Strategic Studies.

Intended for public authorities, law enforcement and intelligence agencies, industry, scientists and experts, as well as a wide range of readers interested in that problem.

ПЕРЕДМОВА

Підготовка та публікація зелених книг є поширеною практикою стимулювання й організації професійних дискусій щодо актуальних безпекових проблем і способів їх вирішення і на національному, і на міжнародному рівнях. Зазвичай видання зеленої книги з певної проблематики передує наступному етапу – розробленню й виданню офіційного документа, де формулюються основи державної політики, спрямованої на розв'язання окресленої проблеми. Дана Зелена книга присвячена питанням захисту критичної інфраструктури в Україні, напряму, що нині посідає важливе місце в забезпеченні національної безпеки країн – членів ЄС і НАТО, а також є елементом загальноєвропейської безпекової політики ЄС.

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

Захист критичної інфраструктури як безпековий напрям був започаткований у США ще в період *холодної війни*, а на початку нинішнього століття став активно розвиватися у провідних країнах світу як відповідь на різке зростання терористичних загроз. Цей безпековий напрям є пріоритетним і для таких міжнародних структур, як ЄС і НАТО, оскільки разом із перевагами та благами, які надають процеси глобалізації та інформатизації, посилюється економічна, фінансова, технологічна, ресурсна

взаємопов'язаність та взаємозалежність між окремими державами, їх об'єднаннями, а також між регіонами світу, що робить сучасне суспільство дуже вразливим до загроз, особливо спрямованих на «вузлові» пункти згаданих взаємозв'язків.

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

Драматичні події 2014–2015 рр. в Україні актуалізували для країни питання захисту інфраструктури, об'єктів і систем, важливих для життєдіяльності суспільства, та сформували потребу створення системи захисту критичної інфраструктури в Україні. На нашу думку, гармонізація підходів щодо її створення з активно запроваджуваними в ЄС і НАТО сприятиме вдосконаленню механізмів забезпечення національної безпеки та посилить потенціал нашої держави стосовно інтеграції в європейський безпековий простір. Біфуркаційний характер поточного історичного моменту відкриває перед нашою країною коридор додаткових можливостей для зменшення відставання від провідних країн світу і для визначення свого місця в системі європейської колективної безпеки, ревізія якої вже почалася.

У зв'язку з цим, з огляду на досвід підготовки зелених книг у ЄС та в країнах – членах НАТО, робочою групою українських експертів,

---

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

[2] *On a European* Programme for Critical Infrastructure Protection : COM/2006/786 final [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

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

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

створеною при Національному інституті стратегічних досліджень (*далі* – НІСД) за участі експертів із країн – членів НАТО й за сприяння Офісу зв'язку НАТО в Україні, було підготовлено проект Зеленої книги з питань захисту критичної інфраструктури в України.

Під час підготовки проекту Зеленої книги було використано результати роботи створеної при НІСД у 2011 р. Міжвідомчої експертної робочої групи (*далі* – 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, підготовлена НІСД аналітична доповідь[5], висновки та рекомендації проведеного НІСД круглого столу із зазначеної тематики (липень 2012 р.), а також міжнародної науково-практичної конференції «Концепція захисту критичної інфраструктури: стан, проблеми та перспективи її впровадження в Україні» (листопад 2013 р.) та серії міжнародних експертних нарад[6].

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

Обговорення тексту проекту Зеленої книги експертами, врахування пропозицій, надісланих зацікавленими державними органами, підприємствами, науковими й науково-дослідними інститутами сприяло представленню НІСД фінальної версії Зеленої книги з питань захисту критичної інфраструктури в України на міжнародній експертній нараді 15–16 жовтня 2015 р.

У збірник увійшли окремі доповіді й повідомлення учасників міжнародних експертних нарад з питань захисту критичної інфраструктури, організовані в НІСД протягом 2014–2015 рр.

---

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

[6]*Конференцію* організовано НІСД спільно з Офісом зв'язку та програмою професійного розвитку НАТО в Україні.

FOREWORD

Preparation and publication of "green papers" is a widespread practice to stimulate and organize professional discussion of topical security subjects and ways to address them both nationally and internationally. As a rule, publication of a "green paper" precedes the subsequent stage: development and publication of an official paper formulating essentials of the government policy to address the defined problem. This Green Paper reviews the issues of critical infrastructure protection in Ukraine – the area being a priority part of assurance of national security of the EU and NATO member states, as well as an component of the EU security policy at the pan-European level.

No doubt, global security developments seen in the world in the past two decades involve numerous crises of varied origins and nature. This indicates the shrinkage of forecasting horizon or even total lack of forecasting capability in the contemporary security management mechanisms, their inability to prevent low-probability emergencies of sophisticated nature, such as US terrorist attacks of 9/11, Hurricane Katrina in the US (2005), world financial crisis (2008), destructive earthquake and tsunami causing a Fukushima Daiichi Nuclear Power Plant accident in Japan (2011), events of the Arab Spring (2011), Russia's hybrid war against Ukraine, or this year's refugee crisis in the EU. Analysis of these, as well as the other large-scale and comprehensive challenges to regional and global security, as well as lessons learned from them clearly put on the agenda the need to assure protection of objects, systems and resources critical for the existence of the state (the critical infrastructure) against all types of threats and their combinations.

Protection of critical infrastructure as a security target emerged during the Cold War and became an actively developing trend in the leading countries in the beginning of this century in response to abrupt growth of a terrorist threat. This security area is seen as a priority by such international structures as the EU and NATO since, in addition to obvious benefits and advantages, globalization

and IT development increase economic, financial, technological and resource interfaces and interdependences between different countries and their alliances, as well as between world regions, making modern society highly vulnerable to threats – in particular those targeting the nodal points of the described interfaces.

Realization of the growing terrorist threats in Europe caused the European Commission to develop and, in November 2005, publish the Green Paper on the European Programme for Critical Infrastructure Protection, and subsequently, in 2006, on completion of the consultations between the EU countries, the European Programme for Critical Infrastructure Protection. Character of the EU approach specific for a community of independent states was reflected in the EC document entitled Protecting Europe's Critical Energy and Transport Infrastructure (February 2007) and in a special directive for the identification of critical infrastructure objects and assessment of a need to enhance their protection (December 2008). Protection of critical power supply infrastructure was named a priority focus for the assurance of energy security of NATO member states and the Alliance in general in the Declaration of the Chicago Summit (20 May 2012).

Dramatic events of 2014-2015 in Ukraine increased urgency of protection of infrastructure, objects and systems vital for the activity of the society and created a need to establish a critical infrastructure protection system for Ukraine. We believe that harmonization of approaches for its establishment with those actively implemented by the EU and NATO will facilitate improvement of national security mechanisms and enhance capabilities of our state regarding integration in the European security context. Bifurcate nature of the current historical moment opens a corridor of additional opportunities for our country to reduce the lag from the advanced nations and to find its place in the European collective security system whose revision is currently underway.

In this light, using the green paper preparation experience of the EU and NATO member states, the National Institute for Strategic Studies (NISS) has initiated development of a draft Green Paper for Critical Infrastructure Protection in Ukraine.

The Green Paper for Critical Infrastructure Protection in Ukraine was developed with the support of the NATO Liaison Office in Ukraine as part of the Ukraine-NATO 2014 and 2015 Annual National Cooperation Programs. Work on the Green Paper was completed by NISS with the active involvement of Ukrainian and international experts.

Inter alia, preparation of the draft Green Paper built on the results of work of the Interagency Expert Working Group for the

Suppression of Threat of Proliferation of Mass Destruction Weapons and Materials and Associated Terrorist Threats and Protection of Infrastructure Critical for State Activity (IEWG), established within the National Institute for Strategic Studies (NISS) in 2011, the analytical report prepared by NISS[1], as well as conclusions and recommendations of the July 2012 round table on this subject and the international scientific and practical conference Critical Infrastructure Protection Concept: State, Problems and Prospects of Implementation in Ukraine (November 2013) organized by NISS jointly with the NATO Liaison Office in Ukraine and PJSC Ukrhydroenergo.

We have taken into account numerous inputs from Ukrainian and international experts. We express gratitude for active participation in the work on individual Green Paper sections to Ukrainian experts: V. Bilokon, V. Grechaninov, O. Ievdin, V. Zaslavsky, V. Luchkov, M. Sungurovsky, O. Fal and to international experts: Valeri Ratchev and Todor Tagarev (Geneva Centre for the Democratic Control of Armed Forces), Krzysztof Brzozowski (Governmental Center for Security, Poland), Martin Linhart (NATO Liaison Office in Ukraine), Christian Papsthart (Federal Ministry of Interior, Germany), Monika John-Koch (Federal Office of Civil Protection and Disaster Assistance, Germany), Heiki Jakson (NATO Energy Security Centre of Excellence).

Discussion of Green Paper text with experts and consideration of suggestions received from concerned government agencies, companies, and research institutions allowed NISS to present this final version of the Green Paper for Critical Infrastructure Protection in Ukraine at the international expert meeting on 15-16 October 2015.

[1]*D. Biriukov*, S. Kondratov. Critical Infrastructure Protection: Problems and Prospects of Implementation in Ukraine. -K.: NISS, 2012. - 57 pages

ЗЕЛЕНА КНИГА З ПИТАНЬ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ[7]

Бірюков Дмитро Сергійович,
Кондратов Сергій Іванович,
Насвіт Олег Іліодорович,
Суходоля Олександр Михайлович

[7]Зелену книгу розроблено відповідно до пункту Річної національної програми співробітництва Україна – НАТО в 2015 р. Підготовлено НІСД із залученням українських і зарубіжних експертів та за підтримки Офісу зв'язку НАТО в Україні.

1. Вступ

Нині Українська держава протистоїть найзначнішому безпековому виклику за роки своєї незалежності. Глибока соціально-політична криза в умовах іноземного воєнного втручання у внутрішні справи України, різке посилення екстремізму й тероризму, небувале зростання злочинності, у т.ч. із використанням зброї, зниження рівня економіки та зростання масштабів гуманітарної кризи в східних регіонах країни, руйнування та пошкодження численних підприємств, інфраструктурних об'єктів – усе це визначає новітні реалії, в яких сьогодні існує Україна та в яких має забезпечуватися безпека її громадян, суспільства й державних інституцій.

Цілком очевидно, що сектор безпеки України потребує докорінного реформування, яке має відбуватися з огляду на світовий досвід і проголошений курс на євроатлантичну інтеграцію. Зазначені чинники в теперішніх умовах роблять особливо актуальним запровадження в нашій державі концептуального поняття «захист критичної інфраструктури», активно використовуваного у провідних країнах Заходу, країнах – членах ЄС і НАТО як один із сучасних інструментів реалізації безпекової політики.

Терміном «критична інфраструктура» зазвичай охоплюються об'єкти, системи, мережі або їх частини, порушення функціонування або руйнування яких призведе до найтяжчих 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 у суспільстві, захистом базових потреб його членів і формуванням у них відчуття безпеки й захищеності.

В Україні, як і в інших країнах, наявні такі системи, об'єкти й ресурси, знищення або пошкодження яких матиме істотний негативний вплив на громадян, суспільство й державні інституції. При цьому було б неправильно стверджувати, що в нашій країні не приділяється увага їх захисту й безпеці. Навпаки, на сьогодні чинними є низка законодавчих і нормативних актів, що визначають повноваження та компетенцію державних органів у цій і суміжних сферах, встановлюють особливості забезпечення охорони та безпечного функціонуван-

ня зазначених об'єктів і систем. Проте в Україні на національному рівні й досі відсутній системний підхід до управління захистом і безпекою всього комплексу таких систем, об'єктів і ресурсів з огляду на взаємопов'язаність об'єктів, які зазвичай належать до критичної інфраструктури. Крім того, досі не розроблено механізм попередження можливих кризових ситуацій, пов'язаних із функціонуванням критичної інфраструктури.

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

Зелену книгу розроблено з метою сприяння експертному обговоренню на національному рівні основних проблем щодо створення системи захисту критичної інфраструктури в Україні та способів їх вирішення, що буде вагомим внеском у процес системного реформування усього сектору безпеки держави, наблизить його структуру та функції до вже наявних у країнах – членах ЄС і НАТО.

2. Що таке критична інфраструктура

Для стабільного й безпечного існування сучасне суспільство та його члени мають гарантовано отримувати найрізноманітніші продукти й послуги, мати доступ до низки важливих ресурсів тощо. Для цього створюються й використовуються певні об'єкти, мережі та системи, фізичні або віртуальні.

Останніми десятиліттями бурхливий розвиток технологій, особливо в ІТ-сфері, спричинив значні, а іноді й революційні, зміни у збільшенні ступеня взаємозв'язку, взаємопроникнення та взаємозалежності різноманітних мереж і систем, виробничих, фінансових, торговельних та інших процесів у всіх сферах життя більшості країн світу. Це суттєво підвищує вразливість таких систем та об'єктів, значно ускладнює забезпечення їх надійного захисту й безпеки.

Водночас згадані процеси відбувалися на тлі різкого зростання загрози тероризму, насамперед міжнародного, зростання кількості техногенних катастроф, у т.ч. викликаних людським чинником, збільшення кількості природних катастроф, спричинених, зокрема, глобальними кліматичними змінами. Усі ці чинники обумовили те, що провідні країни світу стали приділяти значну увагу захисту найбільш важливих для безпеки своїх громадян, суспільства й держави об'єктів, систем і ресурсів.

2.1. Визначення терміна «критична інфраструктура»

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

Необхідно зазначити, що, незважаючи на подібність визначень цього терміна в законодавстві провідних країн та міжнародних організацій, є й певні відмінності, які, очевидно, відображають національну або організаційну (у випадках ЄС і НАТО) специфіку сфери застосування терміна, особливості нормативно-правових систем.

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

У Німеччині до критичної інфраструктури належать «*організаційні та фізичні структури і об'єкти настільки життєво важливі для суспільства та економіки країни, що їх вихід з ладу або погіршення функціонування будуть мати своїм результатом стійкі зриви постачання, значний підрив державної безпеки або інші драматичні наслідки*»[8].

Велика Британія визначила елементами критичної інфраструктури «*ті установки, системи, об'єкти й мережі, необхідні для функціонування країни та надання важливих послуг, від яких залежить повсякденне життя Великої Британії*»[9]. У Нідерландах об'єктами критичної інфраструктури, зокрема, є «*продукція, послуги та пов'язані з ними процеси*». Існують й інші приклади деяких відмінностей у визначенні цього терміна в національних законодавствах.

На наш погляд, важливим є те, що в деяких національних законодавствах у визначенні терміна «критична інфраструктура» акцент дещо зміщено з фізичного виміру, тобто особливо важливих систем мереж і об'єктів, на функції та послуги, якими вони забезпечують сус-

[8]*National* Strategy for Critical Infrastructure Protection [Електронний ресурс]. – Federal Ministry of Interior, Germany, 2009. – Режим доступу: http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf

[9]*Strategic* Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards [Електронний ресурс]. – UK Cabinet Office, March 2010. – Режим доступу: https://www.gov.uk/

пільство, бізнес і державу. Саме такі функції та послуги надають методологічні можливості для встановлення критеріїв відбору елементів критичної інфраструктури та пріоритетності їх захисту[10].

Зрозуміло, що визначення в українському законодавстві цього основного для даної проблематики терміна має залишатися в межах загальновизнаних у світі підходів і повною мірою відображати специфіку безпекових умов, у яких перебуває країна.

В Україні термін «критична інфраструктура» неодноразово використовувався в нормативно-правових документах, проте його визначення й досі відсутнє в чинному законодавстві. Уперше в офіційних документах цей термін з'явився у 2006 р. в тексті Рекомендацій парламентських слухань з питання розвитку інформаційного суспільства, на жаль, без подальшого розвитку. В Стратегії національної безпеки «Україна у світі, що змінюється» (2012 р.) цей термін згадувався при визначенні способів зміцнення енергетичної безпеки та напрямів забезпечення інформаційної безпеки.

У новій Стратегії національної безпеки України (2015 р.) термін «критична інфраструктура» використовується більш деталізовано. Уперше 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 уперше одними з «основних напрямів державної політики в сфері національної безпеки» названо забезпечення безпеки критичної інфраструктури та визначено пріоритети такого напряму.

Відсутність визначення терміна «критична інфраструктура» в українському законодавстві і, як наслідок, переліку об'єктів, які необхідно віднести до цієї інфраструктури, неодноразово перешкоджали ефективному виконанню першочергових безпекових завдань, таких як п. 6 Рішення Ради національної безпеки і оборони України «Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України» від 01 березня 2014 р. (введено в дію Указом Президента України №189/2014 від 02 березня 2014 р.), на виконання

[10]Наприклад, енергетичний сектор у всіх країнах і в таких міжнародних об'єднаннях, як ЄС і НАТО, відносять до критичної інфраструктури. Основна його функція полягає в забезпеченні потреб населення, суспільства й держави в енергії. Якщо акцент робитиметься на енергетичних об'єктах і системах, то без належного аналізу до критичної важливої інфраструктури можуть потрапити переважно об'єкти електрогенерації, тоді як об'єкти системи електропостачання є більш важливими для забезпечення послуг з електропостачання кінцевих споживачів. Як свідчить світовий досвід, найтяжчі наслідки для забезпечення електроенергією суспільства виникають унаслідок аварій у системах передачі та розподілення електроенергії, а не у випадку виходу з ладу одного чи кількох об'єктів генерації.

якого Міністерству внутрішніх справ України наказується забезпечити «посилену охорону об'єктів енергетики та критичної інфраструктури».

З огляду на викладене й досвід провідних країн світу з розроблення підходів до забезпечення національної безпеки на основі застосування концепції «критична інфраструктура», пропонуємо використовувати в Україні таке визначення цього терміна:

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

Хоча в наведеному визначенні не наголошено на взаємозв'язку або взаємовпливі між окремими елементами критичної інфраструктури, саме ця особливість впливає на масштаб наслідків. Відповідно управління безпекою окремих об'єктів має здійснюватися з огляду на загальносистемні функції всієї критичної інфраструктури.

Потрібно надати також тлумачення поняття «захист критичної інфраструктури»:

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

Під *стійкістю критичної інфраструктури* розумітимемо її спроможність надійно функціонувати в нормальному режимі, адаптуватися до умов, що постійно змінюються, протистояти й швидко відновлюватися після аварій і технічних збоїв, зловмисних дій, природних лих та небезпечних природних явищ[11]. Також варто зазначити, що поняття «безпека», використане у визначенні «захист критичної інфраструктури», містить і фізичну (фізичний захист), експлуатаційну та операційну безпеку.

2.2. Сектори, об'єкти, системи й ресурси, які можуть бути віднесені до критичної інфраструктури

Переліки секторів, які в різних країнах належать до критичної інфраструктури, також переважно є подібними, адже розвиток сучасного суспільства відбувається за єдиними законами. Наявні відмінності, обумовлені насамперед національною специфікою, традиціями та особливостями безпекової політики тієї чи іншої країни або міжнародної структури.

Аналізуючи досвід Сполучених Штатів Америки в цій сфері, зазначимо, що перелік секторів, включених до національної критичної

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

інфраструктури цієї країни, є, очевидно, найбільш повним і містить 16 пунктів:

- хімічний сектор (*Chemical*);
- комерційні об'єкти (*Commercial facilities*);
- зв'язок (*Communications*);
- критичне виробництво (*Critical manufacturing*);
- дамби й інші гідротехнічні споруди (*Dams*);
- оборонно-промислова база (*Defense industrial base*);
- служби екстреної допомоги населенню, реагування на надзвичайні ситуації (*Emergency services*);
- енергетичний сектор (*Energy*);
- банки та фінанси (*Banking and finance*);
- продукти харчування та сільське господарство (*Food and agriculture*);
- урядові об'єкти (*Government facilities*);
- охорона здоров'я та медицина (*Healthcare and public health*);
- інформаційні технології (*Information technology*);
- ядерні реактори, матеріали та відходи (*Nuclear reactors, materials and waste*);
- транспортні системи (*Transportation systems*);
- водні ресурси, системи водопостачання та стічних вод (*Water and wastewater systems*).

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

Зрозуміло, що для України, яка перебуває в жорстких безпекових і фінансово-економічних умовах, при формуванні переліку секторів критичної інфраструктури необхідно спиратися насамперед на наявні ресурси та потреби підтримання й захисту базових функцій, без чого неможливе безпечне існування населення, суспільства та функціону-

вання економіки й держави, належний захист національних інтересів. З огляду на такі міркування був запропонований орієнтовний перелік секторів критичної інфраструктури України (наведено в Дод. А).

Наступним після визначення секторів критичної інфраструктури кроком має стати складання переліку конкретних об'єктів, систем і ресурсів (елементів) критичної інфраструктури. Він може містити від кількох десятків пунктів для невеликих країн до багатьох тисяч (наприклад, для США). З огляду на те, що кожна країна може виділити на захист національної інфраструктури лише обмежені ресурси, національне законодавство має встановити критерії віднесення тих чи інших об'єктів і систем до критичної інфраструктури, спираючись на затверджені методи оцінки загроз та ризиків її сталому функціонуванню. Такі переліки використовуються під час планування відповідних заходів і в процесі прийняття рішень. Вони зазвичай підлягають перегляду – періодичному або за значних змін у безпековому середовищі та в разі внесення істотних змін у національне законодавство тощо.

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

Аналіз наявних підходів до визначення переліку елементів критичної інфраструктури (віднесення об'єктів до критичної інфраструктури) свідчить, що можуть братися до уваги, зокрема, такі характеристики:

- масштаб (географічне охоплення території, для якої втрата елементу критичної інфраструктури завдає значної шкоди);
- взаємозв'язок між елементами критичної інфраструктури;
- тривалість впливу (як саме й коли виявлятимуться шкода, пов'язана із втратою чи відмовою, виходом з ладу або порушенням функціонування об'єктів критичної інфраструктури);
- вразливість об'єкта до впливу небезпечних чинників;
- тяжкість можливих наслідків за показниками в таких групах:
  - економічна безпека (вплив на ВВП, розмір економічних втрат – і прямих, і непрямих, частки продукції на ринку, чисельності зайнятих співробітників, податкових надходжень у бюджет);
  - безпека життєдіяльності й здоров'я населення (кількість постраждалих, загиблих, осіб, які отримали серйозні травми, а також чисельність евакуйованого населення, забезпечення роботи аварійно-рятувальних служб, екстреної допомоги населенню);
  - внутрішньополітична, державна безпека (втрата впевненості в дієспроможності влади, авторитету держави, порушення управління державою);

– обороноздатність (зниження боєздатності збройних сил, розголошення таємної інформації);

– екологічна безпека (вплив на навколишнє природне середовище).

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

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

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

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

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

• підприємства, які мають стратегічне значення для економіки та безпеки держави[12];

• особливо важливі об'єкти електроенергетики[13];

• особливо важливі об'єкти нафтогазової галузі[14];

• важливі державні об'єкти, зокрема пункти управління органів державної влади та органів місцевого самоврядування[15];

• об'єкти можливих терористичних посягань[16];

---

[12]*Про затвердження* переліку підприємств, які мають стратегічне значення для економіки та безпеки держави : постанова Кабінету Міністрів України від 23.12.2004 р. № 1734 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/

[13]*Про затвердження* переліку особливо важливих об'єктів електроенергетики, які підлягають охороні відомчою воєнізованою охороною у взаємодії із спеціалізованими підрозділами інших центральних органів виконавчої влади : постанова Кабінету Міністрів України від 28.07.2003 р. № 1170 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/

[14]*Про затвердження* переліку особливо важливих об'єктів нафтогазової галузі : розпорядження Кабінету Міністрів України від 27.05.2009 р. № 578-р [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/

[15]*Постанова* Кабінету Міністрів України від 15.08.2007 р. № 1051 (для службового користування) [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/ru/1051-2007-%D0%BF

[16]*Положення* про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків (затверджене Постановою Кабінету Міністрів України від 15.08.2007 р. № 1051) [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/

• об'єкти, які підлягають охороні та обороні в умовах надзвичайних ситуацій і в особливий період[17];

• об'єкти, що підлягають обов'язковій охороні підрозділами Державної служби охорони за договорами[18];

• органи державної влади, що підлягають безоплатній охороні Національною гвардією України[19];

• об'єкти підвищеної небезпеки[20] (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[21]);

• об'єкти, включені до Державного реєстру потенційно небезпечних об'єктів[22];

• радіаційно небезпечні об'єкти, для яких розробляється об'єктова проектна загроза[23];

• об'єкти, віднесені до категорій із цивільного захисту[24];

• об'єкти, що належать суб'єктам господарювання, проектування яких здійснюється з урахуванням вимог інженерно-технічних заходів цивільного захисту[25];

---

[17]*Щодо затвердження* Переліку об'єктів, які підлягають охороні і обороні в умовах надзвичайних ситуацій і в особливий період : постанова Кабінету Міністрів України від 24.04.1999 р. № 675-019 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/

[18]*Про заходи* щодо вдосконалення охорони об'єктів державної та інших форм власності (із змінами) : постанова Кабінету Міністрів України від 10.08.1993 р. № 615 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/

[19]*Про затвердження* переліку органів державної влади, що підлягають безоплатній охороні Національною гвардією: постанова Кабінету Міністрів України від 25.11.2015 р. №971 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/

[20]*Про об'єкти* підвищеної небезпеки : закон України від 18.01.2001 р. № 2245-III [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/

[21]*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 р. №765) [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/

[22]*Про затвердження* Положення про Державний реєстр потенційно небезпечних об'єктів : постанова Кабінету Міністрів України від 29.08.2002 р. № 1288 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/

[23]*Про затвердження* Переліку радіаційно небезпечних об'єктів в Україні, для яких розробляється об'єктова проектна загроза : наказ Держатомрегулювання від 17.12.2012 р. № 238 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/

[24]Відповідно до порядку, затвердженого Постановою Кабінету Міністрів України від 02.03.2010 р. № 227 (із змінами відповідно до Постанови Кабінету Міністрів України від 24.07.2014 р. № 545.

[25]*Про затвердження* переліку об'єктів, що належать суб'єктам господарювання, проектування яких здійснюється з урахуванням вимог інженерно-технічних заходів цивільного захисту : постанова Кабінету Міністрів України від 09.01.2014 р. № 6 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/

• чергово-диспетчерська система екстреної допомоги населенню за єдиним безкоштовним телефонним номером виклику екстрених служб 112[26];

• аварійно-рятувальні служби;

• Національна система конфіденційного зв'язку[27];

• Державна система урядового зв'язку України[28];

• платіжні системи[29];

• нерухомі об'єкти культурної спадщини[30].

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

3. Основні загрози критичній інфраструктурі

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

Зазвичай у національних законодавствах провідних країн світу загрози критичній інфраструктурі розподіляють на три основні категорії, з огляду на характер їх походження. Проте й тут є деякі відмінності. Наприклад, у США та Канаді до спектра загроз критичній інфраструктурі належать *зловмисні дії* (груп або окремих осіб, таких як терористи і злочинці), *природні небезпеки* (урагани, торнадо, землетруси, цунамі, повені, надзвичайні погодні умови тощо) і *техногенні надзвичайні ситуації* (авіаційні катастрофи, ядерні аварії, пожежі, аварії в системах енергозабезпечення, викиди небезпечних речовин тощо). У Німеччині категорії загроз мають такий вигляд: *небезпечні природні явища* (надзвичайні погодні умови, лісові та степові пожежі, сейсмічні явища, епідемії та пандемії, космічні явища); *технічні аварії/людські помилки* (відмови систем, аварії та надзвичайні події, недбалість, організаційні

---

[26]*Про систему* екстреної допомоги населенню за єдиним телефонним номером 112 : закон України від 13.03.2012 р. № 4499-VI [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/

[27]*Про Національну* систему конфіденційного зв'язку: закон України від 10.01.2002 р. № 2919-III (із змінами) [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/

[28]*Положення* про Державну система урядового зв'язку України: ухвалено указом Президента України від 18.04.2005р. № 663

[29]*Про платіжні* системи та переказ коштів в Україні : закон України від 05.04.2001 р. № 2346-III [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/

[30]*Про охорону* культурної спадщини : закон України від 08.06.2000 р. № 1805-III [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/

помилки тощо); *тероризм, злочинність, війна* (тероризм, диверсії, злочинність, громадянські війни, війни).

Загрози кожної з названих категорій у разі їх реалізації можуть призводити до негативних наслідків, які, своєю чергою, стають ініціюючими подіями для реалізації загроз інших категорій і на інших елементах критичної інфраструктури. У такому разі говорять про т.зв. ефект доміно та/або каскадний ефект.

Стосовно спектра загроз критичній інфраструктурі в Україні, то його специфіка обумовлюється, насамперед, особливістю тієї безпекової ситуації, в якій перебуває наша держава. Бойові дії в межах антитерористичної операції (*далі* – АТО) на території Донбасу, яка й до нинішньої кризи характеризувалася високою зношеністю основних фондів, значними проблемами із забезпеченням екологічної й техногенної безпеки, різко збільшують загрози виникнення аварій на об'єктах підвищеної небезпеки, шахтах, об'єктах електроенергетики, хімічних і металургійних підприємствах та мережах життєзабезпечення (і внаслідок їх випадкового пошкодження або втрати контролю над технологічними процесами, і в результаті терористичних актів і диверсій).

При цьому необхідно підкреслити, що Зелена книга з питань захисту критичної інфраструктури в Україні не розглядає захист критичної інфраструктури в умовах правового режиму воєнного стану (це має бути предметом аналізу інших документів).

Без сумніву, розвиток ситуації на сході України буде значною мірою впливати на загрози національній критичній інфраструктурі. Зокрема, ймовірно, що, нинішня криза може спричинити збереження упродовж досить тривалого часу високого рівня терористичних, диверсійних і кримінальних загроз для критичної інфраструктури.

У чинному нормативно-правовому полі України, що регулює правовідносини в питаннях, близьких до питань захисту критичної інфраструктури, класифікуються не загрози, а надзвичайні ситуації, зокрема за їх походженням. Статтею 5 Кодексу цивільного захисту України визначається, що залежно від характеру походження подій, що можуть зумовити виникнення надзвичайних ситуацій на території України, визначаються такі види надзвичайних ситуацій: техногенного характеру; природного характеру; соціальні; воєнні. На наш погляд, така класифікація не може бути перенесена на загрози критичній інфраструктурі без змін, оскільки має певні методологічні обмеження і не дає змоги реалізувати всі переваги, створювані запровадженням концепції захисту критичної інфраструктури.

Доцільно виділити такі категорії загроз, на які має бути налаштовано захист критичної інфраструктури:

• *аварії й технічні збої*, зокрема авіаційні катастрофи, ядерні аварії, пожежі, аварії в системах енергозабезпечення, викиди небезпечних ре-

човин, відмови систем, аварії та надзвичайні події, зумовлені недбалістю, організаційними помилками тощо;

• *небезпечні природні явища*, зокрема надзвичайні погодні умови, лісові, степові й торф'яні пожежі, сейсмічні явища, епідемії та пандемії, космічні явища, урагани, торнадо, землетруси, цунамі, повені тощо;

• *зловмисні дії*, зокрема зловмисні дії груп або окремих осіб, таких як терористи, злочинці й диверсанти, а також бойові дії в умовах війни.

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

Аварії й технічні збої

Розглядаючи *аварії й технічні збої*, варто зауважити, що в Україні через високий рівень зношеності основних фондів існує загроза виникнення аварій на об'єктах підвищеної небезпеки, об'єктах електроенергетики й мережах життєзабезпечення. Значний ризик техногенних аварій пов'язаний із наявністю на території України значної кількості об'єктів, що належать до категорії потенційно небезпечних (понад 24 тис.), причому понад чверть із них ідентифіковано як об'єкти підвищеної небезпеки[31]. За даними ДСНС[32], аварії на 955 об'єктах, внесених до Державного реєстру об'єктів підвищеної небезпеки, можуть призвести до виникнення надзвичайних ситуацій державного або регіонального рівня, що також може загрожувати критичній інфраструктурі, зокрема функціонуванню об'єктів паливно-енергетичного комплексу, мостів і доріг, комунальної інфраструктури тощо.

Природні лиха та небезпечні природні явища

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

• метеорологічні або надзвичайні погодні умови (снігопади, ожеледь, хуртовини, зливи, градобій, заморозки, посухи, спека, урагани, шквали, смерчі);

• гідрологічні (повені, селі, паводки, підтоплення, цунамі);

• сейсмічні (землетруси);

• геологічні (небезпечні екзогенні геологічні процеси – зсуви, просідання та карст);

• геліофізичні (геомагнітні сонячні бурі);

• лісові, степові й торф'яні пожежі;

---

[31]*Національна* доповідь про стан техногенної та природної безпеки в Україні у 2014 р. (С. 212). [Електронний ресурс]. – Режим доступу: http://www.mns.gov.ua/files/prognoz/report/2014/ND_2014.pdf

[32]*Національна* доповідь про стан техногенної та природної безпеки в Україні у 2013 р. [Електронний ресурс]. – Режим доступу: http://www.mns.gov.ua/content/annual_report_2013.html

• епідемії та пандемії, епізоотії, епіфітотії.

Поміж зазначених видів загроз варто виділити метеорологічні, частота яких в Україні значно збільшилася останніми десятиліттями, зокрема таких як обледеніння, підтоплення, посухи тощо.

Найнебезпечнішими гідрологічними загрозами за наслідками для критичної інфраструктури є 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 перебувають під впливом регіонального підтоплення земель, близько 40 % – у зонах карстових загроз, до 11 % – на територіях можливої активізації зсувних процесів. До 59 % магістральних газопроводів знаходяться в зонах можливого прояву карсту, до 21 % – регіонального підтоплення земель. Активізація небезпечних екзогенних геологічних процесів погіршує інженерно-геологічні умови експлуатації промислових споруд та інженерних мереж промислово-міських агломерацій.

Зловмисні дії

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

Безумовно, найсерйознішою може бути потенційна загроза використання з терористичною метою об'єктів ядерної енергетики. При цьому потрібно зауважити, що на сьогодні на українських АЕС забезпечується рівень фізичного захисту, адекватний поточним загрозам.

Відзначається значне зростання інтенсивності кібератак, здійснюваних 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.

Окремої уваги потребує проблема забезпечення безпеки функціонування державних органів влади, збройних сил, правоохоронних органів і спецслужб (будівель, належної інфраструктури тощо) у кризових ситуаціях. Відповідні інфраструктурні об'єкти в розвинених країнах світу зазвичай також належать до критичної інфраструктури.

Загрози критичній інфраструктурі можна розглядати з огляду не лише на характер їх походження, а й на елементи критичної інфраструктури, на які ці загрози спрямовані:

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

• *системи управління та комунікації*, зокрема автоматизованих систем управління та систем зв'язку;

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

Виділення спрямованості дії загроз методологічно уможливлює більш системний підхід до формування державної політики й організації системи захисту критичної інфраструктури. У планах захисту критичної інфраструктури, розроблених операторами, погоджених і схвалених відповідними державними органами, має бути докладно описано заходи протидії загрозам за такими напрямами захисту:

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

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

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

• інформаційні технології – захист інформації, систем зв'язку та управління;

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

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

4. Державна політика захисту критичної інфраструктури

4.1. Мета захисту критичної інфраструктури в Україні

Одним із пріоритетних напрямів безпекової політики України має стати підвищення безпеки та стійкості національної критичної інфраструктури щодо всього спектра загроз і ризиків, оскільки саме критична інфраструктура забезпечує життєво важливі для населення, суспільства й держави послуги та функції, без яких неможливі їх безпечне існування й добробут, а також належний рівень національної безпеки.

Мета захисту критичної інфраструктури в Україні випливає з визначення критичної інфраструктури та полягає в забезпеченні постачання населенню, суспільству, бізнесу й державі життєво важливих товарів і послуг. Для виконання зазначеної функції критичної інфраструктури необхідно гарантувати безперебійне стале функціонування об'єктів критичної інфраструктури у визначених режимах; мати спроможність запобігати руйнуванню чи завданню невиправної шкоди, припиненню функціонування або втраті контролю над об'єктами критичної інфраструктури внаслідок дії всіх чинників; забезпечувати швидке відновлення функціонування цих об'єктів у випадку переривання їх роботи.

4.2. Стратегічні цілі державної політики захисту критичної інфраструктури

Критична інфраструктура сучасної держави є надскладним комплексом різноманітних за своїм характером елементів, який включає: низку організаційних структур, різні управлінські моделі, залежні і взаємозалежні функції і системи і у фізичному, і у віртуальному просторах. В управлінні критичної інфраструктури беруть участь державні структури на всіх рівнях (з різними сферами відповідальності й повноваженнями), а також власники та оператори об'єктів і систем, що належать до критичної інфраструктури. В умовах глобалізації національна безпека, виробництво, економіка та фінанси кожної країни значною мірою залежать від чинників, що визначають стан безпеки в інших країнах та в глобальному вимірі.

Нині відбувається розвиток нової філософії забезпечення безпеки, в основу якої покладено спільні зусилля громадянина, суспільства, бізнесу й держави. Також формується «культура управління ризиками», яка має стати основою політики у сфері захисту критичної інфраструктури і складатися з таких елементів:

• відкритий обмін інформацією між державними органами, приватним сектором, населенням та окремими громадянами стосовно ризиків з огляду на необхідність захисту певної (чутливої) інформації;

• співробітництво між усіма суб'єктами процесу захисту критичної інфраструктури в запобіганні інцидентам та в реагуванні на них;

• підвищення рівня власних можливостей громадян (самозахисту, взаємодопомоги тощо) та організацій, уразливих до припинення або погіршення послуг, забезпечуваних критичною інфраструктурою[33];

• активне міжнародне співробітництво щодо захисту критичної інфраструктури з огляду на процеси глобалізації та зростання залеж-

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

ності безпекових, економічних, виробничих, фінансових та інших процесів у багатьох країнах від постачання послуг і ресурсів, здійснюваних міжнародними мережами, системами, компаніями тощо.

Викладене обумовлює першу стратегічну ціль політики щодо захисту критичної інфраструктури: *розбудова безпекового партнерства для підвищення безпеки та забезпечення стійкості національної критичної інфраструктури.*

У більшості країн світу і, з огляду на економічні реформи, в Україні очевидним є те, що об'єкти критичної інфраструктури перебуватимуть переважно у приватній власності. Саме приватним операторам належить і більшість об'єктів критичної інфраструктури, і лідерство в розробленні новітніх технологій виробництва й технологій їх захисту.

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

Тому ефективне державно-приватне партнерство (*далі* – ДПП) є головним елементом дієвої сталої політики, спрямованої на підтримання належного рівня безпеки та стійкості критичної інфраструктури. У США та Німеччині необхідною умовою для розбудови такого партнерства визнають формування довіри[34] між партнерами та стимулів для співпраці. Політика країн має стимулювати і приватних власників, і органи державного управління до створення на всіх рівнях такої системи захисту інфраструктури життєзабезпечення суспільства, яка була б спроможною переборювати надзвичайні ситуації, знижувати ризики й наслідки виникнення таких ситуацій. Обов'язковим елементом такого партнерства є створення стимулів для інвестування в безпеку критичної інфраструктури, а також умов для збереження конкурентоспроможності бізнесу, який інвестує в безпеку критичної інфраструктури.

Таким чином, механізм ДПП створює фундамент для стимулювання інвестицій у захист критичної інфраструктури у спосіб адекватного інформування бізнесу про загрози й ризики для елементів критичної інфраструктури. Водночас враховується, що витрати бізнесу на від-

[34] *Partnering* for Critical Infrastructure Security and Resilience / U.S. Department of Homeland Security, National Infrastructure Protection Plan, NIPP 2013 [Електронний ресурс]. – Режим доступу: www.dhs.gov/national-infrastructure-protection-plan

повідні заходи мають бути збалансованими й такими, що не підривають його конкурентоспроможності і спроможності надавати критично важливі для населення, суспільства й держави послуги.

Стосовно України, то до 2014 р. ДПП здійснювалося переважно у сфері економіки в межах Закону України «Про державно-приватне партнерство» від 01 липня 2010 р. № 2404-VI, норми якого не охоплюють діяльність у сфері захисту критичної інфраструктури. Водночас події 2014–2015 рр. виявили важливість залучення громадськості до захисту національних інтересів України і, зокрема, до захисту критичної інфраструктури.

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

Потрібно зауважити, що вжиття заходів з підвищення надійності, живучості та стійкості об'єктів/систем вимагатимуть від операторів додаткових фінансових витрат, що може призвести до підвищення собівартості послуг/товарів, які надають відповідні об'єкти/системи. Як наслідок, при ринковому ціноутворенні підвищаться ціни на відповідні послуги/товари. Цей соціально-економічний аспект захисту критичної інфраструктури необхідно врахувати і під час визначення об'єктів критичної інфраструктури, і під час встановлення вимог до їх захисту. Причому ініціювання з боку держави вимог щодо підсилення захисту критичної інфраструктури має бути усвідомленим кроком з огляду на зазначений соціально-економічний зміст. До того ж для деяких секторів критичної інфраструктури держава (в особі відповідних регулюючих органів), можливо, повинна буде переглянути тарифи на послуги/товари (наприклад, на електроенергію).

Одним з найважливіших інструментів формування довіри між державними та приватними партнерами і в США, і в інших розвинених країнах світу вважають обмін відповідною інформацією.

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

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

Достатньо повними даними та інформацією щодо ризиків і загроз і всій критичній інфраструктурі, і окремим її елементам можуть володіти лише уповноважені державою органи, які, однак, потребують детальної інформації та співпраці з боку приватного сектору. Тому важливим аспектом є створення адекватної нормативно-правової бази щодо обміну інформацією про безпеку функціонування критичної інфраструктури чи захищені системи. При досягненні цієї цілі між партнерами відповідно до встановлених процедур здійснюється ефективний обмін інформацією (зокрема розвідувальною) щодо різних аспектів захисту критичної інфраструктури (у т.ч. про найефективнішу практику), забезпечується захист чутливої інформації (зокрема комерційної), яка може бути використана у зловмисних цілях.

Українська держава має забезпечувати належне врегулювання обміну інформацією, зокрема у спосіб формування загальних стандартів обміну, регламентації діяльності відповідальних з боку операторів за забезпечення цього обміну, методології оброблення й аналізу інформації, інформування операторів інфраструктури щодо потенційних і реальних загроз, встановлення вимог та обмежень щодо використання чутливої інформації для недопущення зловживань.

У більшості розвинених країн світу стратегічною ціллю також є побудова системи захисту критичної інфраструктури та підвищення її стійкості на основі *підходу до управління ризиками, пов'язаними з усіма видами загроз* (англ., *all-hazard approach*).

З огляду на зарубіжний досвід першим кроком на шляху до цієї цілі є заснована на всебічному аналізі ідентифікація всіх загроз і ризиків для критичної інфраструктури України. У процесі управління ризиками для їх зниження доцільно вживати таких заходів[35]:

• підвищення стійкості критичної інфраструктури до ідентифікованих загроз і небезпек;

---

[35]*National* Infrastructure Protection Plan / U.S. Department of Homeland Security. – 2006 [Електронний ресурс]. – Режим доступу: http://www.naruc.org/publications/nipp_plan4.pdf

• запобігання загрозам, пов'язаним із зловмисними діями (тероризм, злочинність тощо);

• планування своєчасного реагування на збої у функціонуванні критичної інфраструктури з метою зменшення їх негативного впливу на здоров'я та безпеку населення, економіку й базові функції держави;

• планування швидкого ремонту й відновлення функціонування критичної інфраструктури для випадку надзвичайних ситуацій, яким не можна запобігти.

Незважаючи на критичну важливість заходів із підвищення рівня захищеності й стійкості критичної інфраструктури, їх планування в будь-якій країні здійснюється в межах бюджетних і ресурсних обмежень. У зв'язку із цим ще однією стратегічною ціллю політики в цій сфері має бути *максимально ефективне використання ресурсів для захисту критичної інфраструктури*. Розбудоване партнерство і на національному, і на міжнародному рівнях, координація дій та обмін інформацією між партнерами створюють передумови для досягнення такої цілі, в результаті чого виключаються дублювання функцій, а також розпорошення ресурсів поміж окремих суб'єктів процесу забезпечення захисту критичної інфраструктури.

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

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

Очевидно, що стратегічні цілі державної політики України у сфері захисту критичної інфраструктури має бути зафіксовано у вітчизняному законодавстві. Так, доцільно розробити окремий закон України, пропозиції щодо структурних елементів якого наведено в Додатку Б.

4.3. Основні принципи формування захисту критичної інфраструктури в Україні

Пріоритети політики захисту критичної інфраструктури в Україні сформульовані з огляду на значущість захисту критичної інфраструктури для забезпечення національної безпеки сучасної держави. Принципи, на яких має будуватися такий захист, мають стратегічний безпековий контекст.

На наш погляд, до основних принципів формування (побудови) захисту критичної інфраструктури в Україні належать такі.

Принцип координованості, що означає:

• планування безпеки на національному рівні, узгодження розвитку нормативно-правових, організаційних і науково-технологічних інструментів, призначених для виконання завдань захисту критичної інфраструктури;

• урахування необхідності забезпечення захищеності критичної інфраструктури під час планування, визначення пріоритетів та оцінювання соціально-економічного розвитку країни;

• створення механізмів впливу на стан захищеності критичної інфраструктури;

• функціонування єдиного центру оцінювання стану захищеності критичної інфраструктури, прогнозування загроз та оцінювання ризиків для об'єктів критичної інфраструктури, координації дій усіх зацікавлених сторін із захисту критичної інфраструктури;

• створення механізмів координації зусиль усіх зацікавлених сторін – влади, бізнесу й суспільства – щодо захисту критичної інфраструктури, зокрема горизонтальної координації операторів взаємозалежних та однотипних об'єктів критичної інфраструктури;

• управління всіма наявними в державі ресурсами з метою їх раціонального використання;

• запровадження підходу до формування національної проектної загрози, розробленої в ядерній галузі, для критичної інфраструктури та окремих її елементів із урахуванням оцінки загроз національній безпеці;

• планування розвитку кадрового забезпечення з огляду на наявні можливості спеціалізованих навчальних закладів.

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

• використання єдиної понятійної та методологічної бази для аналізу загроз критичній інфраструктурі;

• розроблення методології ідентифікації об'єктів критичної інфраструктури (визначення переліку) на основі оцінки важливості надання ними товарів і послуг (оцінки критичності);

• урахування та оцінювання всього комплексу загроз об'єктам критичної інфраструктури, використання ризик-орієнтованих методів аналізу та прогнозування ризиків і загроз;

• періодичне оцінювання загроз, ризиків та вразливості об'єктів критичної інфраструктури з використанням відповідного досвіду;

• встановлення особливостей функціонування та захисту критичної інфраструктури в мирний час (в умовах повсякденного функціонування, надзвичайної ситуації й режиму надзвичайного стану) та в особливий період (беручи до уваги особливості періоду мобілізації, режиму воєнного стану та відбудовного періоду);

• надання однакової уваги заходам із попередження загроз надзвичайних ситуацій, підвищення готовності до реагування та ліквідації наслідків таких ситуацій;

• поєднання заходів фізичного захисту із заходами забезпечення надійності, живучості й здатності до швидкого відновлення;

• забезпечення багато ешелонованості й різнотипності бар'єрів захисту;

• поступового впровадження нормативно-правових, організаційних і науково-технологічних інструментів, на основі яких мають удосконалюватися засоби та заходи із забезпечення захисту й безпеки критичної інфраструктури.

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

Реалізація цього принципу має включати:

• обмін інформацією між державними органами, приватним сектором, населенням та окремими громадянами стосовно ризиків з огляду на необхідність захисту певної (чутливої) інформації;

• використання ресурсів і держави, і приватного сектору для досягнення цілей забезпечення захисту критичної інфраструктури;

• декларування безпеки об'єкта власником (оператором);

• паспортизація об'єктів критичної інфраструктури;

• партнерський розподіл і чітке розмежування відповідальності за забезпечення захищеності, безпеки та стійкості критичної інфраструктури між оператором і державою;

• створення стимулів для інвестування в безпеку критичної інфраструктури, створення умов для забезпечення конкурентоспроможності бізнесу, що робить належні інвестиції в безпеку об'єктів/систем критичної інфраструктури;

• залучення громадськості й експертного співтовариства, використання консультаційних (дорадчих) рад при визначенні вимог до захищеності, безпеки та стійкості критичної інфраструктури.

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

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

5. Система захисту критичної інфраструктури в Україні

5.1. Основні завдання системи захисту критичної інфраструктури в Україні

З огляду на цілі та принципи побудови системи захисту критичної інфраструктури, можна сформулювати такі *основні завдання* цієї системи.

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

• створення та підтримку функціонування національного центру з управління в кризових ситуаціях і захисту критичної інфраструктури;

• формування пропозицій щодо вдосконалення нормативно-правової бази у сфері національної безпеки і оборони (зокрема, щодо цивільного захисту, боротьби з тероризмом, протидії кіберзагрозам), пов'язаних із захистом критичної інфраструктури;

• оцінювання загроз критичній інфраструктурі на національному рівні (з урахуванням взаємозв'язків окремих об'єктів і секторів інфраструктури, впливу всіх видів загроз), а також ризиків на рівні окремих регіонів і держави загалом;

• прийняття рішення та оповіщення щодо зміни режиму функціонування системи захисту критичної інфраструктури залежно від рівня загроз, зміни правового стану (мирний час, надзвичайна ситуація, особливий період);

• підготовку національного плану захисту критичної інфраструктури;

• підготовку національної проектної загрози для критичної інфраструктури;

• координацію зусиль усіх зацікавлених сторін (державних органів і місцевої влади, бізнесу й суспільства) щодо захисту критичної інфраструктури, включно з горизонтальною координацією операторів взаємозалежних та однотипних об'єктів;

• взаємодію та обмін інформацією з мережею ситуаційних (інформаційно-аналітичних) центрів у сфері безпеки і оборони;

• підготовку державної цільової програми у сфері захисту критичної інфраструктури;

• формування комплексної науково-дослідної програми з питань захисту критичної інфраструктури;

• здійснення взаємодії (точка контакту) зі структурами ЄС і державними органами країн – членів ЄС.

2. Попередження кризових ситуацій, забезпечення готовності до дій у кризових ситуаціях, управління в умовах надзвичайних ситуацій, пов'язаних із функціонуванням критичної інфраструктури (об'єктами

критичної інфраструктури), забезпечення відновлення функціонування критичної інфраструктури:

• вжиття розроблених і формування нових заходів із попередження можливих кризових ситуацій, що пов'язані з функціонуванням критичної інфраструктури (її окремих секторів чи об'єктів);

• забезпечення готовності критичної інфраструктури, її спроможності функціонувати в умовах кризової ситуації;

• створення нових і вдосконалення наявних інструментів (нормативно-регламентуючих, організаційних, технологічних) попередження та управління в кризових ситуаціях, пов'язаних із функціонуванням критичної інфраструктури (її окремих секторів чи об'єктів);

• підготовка в межах національного плану захисту критичної інфраструктури планів попередження кризових ситуацій, пов'язаних із функціонуванням критичної інфраструктури;

• забезпечення фізичного захисту об'єктів критичної інфраструктури, запобігання несанкціонованим діям (зокрема терористичним актам) щодо об'єктів критичної інфраструктури, пом'якшення негативних наслідків і відновлення функціонування об'єктів критичної інфраструктури, якщо мали місце несанкціоновані дії;

• забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак, а також даних і технологічної інформації, що містяться в системах управління технологічними процесами на об'єктах критичної інфраструктури, від несанкціонованого блокування та модифікації;

• забезпечення необхідного рівня експлуатаційної безпеки на об'єктах критичної інфраструктури, розроблення та вжиття інженерно-технічних заходів підвищення безпеки критичної інфраструктури;

• забезпечення стабільного функціонування критичної інфраструктури в умовах надзвичайних ситуацій та в особливий період;

• формування матеріальних резервів, оцінювання та інвентаризація ресурсів;

• забезпечення відповідно до встановлених законодавством вимог конфіденційності інформації під час оброблення даних про об'єкти критичної інфраструктури;

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

3. Підтримка прийняття рішень щодо захисту критичної інфраструктури, зокрема:

• моніторингу та виявлення можливих кризових ситуацій, пов'язаних із функціонуванням критичної інфраструктури;

• формування пропозицій щодо попередження загроз критичній інфраструктурі;

• встановлення та перегляду вимог до захисту об'єктів критичної інфраструктури в різних режимах функціонування;

• ідентифікації об'єктів критичної інфраструктури; ведення автоматизованого реєстру критичної інфраструктури; збирання, узагальнення й аналізу даних щодо об'єктів критичної інфраструктури та їх функціонування;

• забезпечення функціонування системи обміну інформацією, здійснення постійного моніторингу, аналізу та прогнозування загроз об'єктам критичної інфраструктури;

• виявлення та оцінки взаємозалежності між об'єктами критичної інфраструктури;

• визначення та прогнозування об'ємів необхідних ресурсів для забезпечення захисту критичної інфраструктури;

• підтримку прийняття рішень щодо реагування на надзвичайні ситуації, пов'язані з безпекою та стійкістю критичної інфраструктури;

• аналіз ефективності організаційно-технічних засобів стосовно зниження ризиків життєдіяльності в умовах можливих і реальних загроз функціонуванню критичної інфраструктури.

4. Застосування механізмів регулювання та контролю за функціонуванням критичної інфраструктури:

• здійснення раннього оповіщення (попередження про загрози) операторів об'єктів критичної інфраструктури та надання інформаційної, консультативної, експертної, технологічної допомоги операторам критичної інфраструктури, користувачам їх послуг (населенню) задля попередження, реагування, мінімізації можливого впливу загроз;

• зміна режимів функціонування системи захисту критичної інфраструктури залежно від рівня загроз і правового стану;

• запровадження автоматизованих систем раннього виявлення надзвичайних ситуацій та оповіщення про них;

• розроблення й упровадження стандартів, норм і регламентів захисту критичної інфраструктури;

• здійснення перевірок та оцінки захищеності об'єктів критичної інфраструктури;

• здійснення перевірок та оцінки інформаційної безпеки на об'єктах критичної інфраструктури;

• формування, облік та оновлення паспортів об'єктів критичної інфраструктури, а також карт ризику адміністративно-територіальних одиниць.

5. Міжнародне співробітництво у сферах захисту критичної інфраструктури:

• забезпечення оцінки транскордонних впливів функціонування критичної інфраструктури і трансграничних загроз;

• обмін інформацією та ліпшим досвідом з питань захисту критичної інфраструктури;

• участь України у європейських механізмах захисту критичної інфраструктури;

• аналіз вимог нормативних документів ЄС та їх можливої імплементації в Україні.

Необхідно зауважити, що деякі завдання з наведеного переліку частково охоплені наявними в Україні системами цивільного захисту, боротьби з тероризмом, протидії кіберзагрозам, забезпечення обороноздатності держави. Проте більшість завдань є принципово новими й пов'язані із принципами побудови захисту критичної інфраструктури відповідно до стратегічних цілей державної політики в цій сфері.

Потрібно окремо зупинитися на деяких із наведених завдань системи захисту критичної інфраструктури. Перша група завдань щодо загальної координації містить пункт про створення й підтримку функціонування *національного центру з управління в кризових ситуаціях та захисту критичної інфраструктури* (*далі* – Центр). Таке інституціональне нововведення має сприяти організаційному забезпеченню роботи системи захисту критичної інфраструктури. Центр може бути створений як окремий орган або як структурна частина в межах органу влади, який буде відповідальним за координацію діяльності із захисту критичної інфраструктури. Поміж функцій Центру мають бути такі, здійснення яких спрямоване на вирішення завдань системи захисту критичної інфраструктури, не врахованих у наявних державних системах (цивільного захисту, боротьби з тероризмом, протидії кіберзагрозам тощо), зокрема функції, пов'язані з вирішенням завдань координації (всіх завдань даної групи), підтримки прийняття рішень (більшості завдань), міжнародного співробітництва, а також із частиною функцій двох інших груп.

Завдання захисту критичної інфраструктури зміщують фокус уваги на попередження кризових ситуацій, пов'язаних із функціонуванням критичної інфраструктури в Україні. Потрібно зауважити, що поняття кризова ситуація не має однозначного визначення у вітчизняному законодавстві. Воно вживається і в широкому розумінні як «крайнє загострення протиріч, гостра дестабілізація становища в будь-якій сфері діяльності, регіоні, країні»[36] 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», і у вузькому (галузевому) розумінні, наприклад для системи фізичного захис-

[36]Із 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».

ту 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»[37]. Поняття кризової ситуації для критичної інфраструктури має проміжний характер і враховує вплив зовнішніх чинників безпекового середовища та чинники функціонування самих об'єктів критичної інфраструктури. Для уникнення неоднозначності надамо визначення цього терміна в тому розумінні, в якому він використовується в даній Зеленій книзі.

Кризова ситуація, пов'язана із функціонуванням критичної інфраструктури – це ситуація, за якої виникають чи загострюються чинники, змінюються умови чи характеристики безпекового середовища або 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).

Отже, саме попередження кризових ситуацій має стати головним складником роботи *національного центру з управління в кризових ситуаціях та захисту критичної інфраструктури*. При цьому мають здійснюватися постійний моніторинг і виявлення можливих кризових ситуацій, пов'язаних із функціонуванням критичної інфраструктури. Виконання останнього можливе лише за умов створення в структурі Центру підрозділу (відділу), який виконуватиме функції, притаманні ситуаційним центрам, оперативно та в цілодобовому режимі «24/7» здійснюватиме функції, пов'язанні із завданнями щодо підтримки прийняття рішень у системі забезпечення захисту критичної інфраструктури. Зокрема, такий підрозділ Центру має взаємодіяти (стане невід'ємною частиною) з мережею відомчих і корпоративних ситуаційних центрів (кризових/інформаційно-аналітичних тощо). З огляду на високі здобутки вітчизняних вчених у сфері інформаційних технологій, досить оптимістично сприймається завдання технологічного, методологічного й кадрового оснащення такого підрозділу з функціями ситуаційного центру.

Ще одним нововведенням, закладеним у перелік завдань захисту критичної інфраструктури, є поняття «режим функціонування» зазначеної системи. Потрібно зазначити, що на сьогодні передбачено виокремлені режими функціонування в державних системах цивільного захисту (повсякденного функціонування, підвищеної готовності, надзвичайної ситуації, надзвичайного стану), боротьби з тероризмом (за рівнями терористичної загрози – нормальний, підвищений, високий, критичний), фізичного захисту (нормальне функціонування,

[37]Згідно з визначеннями нормативних галузевих документів, затверджених наказами Держатомрегулювання від 28.08.2008 р. № 156 та від 15.09.2011 р. № 501/1001.

підвищена готовність, функціонування у кризовій ситуації, відновлення нормального функціонування). Не підлягає сумніву, що режими функціонування цих систем пов'язані зі станом захисту критичної інфраструктури. Однак такі режими не співвідносяться із завданнями захисту критичної інфраструктури і не можуть бути зведені разом у єдину шкалу для побудови режимів функціонування системи захисту критичної інфраструктури. Також потрібно враховувати особливості правових режимів надзвичайного стану[38] та зони надзвичайної екологічної ситуації[39], воєнного стану[40], які теж тісно пов'язані з функціонуванням захисту критичної інфраструктури.

З огляду на зазначене та на пріоритет завдання попередження кризових ситуацій для системи захисту критичної інфраструктури, виокремимо такі режими її (системи) функціонування:

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

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

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

---

[38]*Про правовий* режим надзвичайного стану : закон України від 16.03.2000 р. № 1550-III [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/

[39]*Про зону* надзвичайної екологічної ситуації : закон України від 13.07.2000 р. № 1908-III [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/

[40]*Про правовий* режим воєнного стану» : закон України від 12.05.2015 № 389-VIII (в редакції від 11.06.2015 р.) [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/

Перехід до функціонування у режимах надзвичайного та воєнного станів відбувається із проголошенням відповідних правових режимів.

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

Третім нововведенням є створення *національного плану захисту критичної інфраструктури* (*далі* – План). Метою такого документа є детальний огляд системи захисту критичної інфраструктури, що містить і визначення способів розвитку системи, і загальний опис конкретних механізмів досягнення завдань системи. Особливу увагу в Плані необхідно приділити *діям з попередження кризових ситуацій*[41] задля визначення механізмів виявлення та пом'якшення загроз критичній інфраструктурі (її секторам). Ще одним нововведенням завдань системи захисту критичної інфраструктури, на яку потрібно звернути увагу, є підготовка *національної проектної загрози для критичної інфраструктури*. На сьогодні в Україні в державній системі фізичного захисту передбачено розроблення й періодичне уточнення проектної загрози, що фактично визначає перелік тих загроз (та їх характеристики), на які має бути розраховано фізичний захист об'єктів. Хоча система фізичного захисту спрямована на захист лише окремої категорії об'єктів (ядерних матеріалів, ядерних установок, радіоактивних відходів, інших джерел іонізуючого випромінювання), механізм визначення проектної загрози є важливим з погляду визначення вимог до систем фізичного захисту, і, відповідно, до обов'язків оператора із забезпечення безпеки об'єктів. На нашу думку, досвід ядерної галузі щодо розроблення проектної загрози можна поширити (із внесенням відповідних коректив) і на інші сектори критичної інфраструктури.

---

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

5.2. Суб'єкти системи захисту критичної інфраструктури

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

Разом з тим у багатьох країнах світу саме в приватній власності перебуває значна, а подекуди й основна частина об'єктів критичної інфраструктури. Тому, наприклад, у Національній стратегії (безпеки) критичної інфраструктури Канади підкреслюється, що «головна відповідальність за підвищення стійкості/здатності до швидкого відновлення (*resilience*) критичної інфраструктури залишається за власниками та операторами»[42]. У зв'язку із цим ефективне державно-приватне партнерство (*далі* – ДПП) у сфері безпеки загалом і захисту критичної інфраструктури зокрема є чи не найважливішим складником здійснення державної політики в цьому напрямі.

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

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

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

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

---

[42]*National* Strategy for Critical Infrastructure [Електорнний ресурс]. – Режим доступу: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx

У Польщі завдання координації заходів щодо захисту критичної інфраструктури покладено на Урядовий центр безпеки (*Government Centre for Security*), який є надміністерською організацією, підпорядкованою безпосередньо прем'єр-міністру. Цим центром було розроблено Національну програму захисту критичної інфраструктури.

В Україні відсутнє визначення критичної інфраструктури на законодавчому рівні, тому відсутнє й поняття суб'єкта захисту критичної інфраструктури. У нашій державі сьогодні паралельно функціонують Єдина система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків (Положення затверджено Постановою Кабінету Міністрів України від 15.08.2007 р. № 1051), Єдина державна система цивільного захисту (Положення затверджено Постановою Кабінету Міністрів України від 09 січня 2014 р. № 11), Державна система фізичного захисту (Порядок функціонування затверджено Постановою Кабінету Міністрів України від 21 грудня 2011 р. № 1337).

Зазначені системи створені, зокрема, для захисту життєво важливих для держави об'єктів від окремих видів загроз, що обумовлює домінування відомчих підходів до розв'язання безпекових проблем національного масштабу.

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

Через об'єктивну необхідність забезпечення захисту від кіберзагроз, активізувалася робота щодо створення національного центру кіберзахисту і протидії кіберзагрозам, а також національного центру оперативно-технічного управління мережами телекомунікацій України для забезпечення потреб обороноздатності держави в особливий період (відповідне завдання згадується в Рішенні РНБОУ[43]).

У січні 2015 р. Кабінет Міністрів України Постановою № 18 затвердив Положення про Державну комісію з питань техногенно-екологічної безпеки та надзвичайних ситуацій (*далі* – Положення) та її склад. Згідно із цим документом Державна комісія з питань техногенно-екологічної безпеки та надзвичайних ситуацій (*далі* – Державна надзвичайна комісія) є постійно діючим органом, який забезпечує

[43]*Про невідкладні* заходи щодо захисту України та зміцнення її обороноздатності : рішення Ради національної безпеки і оборони України від 28.08.2014 р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/

координацію діяльності центральних і місцевих органів виконавчої влади, пов'язаної із забезпеченням техногенно-екологічної безпеки, захисту населення й територій від наслідків надзвичайних ситуацій, організаційних заходів протидії терористичній діяльності й воєнній загрозі, запобігання виникненню надзвичайних ситуацій і реагування на них.

Поміж основних завдань Державної надзвичайної комісії зазначено й такі, що є близькими за змістом до завдань захисту критичної інфраструктури:

• координація діяльності центральних і місцевих органів виконавчої влади щодо забезпечення:

– живучості об'єктів національної економіки та державного управління *під час реагування на надзвичайну ситуацію*;

– стабільного функціонування паливно-енергетичного комплексу *під час виникнення надзвичайної ситуації*, злагодженої роботи підприємств, установ та організацій для забезпечення сталої й безперебійної роботи Єдиної газотранспортної та об'єднаної енергетичної систем України;

– безпеки та сталої роботи транспортної інфраструктури, послуг поштового зв'язку та всіх видів електричного зв'язку;

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

Формально прийняття зазначеної Постанови частково вирішує питання координації дій щодо захисту критичної інфраструктури, проте обмежується лише межами надзвичайних ситуацій у розумінні системи цивільного захисту.

Системне комплексне вирішення питань захисту критичної інфраструктури неможливе в межах наявної системи цивільного захисту через методологічні обмеження.

Вибір тієї чи іншої організаційної моделі захисту критичної інфраструктури для України потребує ретельного вивчення зарубіжного досвіду. Попередній аналіз свідчить про прийнятність для України організаційного підходу, застосованого в сусідній Польщі, в межах якого можна було б використати деякі українські напрацювання у створенні ситуаційних центрів національного й галузевого рівнів для побудови національної мережі розподілених ситуаційних центрів. Однією з головних функцій зазначеної мережі має бути інформаційно-аналітична підтримка національного ситуаційного/кризового центру.

5.3. Розвиток механізмів захисту критичної інфраструктури в Україні

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

• створення нормативно-правових та організаційних механізмів захисту критичної інфраструктури;

• визначення пріоритетних секторів критичної інфраструктури;

• визначення органів державної влади, відповідальних за формування та реалізацію державної політики щодо захисту критичної інфраструктури, чіткий розподіл відповідальності між усіма учасниками процесів/заходів із захисту критичної інфраструктури;

• розроблення й 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 і способів зменшення ризиків, пов'язаних із функціонуванням критичної інфраструктури, підвищення надійності, живучості та стійкості об'єктів критичної інфраструктури, запобігання виникненню на них надзвичайних ситуацій;

• удосконалення механізмів державно-приватного партнерства, визначення джерел фінансування захисту критичної інфраструктури;

• упровадження інноваційних розробок та вдосконалення наявних засобів забезпечення безпеки та захисту об'єктів критичної інфраструктури;

• розроблення й упровадження стандартів, правил, технічних умов захищеності об'єктів критичної інфраструктури;

• упровадження в систему управління діяльністю операторів «культури управління ризиками»;

• удосконалення систем і режимів охорони об'єктів критичної інфраструктури;

• залучення експертного співтовариства, громадськості, поширення інформації та передових досягнень, підготовка кадрів, проведення тренувань і навчань;

• усунення джерел загроз, зменшення рівня загроз у спосіб застосування комплексних безпекових заходів (наприклад, у межах системи боротьби з тероризмом);

• розвиток міжнародного співробітництва з питань захисту критичної інфраструктури.

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

Щодо забезпечення нормативно-правового регулювання захисту критичної інфраструктури:

• визначення основних термінів (критична інфраструктура, захист критичної інфраструктури, оператор критичної інфраструктури тощо);

• запровадження порядку ідентифікації (визначення переліку) об'єктів критичної інфраструктури;

• запровадження порядку зміни режимів функціонування системи захисту критичної інфраструктури залежно від визначеного рівня загроз;

• врегулювання порядку обміну інформацією, збору даних про об'єкти критичної інфраструктури, загрози та ризики для цих об'єктів.

Щодо інституційного забезпечення відповідних заходів:

• створення *національного центру з управління в кризових ситуаціях та захисту критичної інфраструктури*, забезпечення організаційно-технічної та наукової підтримки функціонування в його структурі ситуаційного центру як вузла мережі ситуаційних центрів, побудованої на основі єдиних регламентів взаємодії та уніфікованих методологічних та організаційних підходів;

• проведення аналізу та оцінки функціонування наявних галузевих ситуаційних центрів (зокрема їх апаратного, методологічного, кадрового забезпечення) задля створення національної мережі розподілених ситуаційних центрів, однією з головних функцій якої має бути інформаційно-аналітична підтримка Головного ситуаційного центру;

Щодо організаційно-технічного, методологічного й кадрового забезпечення:

• розроблення методології віднесення об'єктів до критичної інфраструктури;

• розроблення методології визначення стану об'єктів критичної інфраструктури, а також оцінки ефективності реагування на надзвичайні ситуації на таких об'єктах;

• удосконалення систем моніторингу, зокрема дистанційне зондування Землі, систем прогнозування й підтримки прийняття рішень;

• розроблення та впровадження системи підтримки прийняття рішень для національного ситуаційного центру;

• розроблення рекомендацій щодо започаткування цільових комплексних програм наукових досліджень і 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 на-

вчальних курсів на базі вже наявних навчальних центрів у ядерній галузі, у сфері цивільного захисту тощо.

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

• інформування населення щодо основних цілей захисту об'єктів критичної інфраструктури;

• організація державно-приватного партнерства у сфері безпеки;

• створення умов/стимулів участі компаній-операторів (власників) у забезпеченні захисту критичної інфраструктури;

• підтримка національних виробників на ринку безпекових послуг (зокрема у сфері кібербезпеки);

• створення та підтримка функціонування відповідних консультаційних, дорадчих груп тощо.

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

Через своє географічне розташування Україна має особливо тісні зв'язки з енергетичною і транспортною інфраструктурою країн – членів ЄС. Наша країна є невід'ємною частиною глобального кіберпростору, тому, з огляду на сучасні геополітичні реалії, потрібно усвідомлювати, що, наприклад, газотранспортна система України може розглядатися європейськими й трансатлантичними партнерами як елемент критичної інфраструктури загальноєвропейського значення.

Підписання 21 березня 2014 р. політичної (а 27 червня 2014 р. й економічної) частини Угоди про асоціацію[44], подальша її ратифікація Україною та низкою країн – членів ЄС обумовлюють необхідність визначення першочергових кроків, які повинна зробити Україна з метою приведення своїх підходів у сфері захисту критичної інфраструктури у відповідність до підходів, застосовуваних у цій сфері в ЄС.

В ЄС створення правових та організаційних механізмів захисту критичної інфраструктури було ініційовано в 2004 р. у зверненні Європейської Ради до Європейської Комісії (*далі* – ЄК), в якому ЄК доручалося підготувати загальну стратегію захисту критичної інфраструктури. У жовтні 2004 р. ЄК оприлюднила офіційне повідомлення[45], в якому міс-

[44] *Угода* про асоціацію між Україною, з однієї сторони, та Європейським союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/984_011

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

тився огляд дій ЄК у цій сфері та пропозиції стосовно додаткових заходів заради вдосконалення європейської системи запобігання, готовності й реагування щодо терористичних атак, спрямованих проти елементів критичної інфраструктури ЄС. У повідомленні наголошувалося, що підхід до захисту критичної інфраструктури у всіх країнах ЄС має бути методологічно близьким. Забезпечити впровадження та реалізацію такого загального підходу мають Європейська програма захисту критичної інфраструктури (*далі* – ЄПЗКІ) та Європейська інформаційна мережа попередження загроз критичній інфраструктурі (*European Critical Infrastructure Warning Information Network*, *далі – CIWIN*).

В офіційному повідомленні № 786 за 2006 р.[46] ЄК рекомендувала всім країнам ЄС вжити заходів, зазначених в ЄПЗКІ:

• розробити національну програму (план) захисту критичної інфраструктури як документ, що має правову силу;

• задовольнити такий рівень охорони здоров'я, технологічної безпеки, соціально-економічного добробуту, який би гарантував стійкість нації до загроз;

• уніфікувати зусилля, спрямовані на захист критичної інфраструктури, надавши єдиному державному органу, що підзвітний із цього питання, функції координації дій державних органів влади, які спеціалізуються та мають тісні зв'язки 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 й досвідом між країнами – членами ЄС, урядовими структурами та приватним сектором;

• зробити внесок у створення гармонізованої методології на рівні ЄС та загальноєвропейської системи аналізу ризиків.

Пропозиції щодо процедури та критеріїв визначення об'єктів критичної інфраструктури на загальноєвропейському рівні було представлено в Зеленій книзі (2005 р.)[47]: розглянуто 11 секторів критичної інфраструктури, які охоплюють 37 підсекторів. Надалі під час підготовки проекту Директиви, було визначено 11 секторів із 29 підсекторами[48], а

[46] *On a European* Programme for Critical Infrastructure Protection : COM/2006/786 final [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

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

[48] *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/

вже в ухваленій Директиві ЄК[49] згадуються тільки два сектори європейської критичної інфраструктури, що складаються з восьми підсекторів:

• енергетика (електромережі та об'єкти з генерування й передачі електроенергії; нафтопереробна й нафтовидобувна промисловість, нафтопроводи та сховища; газовидобувна промисловість, газопроводи, термінали зрідженого газу);

• транспорт (автомобільний; залізничний; авіаційний; річковий флот; океанічний і морський флот і порти).

Водночас Директивою не заборонено визначати національні критичні інфраструктури в інших секторах.

Щодо *CIWIN*, то основним завданням цієї мережі є створення інструментів координації та інформаційного обміну щодо критичної інфраструктури на загальноєвропейському рівні. *CIWIN* характеризується високими вимогами до забезпечення інформаційної безпеки, оскільки в мережі обробляється інформація, чутлива щодо забезпечення безпеки об'єктів критичної інфраструктури[50].

Отже, під час розроблення системи захисту критичної інфраструктури в Україні, з огляду на євроінтеграційний курс нашої держави, необхідно спрямувати зусилля на досягнення узгодженості національного законодавства з нормативними актами ЄС щодо:

• загальних принципів захисту критичної інфраструктури;

• тлумачення основних термінів (див. Дод. В);

• визначення «контактної точки»[51];

• узгодженості щодо пріоритетності захисту критичної інфраструктури (вибору пріоритетних секторів і відповідних підсекторів критичної інфраструктури;

• методологій порівняння та визначення пріоритетних об'єктів у різних секторах;

• упровадження чинних в ЄС стандартів захисту критичної інфраструктури.

Необхідно також зауважити, що в процесі розбудови системи захисту критичної інфраструктури в Україні потрібно враховувати той факт, що відповідно до Угоди про асоціацію в Україні вже створено Механізм раннього попередження, призначений для раннього оцінювання потенційних ризиків і проблем, пов'язаних із попитом та

---

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

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

[51] З англ. – «*point of contact*».

пропозицією на природний газ, нафту чи електричну енергію, та для попередження й швидкої реакції у випадку надзвичайної ситуації чи загрози надзвичайної ситуації.

Особливу увагу в процесі розвитку національної нормативно-правової бази у сфері захисту критичної інфраструктури потрібно приділити документам, призначеним максимально наблизити вимоги національного законодавства до вимог щодо функціонування та захисту критичної інфраструктури в галузі енергетики й транспорту, визначених у директивах ЄС і вказаних в Угоді про асоціації між Україною та ЄС[52]:

• Директива № 2005/89/ЄС щодо заходів із забезпечення безпеки постачання електроенергії та інвестицій в інфраструктуру;

• Директива № 2004/67/ЄС стосовно заходів щодо забезпечення безперервного постачання природного газу (у 2010 році Директива була замінена Регламентом №994/2010 щодо заходів забезпечення безпеки газопостачання)[53];

• Директива № 2005/65/ЄС Європейського Парламенту та Ради від 26 жовтня 2005 р. про посилення безпеки портів;

• Регламент (ЄС) № 725/2004 від 31 березня 2004 р. про посилення безпеки суден та портових споруд;

• Директива 2004/49/ЄС Європейського Парламенту та Ради від 29 квітня 2004 р. про безпеку залізниць у Співтоваристві[53];

• Регламент (ЄС) № 336/2006 Європейського Парламенту та Ради від 15 лютого 2006 р. про імплементацію Міжнародного кодексу з управління безпекою в межах Співтовариства[54].

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

---

[52]*Додаток* XXVII до Угоди про асоціацію [Електронний ресурс]. – Режим доступу: http://www.kmu.gov.ua/docs/Agreement/Annex_XXVI_to_XLIII_to_Agreement.pdf

[53]*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

[54]*On the implementation* of the International Safety Management Code within the Community and repealing Council Regulation (EC) No 3051/95 : Regulation (EC) No 336/2006 of the European Parliament and of the Council of 15 February 2006 [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006R0336

7. Основні висновки

Зелена книга окреслила широкий спектр питань, пов'язаних із захистом критичної інфраструктури. У ній міститься як аналіз ситуації в Україні щодо вирішення завдань захисту окремих груп об'єктів критичної інфраструктури, так і аналіз досвіду побудови системи захисту критичної інфраструктури у провідних країнах світу. Не применшуючи значення інших питань, увагу сфокусовано на аспектах, пов'язаних передусім із формуванням державної політики в цій сфері та створенням у майбутньому системи захисту критичної інфраструктури в Україні.

1. Нині захист критичної інфраструктури є складником безпекової політики і на національному рівні окремих країн – членів ЄС та НАТО, і на міжнародному – в межах зазначеного міждержавного об'єднання та воєнно-політичного блоку. Для України, з огляду на складну безпекову ситуацію, завдання створення системи захисту критичної інфраструктури може здатися надто амбітним. Проте його поступове втілення в життя уможливить зміцнення системи захисту національної безпеки, посиливши її здатність до попередження кризових ситуацій, пов'язаних із функціонуванням критичної інфраструктури. Разом з тим запровадження системи захисту критичної інфраструктури ще більше наблизить вітчизняні механізми управління у сфері національної безпеки до вже впроваджених у країнах – членах ЄС і НАТО. Захист критичної інфраструктури в Україні має стати невід'ємною частиною загальноєвропейського механізму у сфері безпеки.

2. У Зеленій книзі визначено *стратегічні цілі державної політики* у сфері захисту критичної інфраструктури, а відповідно до них – *завдання системи захисту* критичної інфраструктури та *принципи побудови* захисту критичної інфраструктури. Своєю чергою, завдання системи обумовлюватимуть *функції суб'єктів захисту* критичної інфраструктури. Для створення державної системи захисту критичної інфраструктури в Україні необхідно внести певні зміни до національного законодавства. Доречно прийняти окремий *Закон України*, який би визначив принципи державної політики у сфері захисту критичної інфраструктури в Україні, суб'єкти, завдання та структуру системи захисту критичної інфраструктури в Україні, встановив відповідальність органів державної влади щодо визначення особливостей функціонування цієї системи.

3. Політика захисту критичної інфраструктури має будуватися на фундаменті співробітництва між державним і приватним секторами. Тому формування та розвиток системи державно-приватного партнерства є наріжним каменем державної політики з питань захисту критичної інфраструктури й має знайти законодавче врегулювання, методологічне та організаційно-технічне забезпечення узгоджених дій.

Зокрема, взаємовідносини між оператором та державою і щодо забезпечення функціонування системи захисту критичної інфраструктури, і щодо обміну інформацією відповідно до встановлених вимог потребують нормативного, організаційного й технічного врегулювання в межах функціонування державної системи захисту критичної інфраструктури.

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

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

4. Особливості завдань захисту критичної інфраструктури, що відрізняють її від діючих систем цивільного захисту, боротьби з тероризмом, протидії кіберзагрозам тощо, обумовлюють необхідність організаційних нововведень: *створення національного центру з управління в кризових ситуаціях та захисту критичної інфраструктури* як окремого органу або як структурної частини в межах органу влади, визначеного відповідальним за координацію діяльності із захисту критичної інфраструктури. Такий Центр має координувати розроблення правових, організаційних, технологічних та інших інструментів захисту критичної інфраструктури, організовувати й залучати до роботи всі зацікавлені сторони (операторів, регуляторів, органи місцевого самоврядування, громадськість тощо). Уточнення завдань системи захисту критичної інфраструктури, визначення функцій її суб'єктів потребує подальшого обговорення цієї проблематики в експертному співтоваристві, поміж державних службовців, співробітників правоохоронних органів і спецслужб та представників приватного сектору, до компетенції та інтересів яких входить зазначена проблематика.

5. Хоча в Зеленій книзі запропоновано *перелік секторів* критичної інфраструктури, а також наведено загальну структуру *критеріїв віднесення об'єктів* до переліку критичної інфраструктури, процес їх ідентифікації потребуватиме нормативно-законодавчого, організаційного та методологічного забезпечення. Варто зауважити, що жодна з наявних нині категорій об'єктів, для яких встановлюються особливі умови забезпечення їх захисту та функціонування, не має підстав бути віднесеною в повному складі до критичної інфраструктури без додаткового аналізу.

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

Додаток А

Пропозиції щодо переліку секторів критичної інфраструктури та відповідальних відомств[55]

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

* У межах завдань боротьби з тероризмом;
** Щодо забезпечення охорони об'єктів;
*** Щодо протидії кіберзагрозам;
**** У межах завдань безпеки цивільної авіації;
***** У межах завдань цивільного захисту.

[55]Відповідальні відомства при прийнятті нормативно-законодавчих актів з регулювання захисту критичної інфраструктури має бути уточнено.

Додаток Б

Структура Проекту закону України «Про критичну інфраструктуру»

I. Загальні положення
1. Сфера дії Закону
2. Визначення
II. Державна політика захисту критичної інфраструктури
3. Принципи державної політики у сфері захисту критичної інфраструктури
4. Цілі державної політики захисту критичної інфраструктури
5. Об'єкти захисту критичної інфраструктури
6. Суб'єкти захисту критичної інфраструктури
III. Система захисту критичної інфраструктури
7. Цілі та завдання системи захисту критичної інфраструктури
8. Повноваження та завдання органів державної влади у сфері захисту критичної інфраструктури
9. Взаємодія з іншими системами захисту у сфері національної безпеки
10. Організація взаємодії у сфері захисту критичної інфраструктури
11. Обмін інформацією у сфері захисту критичної інфраструктури
12. Визначення та оповіщення щодо рівня загроз критичній інфраструктурі
13. Зміна режимів функціонування систем захисту критичної інфраструктури залежно від рівня загроз і правового стану
14. Участь громадськості в захисті критичної інфраструктури
IV. Механізми реалізації політики захисту критичної інфраструктури
15. Критерії та методологія віднесення об'єктів до переліку критичної інфраструктури
16. Система моніторингу стану об'єктів критичної інфраструктури, аналізу та прогнозування загроз критичній інфраструктурі
17. Національна та об'єктова проектна загроза для критичної інфраструктури
18. Національний план і програма захисту критичної інфраструктури
19. Плани реагування операторів на кризові ситуації
20. Національна система ситуаційних центрів
V. Державно-приватне партнерство у сфері захисту критичної інфраструктури
20. Завдання та відповідальність органів державної влади
21. Повноваження та завдання операторів критичної інфраструктури
22. Відповідальність операторів критичної інфраструктури

Додаток В

Основні визначення у 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 підтримання життєво важливих функцій суспільства, здоров'я, безпеки, захищеності, економічного та соціального добробуту людей. Порушення їх функціонування або знищення матимуть значний вплив у країні – члені ЄС та призведуть до неспроможності 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. Значущість впливу має бути оцінено в термінах міжсекторальних критеріїв (зокрема впливу, спричиненого міжсекторальними взаємозв'язками з 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 оцінення вразливості й 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 може бути використано 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 – усі види діяльності, спрямовані на забезпечення функціональності, безперервності й цілісності критичної інфраструктури задля недопущення, пом'якшення та нейтралізації загроз, ризиків і 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'єкта, системи або її частини, що згідно з Директивою Європейської Комісії 2008/114 визначені як Європейська критична інфраструктура	**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.

ДОПОВІДІ УЧАСНИКІВ МІЖНАРОДНИХ ЕКСПЕРТНИХ НАРАД З ПИТАНЬ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

INTRODUCING CRITICAL INFRASTRUCTURE PROTECTION CONCEPT IN UKRAINE: LESSONS TO LEARN

Sergii KONDRATOV,
Senior Researcher at National Institute for Strategic Studies

The terrorist attacks against the U.S. on 11 September 2001 showed inadequacy of the security systems both at national and global levels to the sharply increased threats of terrorism and extremism, and forced the international community to cardinally reconsider security approaches worldwide. One of the most important results of such reconsideration was enhanced attention the developed nations began to pay to protection of their critical infrastructures. Following the U.S., a pioneer in this field, a number of nations, first of all NATO and EU member-states, put on the priority list a challenging goal – to protect critically important for them systems, objects and resources against terrorist and other, more traditional, threats such natural disasters and man-made catastrophes and their combinations.

As for Ukraine, our country's security sector since our nation gained independence until the recent crisis was mostly remaining under conditions of stagnation or, even, degradation. That is why its structure, agencies' and bodies' responsibilities and authorities as well as conceptual approaches to respond to modern threats and challenges to national security were far from required ones. Thus, efforts to introduce the concept of critical infrastructure protection in Ukraine were started practically from scratch.

When considering the current situation in Ukraine, undoubtedly, our main concerns are connected with the human costs of the crisis which has led to about 6,500 people killed and 16,000 wounded[1]. Another important aspect of the crisis is the severe humanitarian situation directly connected with the damage and destruction of critical infrastructure systems and objects, first of all those providing water and energy supply. At this point, bearing in mind that after violence cessation the urgent steps will be addressed to restore, first of all, services and functions vitally important to

[1] *UN Office* for the Coordination of Humanitarian Affairs (OCHA) 29 June 2015 [Електронний ресурс]. – Режим доступу: http://www.unocha.org/top-stories/all-stories/five-things-you-need-know-about-crisis-ukraine

public health, safety and security, state governance, economy, etc., understanding a critical infrastructure idea will be of use as well.

This paper outlines the first steps made by Ukraine to introduce critical infrastructure protection (CIP) concept, analyzes the difficulties and obstacles Ukrainian experts and public servants faced as well as experience gained on this way.

First step: creation of the interagency expert working group

Despite Ukrainian political leaders repeatedly stated about Ukraine's choice one day to join the European community in the field of critical infrastructure protection nothing was made to approach Ukrainian legislation to EU's one not saying about practical steps, and by the beginning of 2011 nobody could find the term «critical infrastructure» in the Ukrainian laws and regulations, as opposed to the NATO- and EU-member-states where CIP protection had been intensively developed since 9/11. Thus, in this field by 2011 Ukraine could found itself behind the nations mentioned by, at least, 10 years.

The first practical step to catch this gap was made in March 2011 when the Interagency Expert Working Group (IEWG) on WMD Nonproliferation, Counterterrorism & Critical Infrastructure Protection was established at the National Institute for Strategic Studies. CIP and related issues has become one of the principal subject areas the IEWG addressed in its activities. More than a third of all events carried out by the IEWG were directly devoted to CIP, including international conference on CIP protection (September 2013) carried out with and sponsored by the PDP of the NATO Liaison Office in Ukraine. Besides, a number of problems discussed at the IEWG's meetings considered the issues (e.g. combating nuclear and radiological terrorism, threats and risk assessment in nuclear security area) were also relevant to CIP.

At this stage we faced mostly alert colleagues' attitude which was based on the following:

- misunderstanding of the critical infrastructure (CI) idea;
- doubts regarding whether or not Ukraine being in poor economic condition and suffering from lack of funding for cardinal reforms in all sectors was needed to implement such a concept;
- attempts to incorporate a would-be CIP system into existing state ones dealing with either civil defense (response to emergencies) or combating terrorism, etc.;
- just reluctance to change anything connected with their status, duties, authorities, etc.

Nevertheless, we continued our efforts including making presentations at the meetings and conferences, publication of papers on a subject matter and so on. The situation concerning CIP began getting more favorable, but

a real turnaround occurred when the NISS decided to seek support from the PDP of NATO Liaison Office in Ukrainian on this particular issue. Our experts were informed about CIP as one of the priorities in NATO activities named as «protecting Allied nations' critical infrastructure». When persuading our Ukrainian colleagues in importance of the CIP we often referred to the NATO's and EU's efforts and argued that it would be impossible to join one day either of these organizations without harmonizing Ukraine's security approaches (including that CIP was based on) with Alliance's and European ones.

Our bilateral cooperation with the PDP of NATO Liaison Office (hereinafter, PDP) began its development and the next landmark of it became the international conference on subject matter which was arranged by NISS jointly with and sponsored by the PDP.

Second Step: International Conference on CIP[2]

The original idea was to carry out an enlarged meeting of the IEWG focused on the CIP inviting NATO member-states' experts to share experience of their countries concerning CIP concept introduction and further implementation. Then we understood that it would be reasonable to transform the group's meeting into a conference essentially expanding the number of Ukrainian participants to promote CIP idea popularization. And the NISS was supported by the PDP with this regard. Later on one more organization – Public Company «Ukrhidroenergo», the largest hydroelectricity generating company of Ukraine, joined to the NISS and PDP to organize the conference. Its active involvement provided participants with opportunity to have the technical tour of the Kyiv Hydroelectric Power Station (Vyshgorod, Kyiv oblast) and to familiarize with security measures taken at the PC «Ukrhidroenergo».

As for foreign participants of the conference, we were especially interested in involving experts and public servants from Eastern Europe, but other nations' experience was also of great use for us. And the PDP team dealing with conference arrangements succeeded in inviting proper people from such countries as Bulgaria, Finland, Hungary and Poland. The conference was carried out at two venues – the NISS (Kyiv) and PC «Ukrhidroenergo» headquarter (Vyshgorod).

In total, 50 participants took part at the two-day conference, represented four NATO member-states and the PDP. 15 papers on different issues related with CIP were presented. In my view, one of the most useful outputs of the conference in terms of CIP concept introduction in Ukraine was that the majority of participants understood that:

[2]*Концепція* захисту критичної інфраструктури: стан, проблеми та перспективи її впровадження в Україні : Міжнародна науково-практична конференція / НІСД [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/1349

• CIP is an actual direction in ensuring national and international security in NATO and EU member-states, and Ukraine should pay much more attention to this issue;

• NATO would continue support Ukrainian organizations efforts to introduce the CIP concept in our country.

Third Step: Development and Presentation of the Green Paper on Critical Infrastructure Protection in Ukraine

Despite some progress achieved by the NISS to facilitate the CIP concept promotion in Ukraine the main obstacle for further steps was not overcome. The case in point was that in our country by that time the bureaucratic practice established not to deal with something if it was not mentioned in Ukrainian legislation. Thus, the problem was to involve authorities in efforts to promote the CIP concept in Ukraine not having even a definition of the term «critical infrastructure» in the national legislation. The NISS team decided that the way out of this situation could be found in our developing cooperation with the PDP of the NATO Liaison Office in Ukraine.

After a number of consultations and working meetings with the PDP staff the NISS put forward a proposal to include the item on development of the Green Paper on Critical Infrastructure Protection in Ukraine (GP) in the Annual National Programme of Ukraine – NATO cooperation for 2014. This development provided us with «soft legitimization» of the term «critical infrastructure»: while not having the term defined in national legislation we had it in an important official document outlining our country's cooperation with the Alliance. Another important result of this step was strengthening our relationships with the PDP that provided expert, financial and organizational support to our efforts to develop the GP. Such a support was very important for us since our work in this direction was being placed against the background of the dramatic events in Ukraine resulted in, inter alia, sharp deterioration of the political, economic and financial conditions in the country.

The first draft GP was written by D. Biriukov chief advisor at the NISS Department of Technogenic and Ecological Safety[3] in the mid of October 2014. Then, for some reasons, the drafting work on GP was carried on by S. Kondratov and O. Nasvit, senior researchers at the NISS Department of Energy and Technogenic Safety. In so doing the agreed with the PDP algorithm of further drafting work was the following:

• Drafting the text of the GP;

• The draft GP circulation among Ukrainian authorities and organizations involved with its simultaneous translation into English for deliver-

[3]Soon after this due to changes in the NISS organization structure the Department mentioned was included in the newly established NISS Department of Energy and Technogenic Safety and Security.

ing to NATO member-states' experts selected upon the PDP's request to receive feedback;

• Processing comments, notes and proposals received from Ukrainian and NATO experts to take their opinions into consideration when developing the next GP version.

To announce the start of GP development and to implement this algorithm the first international expert meeting («kick-off meeting») was convened by the NISS and the PDP on 9 September 2014. At this meeting the future GP structure was presented and the expert core group was established for follow-up efforts[4].

By 15 October 2014 the first version of the draft GP had been prepared by the NISS team and circulated among expert core group members from Ukraine. To provide experts from the NATO member-states with this and later versions of the draft GP it was necessary to translate the document into English.

The next, second, international expert meeting on GP development was carried out on 25 November 2014. Its aim was to track progress and to present the second version of the draft GP in which Ukrainian experts' remarks, notes and proposals were taken into consideration. Besides, this meeting was marked with a very important development for further Ukraine's international cooperation in this field – the representatives of the NATO ENSEC COE took active part in the event and follow-ups. Unfortunately, at that time because of delay caused by GP translation into English feedback from NATO member-states experts' was not available.

The third international expert meeting was held on 25 February 2015 to discuss further developments regarding GP[5]. At that stage, in author's opinion, the most challenging task appeared to be processing simultaneously a number of fundamental comments and reservations received from the European experts regarding the *first version* of the draft GP while already having feedback from Ukrainian experts on the *second version* of the draft. To, at least partially, fix the situation it was decided to develop the executive summary of the GP in which to take into account European experts comments and proposals as far as possible.

Final version of the GP was presented on the International Expert Meeting held by NISS and NATO NLO in October 2015. This document received significant attention, and it was discussed in November 2015 during Ukraine – NATO Joint Working Group on Civil Emergency Planning and Disaster Preparedness meeting in NATO HQ.

---

[4]See the updated List of the expert core group participants in the Annex 1 to this paper.

[5]See the list of Ukrainian authorities and organizations invited in the Annex 2 to this paper.

At the same time, at this stage of joint efforts a number of methodological and technical difficulties revealed caused by the reasons briefly outlined below.

1. *Novelty of the document (Green Paper) format and CIP concept.* The results of searches in the national databases of legislative and official documents indicated that a Green Paper format, quite a popular in the Western countries, proved to be a rather new one for most of Ukrainian public servants and considerable part of experts. Some of them believe, for instance, that a Green Paper is just another trendy format for documents describing a whole complex of problems existing in a particular field. One more consequence resulted from lack of experience in development and publication of such documents in Ukraine is still the unresolved issue of the GP approval. The question: «Who and how shall approve the GP?» is yet under consideration.

As one of the consequences of poor governance and state machine corruption Ukraine suffered from for decades, new trends and international developments were often ignored by the authorities including those within the national security sector. That was, in author's view, one of the reasons of this sector degradation, and likely explanation to the concrete fact that the CIP concept proved to be an absolutely new subject matter for most of public servants and experts involved in our efforts. In combination with lack of a «*critical infrastructure*» definition in the Ukrainian legislation it was resulted in producing proposals aiming at assigning to critical infrastructure all assets related in one way or another with important functions and services for population and the State regardless of their criticality and time frames within which negative impact caused by their loss might occur. One of the examples of such proposals was a suggestion to include National Parks to the list of critical infrastructure sectors.

2. *Departmental and institutional interests influence.* It is natural that representatives of authorities, law enforcement bodies, research and other institutions consider a problem in terms of their organizations' missions, responsibilities and interests, but this becomes a problem for development when departmental and institutional interests dominate national ones. In such cases we tried to persuade our opponents by means of referring to the experience gained in this field by the NATO and EU member-states. Nevertheless, we faced repeatedly departmental interests which revealed themselves in the following forms:

• Intention to maintain the status-quo;

• Aspiration for including the would-be CIP system in existing ones even though they were not capable of addressing all threats and risks by their purposes and missions[6];

[6]For instance, the Ukrainian civil defense system does not cover counteraction terrorism, but at the beginning of our effort we had a long discussion with domestic experts who persistently argued the core group experts into integrating the CIP into the national civil defense system.

• Attempts to re-orient our activities from the very beginning aimed at creation of a national system to protect critical infrastructure towards solely sectoral infrastructures, e.g. energy one.

While not denying the crucial importance of the energy sector for each country including Ukraine the expert group argued that GP should not be considered as the only tool for ensuring security of critical energy infrastructure. The expert group and the NISS would certainly address energy security and critical energy infrastructure protection issues both in parallel and in the framework of other efforts including cooperation with such a partner as the NATO ENSEC COE.

3. *Technical and organizational problems.* The draft GP developed by the NISS team is a rather large and complicated document. Unfortunately the NISS team failed to fully implement some European experts' recommendations to reduce it to maximum 15 pages.

It was already mentioned before that the role of foreign experts in development in drafting has been exclusively important not only due to valuable contribution in a form of notes, comments and proposals, but also because NATO member-states' experts relying upon their countries experience in this field played a role of arbiters when discussions of Ukrainian experts reached a deadlock. But to facilitate their participation in our efforts we *had to provide them with the draft GP versions translated into English*. This work appeared to be money- and time consuming and was done only through PDP financial and technical support. But even with that support our team failed to synchronize feedbacks from NATO member-states and Ukrainian experts that considerably complicated the process of amending the draft. Ability to communicate in English still remains the problem for a lot of Ukrainian experts and public servants, and the relevant PDP projects designed to improve this situation remain urgent.

Another problem is *lack of special funding* allocated for drafting the GP. The only source of funding has been the limited PDP's budget for relevant projects. This situation does not allow involving NATO member-states' experts for long-term efforts on a permanent basis.

Critical Energy Infrastructure Protection

All countries concerning CIP give without exception their energy sectors the highest priority even among other critical infrastructure elements. And it is understandable because a modern society is heavily dependent on energy sources practically in all spheres of life. Needs in energy are especially escalated during warfare and armed conflicts leading to critical energy infrastructure (CEI) damage and destruction. Unfortunately, Ukraine has suffered from such negative processes for more than a year being a deliberate target of so called «hybrid warfare».

According to the Information Analysis Center of the National Security and Defense Council of Ukraine[7], as of 17 February 2015 besides the greatest concern emerging from vast number of injuries and deaths caused by «hybrid warfare» it also has led to very severe consequences for infrastructure systems and objects, including those relating to energy supply, namely: 2 772 gas pipelines destroyed; 1 080 energy objects either destructed or damaged; damages and loss of control over the technological processes at the coal mines resulted in reduction in coal mining in Ukraine by 35 %.

Of course, only a small part of objects and systems mentioned above may be assigned to national critical infrastructure and CEI, but the general situation with security of critical infrastructure including CEI in Donbas is so severe that one of the Ukrainian experts even proposed to introduce the term «region with the critical state of infrastructure».

Under «hybrid warfare» conditions we must pay extraordinary attention to CEI, and Ukrainian experts, like their foreign colleagues, well understand it. Some discrepancy between the most core group members and representatives of the Ukrainian Ministry of Energy and Coal Industry regarding the purpose and scope of the GP did not follow from lack of awareness of energy infrastructure vital importance for any state but derived from different visions of sequence of measures to be taken. This statement can be confirmed with the development of cooperation between the ENSEC COE and the NISS. It was energy security and CEI protection that were determined as the principal directions of cooperation between the NATO ENSEC COE and the NISS formally launched on 8 July 2015 in Vilnius with the signing the Letter of Intent on Cooperation by both parties.

Particularly, the Ukrainian and NATO experts agreed to cooperate within the framework of the ENSEC COE's project «Hybrid Warfare and Critical Energy Infrastructure: The Ukrainian Conflict Case-Study» and in other efforts addressing energy security.

Conclusions

The significant progress has been made in introduction critical infrastructure protection concept in Ukraine through drafting the Green Paper on a subject matter which expected to be published October 2015.

Participation of NATO member-states' experts has played a key role in progress achieved providing with relevant expertise and best practice examples.

---

[7] «*Чорна* книга Кремля»: зафіксовано наслідки російської агресії в Україні [Електронний ресурс]. – Режим доступу: http://mediarnbo.org/2015/02/18/chorna-kniga-kremlya-zafiksovano-naslidki-rosiyskoyi-agresiyi-v-ukrayini/

The technical and organizational problems when developing the Green Paper in Ukraine are mostly derived from lack of funding for this particular effort and necessity to spend time for drafts translation into English.

Efforts aiming at critical energy infrastructure protection shall be considered as those of highest priority and experience gained in this sphere (especially, in nuclear one) shall be disseminated (where applicable) to other sectors of national critical infrastructure.

ДОСВІД УКРАЇНИ В ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ТА СТІЙКОСТІ КРИТИЧНОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ

СУХОДОЛЯ Олександр Михайлович,
завідувач відділу енергетичної та техногенної безпеки НІСД

Забезпечення сталого функціонування інфраструктури життєдіяльності суспільства не є цілком новим завданням для Української держави. Однак саме сьогодні Україна протистоїть найсерйознішому безпековому виклику за роки своєї незалежності.

З одного боку, спостерігається загальносвітова тенденція до різкого посилення екстремізму й тероризму, небувале зростання рівня організованої злочинності, зокрема й міжнародної, що загалом ускладнює безпекову ситуацію для всіх без винятку країн світу. З іншого боку, розв'язана Росією гібридна війна[8] проти України чітко виявила нові виклики національній безпеці. Порушення інфраструктури стало одним з найбільш значущих чинників підриву стабільності соціально-економічної ситуації в країні.

Аналіз випадків пошкодження енергетичної інфраструктури на території окремих районів Донецької й Луганської областей та в Криму протягом 2014–2015 рр. дозволяє виділити типові випадки (дії), спрямовані на суттєве порушення функціонування системи енергопостачання з огляду на цілі суб'єкта «зловмисної дії»[9].

Одна група випадків може бути класифікована як випадки без цільового наміру: порушення функціонування інфраструктури є своє-

[8]На наш погляд, гібридна війна є не новим феноменом, а лише відображає застосування нових методів та інструментів реалізації інтересів (або трансформованих до вимог нового часу старих методів). У війні проти України Росія застосувала практику диверсійної діяльності, психологічного тиску та інформаційного прикриття операцій, а також елементи кримінальної практики, що стало несподіваним для непідготовленої до такого розвитку подій України.

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

рідним «побічним» наслідком діяльності, спрямованої на виконання інших завдань. Так, на наш погляд, більшість руйнувань енергетичної інфраструктури на сході України була спричинена неточністю обстрілів при веденні бойових дій. До цієї групи також доцільно віднести розукомплектування окремих елементів інфраструктури з метою отримання доходу від їх продажу (металобрухт)[10].

Другу групу випадків становлять цілеспрямовані дії суб'єкта, спрямовані на порушення спроможності інфраструктури виконувати свої функції, які можна розділити за ступенем руйнівного впливу:

• захоплення об'єктів (як це відбулося в АР Крим);

• тимчасове пошкодження або захоплення з метою диктування певних тактичних вимог;

• руйнування інфраструктури;

• блокування відновлення інфраструктури.

Усі зазначені дії є інструментами гібридної війни, спрямованими на здійснення політичного тиску на уряд країни та психологічного впливу на населення, нанесення економічної шкоди країні або отримання локальних переваг в окремих військових та економічних операціях.

Загальною метою таких дій є підпорядкування України інтересам агресора. Причому загальний підхід до досягнення цілі полягає не стільки в нанесенні поразки збройним силам країни, скільки в повалennі уряду місцевим населенням у спосіб цілеспрямованого погіршення умов життєдіяльності населення та функціонування економіки цієї країни. У цьому контексті пошкодження чи знищення критичної інфраструктури (*далі* – КІ) є одним із найголовніших інструментів впливу агресора.

Водночас необхідно зауважити, що спостерігається різке загострення проблеми захисту критичної інфраструктури життєдіяльності для всіх країн світу. З одного боку, людство внаслідок технологічного розвитку (забезпечення комфортності умов існування, доступу до інформації, послуг) стало надміру залежним від наявності КІ, послуг і функцій, які вона надає. Саме тому порушення звичних умов існування людини формуватиме невдоволення населення власним урядом, а отже, стане підґрунтям соціально-політичних протестів проти влади.

З іншого боку, на сучасному етапі виділяється низка тенденцій, які дедалі більше вказують на необхідність формування ефективної системи захисту КІ. Використання інфраструктури як інструменту ведення війни з метою вчинення політичного тиску може розглядатися як прототип майбутніх воєн – «інфраструктурних війн». При цьому,

[10]Значний негативний вплив на стан енергетичної інфраструктури спричинили дії місцевих кримінальних груп, які, зокрема, розбирали на металобрухт окремі конструкції об'єктів електроенергетики.

як свідчать події в Україні, суб'єктом зловмисних дій проти КІ може бути держава-агресор, а не лише окремі групи зловмисників (терористичні групи), як вважалося до цього часу. Крім того, в умовах глобалізації економіки й торгівлі, об'єднання транспортних мереж знищення інфраструктури життєдіяльності суспільств може бути інструментом опосередкованого впливу одних країн на інші, навіть на країни, непричетні до конфлікту. Прикладом цього є міграційний потік із країн, охоплених війною (Сирія, Ірак, Афганістан) до країн ЄС[11].

Саме тому реалізація завдання з формування державної системи захисту КІ потребує значних зусиль і залучення наявного практичного досвіду у цій та суміжних сферах.

Першим кроком у напрямі визначення проблеми та формування концептуальних засад такої політики стала «Зелена книга з питань захисту критичної інфраструктури»[12], розроблена Національним інститутом стратегічних досліджень. У ній сформульовано основні концептуальні засади цього напряму безпекової політики, визначено стратегічні цілі державної політики у сфері захисту КІ, а відповідно до них – суб'єкти й завдання системи захисту КІ, принципи побудови захисту КІ та основні механізми здійснення політики.

Пріоритетним напрямом політики є підвищення рівня безпеки та стійкості національної КІ стосовно всього спектра загроз і ризиків. Метою захисту є забезпечення безперебійного сталого функціонування КІ у визначених режимах, запобігання руйнуванню та припиненню її функціонування внаслідок дії всіх чинників, забезпечення швидкого відновлення функціонування КІ після збою в роботі.

Принципова відмінність системи захисту КІ від наявної системи цивільного захисту полягає в її цільовій спрямованості. Метою системи захисту КІ є гарантування спроможності інфраструктури виконувати передбачені функції (надавати послуги), а не захист населення й довкілля від наслідків надзвичайних ситуацій, що є головним завданням системи цивільного захисту. Фактично ідеться про зміщення фокусу уваги на попередження кризових ситуацій, пов'язаних із функціонуванням КІ.

Завданнями системи захисту КІ є запровадження оцінювання ризиків формування кризових ситуацій на рівні і держави, і операторів інфраструктури, а також планування та вжиття заходів із недопущення їх реалізації, що формалізується в межах «превентивного планування». Фактично ідеться про формування спроможності держави запобігати

---

[11] *Туск:* хвиля біженців – новий інструмент в гібридній війні [Електронний ресурс]. – Режим доступу: http://www.polradio.pl/5/38/Artykul/223774

[12] *Зелена* книга з питань захисту критичної інфраструктури / Д. С. Бірюков, С. І. Кондратов, О. І. Насвіт, О. М. Суходоля [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/public/File/2015_nauk_an_rozrobku/Green %20 Paper %20- %20dopovid.pdf

можливим загрозам (зокрема «цілеспрямованим, зловмисним діям» як інструменту завдання поразки країні агресором) у спосіб створення «проактивної» системи захисту, що має низку важливих елементів.

Одним з основних елементів має стати запровадження підготовки проектної загрози для КІ. Проектна загроза має визначати перелік загроз (та їх характеристики), на які має бути розраховано захист КІ, що, відповідно, формуватиме вимоги до оператора щодо забезпечення безпеки об'єктів. Формалізація «національної проектної загрози» на національному рівні дозволить визначити вимоги держави щодо необхідного рівня захисту КІ на державному рівні.

На сьогодні в Україні такий інструмент реалізовано в державній системі фізичного захисту лише окремої категорії об'єктів (ядерних матеріалів, ядерних установок, радіоактивних відходів, інших джерел іонізуючого випромінювання)[13]. Система достатньо відпрацьована, передбачає періодичне уточнення проектної загрози, і, на наш погляд, отриманий у ядерній галузі досвід доцільно поширити на інші об'єкти енергетичної сфери та сфери КІ. Запровадження об'єктової проектної загрози для КІ має сформувати систему взаємодії та відповідальність між операторами і державою у цій сфері, а також створити інструмент визначення фінансових та матеріальних ресурсів, необхідних операторам КІ для створення системи захисту.

Іншим елементом системи захисту КІ є план реагування, що визначає заходи, які мають бути здійснені для ліквідації (пом'якшення) впливу порушення функціонування енергетичної КІ. Прикладом такого підходу в Європейському Союзі є формування системи забезпечення безпеки газопостачання[14], що вимагає від національних урядів розроблення Плану попередження криз (*Preventive Action Plan*) та Плану реагування на кризи (*Emergency Plan*) у сфері газопостачання.

Загалом План попередження криз має містити заходи щодо запобігання, усунення або пом'якшення ризиків порушення функціонування КІ, а План реагування на кризи – заходи щодо забезпечення належного функціонування критичної інфраструктури відповідно до рівня кризової ситуації (визначається режим функціонування) та заходів щодо відновлення функціонування КІ в нормальному режимі[15].

---

[13]*Про фізичний* захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання : закон України від 19.10.2000 р. № 2064-III [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2064-14

[14]*Concerning* measures to safeguard security of gas supply and repealing Council Directive 2004/67/EC : Regulation (EU) No 994/2010 / The European Parliament and of the Council. – 2010. – 20 October .

[15]У серпні 2015 р. відповідно до такого підходу було розроблено План підготовки паливно-енергетичного комплексу України до осінньо-зимового періоду 2015–2016 років та його проходження.

Зазначені плани мають містити заходи протидії загрозам за такими напрямами:

• фізичний захист (спрямований на забезпечення захищеності об'єктів);

• технологічний захист (передбачає підвищення живучості систем, функціональне резервування);

• захист персоналу (підготовка та перевірка персоналу щодо його захищеності);

• захист систем управління (забезпечення захисту системи управління та обміну інформацією);

• правове врегулювання питань функціонування інфраструктури та персоналу в різних режимах;

• плани відновлення (створення планів, резервів і сервісів для швидкого відновлення втрачених функцій).

Ще одним елементом системи захисту КІ є формування системи взаємодії та комунікації між суб'єктами системи захисту. Зазначені питання досить детально відпрацьовано в системі фізичного захисту ядерних установок і матеріалів[16]. Зокрема, затверджено порядок функціонування державної системи фізичного захисту, яким визначено повноваження й завдання учасників державної системи, режими функціонування системи та суб'єктів взаємодії. Запроваджено також державний план взаємодії суб'єктів системи на випадок вчинення диверсій[17], який визначає основні правові та організаційні засади взаємодії суб'єктів системи фізичного захисту, встановлює порядок взаємодії та повноваження учасників плану захисту, процедури взаємодії сил захисту оператора та зовнішніх сил, обміну інформацією між різними суб'єктами.

Необхідно підкреслити важливість розроблення планів реагування та системи взаємодії, а саме необхідність передбачення та виокремлення режимів функціонування системи захисту КІ. Пропонуємо таку класифікацію:

• стале функціонування – КІ функціонує в нормальному режимі (ринкових умовах), обмеження щодо економічної діяльності чи правового регулювання не запроваджуються, здійснюється моніторинг загроз;

---

[16]*Про затвердження* Порядку функціонування державної системи фізичного захисту : постанова Кабінету Міністрів України від 21.12.2011 р. № 1337 [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1337-2011- %D0 %BF

[17]*Про затвердження* державного плану взаємодії центральних та місцевих органів виконавчої влади на випадок вчинення диверсій щодо ядерних установок, ядерних матеріалів, інших джерел іонізуючого випромінювання у процесі їх використання, зберігання або перевезення, а також щодо радіоактивних відходів у процесі поводження з ними : постанова Кабінету Міністрів України від 24.07.2013 р. № 598 [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/598-2013- %D0 %BF

• попередження кризових ситуацій – КІ функціонує в стані готовності до застосування чи вжиття окремих заходів, проте без обмежень щодо економічної діяльності чи правового регулювання, здійснюється моніторинг загроз та оцінювання ризиків, застосовуються ресурси й сили, передбачені об'єктовою проектною загрозою без залучення зовнішніх сил;

• діяльність в умовах кризової ситуації – КІ функціонує в умовах обмежень, запроваджуються особливі режими економічної діяльності й правового регулювання, здійснюється реагування на ризики припинення функціонування із залученням зовнішніх сил і ресурсів[18];

• функціонування в режимі надзвичайного чи воєнного стану – КІ функціонує в особливих умовах, визначених окремими законами[19];

Пропоновані режими функціонування КІ мають бути пов'язанні з режимами функціонування системи забезпечення захисту КІ, що є окремим додатковим завданням, з огляду на наявність різних систем. Зокрема, в державних системах цивільного захисту (повсякденного функціонування, підвищеної готовності, надзвичайної ситуації, надзвичайного стану), боротьби з тероризмом (за рівнями терористичної загрози – нормальний, підвищений, високий, критичний), фізичного захисту (нормальне функціонування, підвищена готовність, функціонування в кризовій ситуації, відновлення нормального функціонування), безпеці газопостачання (раннього попередження (*early warning*); оповіщення ризику (*alert*); аварійна ситуація (*emergency*).

Одним з елементів ефективного функціонування системи захисту критичної інфраструктури є навчання. Цей елемент потребує суттєвого доопрацювання в частині запровадження системи підготовки фахівців за цим напрямом. Варто виділити також позитивний досвід фізичного захисту в ядерній сфері, де регулярно проводяться періодичні спільні навчання із залученням суб'єктів системи захисту відповідно до вимог об'єктового плану взаємодії[20].

Насамкінець необхідно зауважити, що розглянуті проблеми та пропоноване вдосконалення системи захисту КІ потребують свого системного відображення в законодавстві. Хоча в Україні окремі функції, притаманні захисту КІ, вже здійснюються в межах наявних систем (цивільний захист, боротьба з тероризмом, захист від кіберзагроз, фі-

[18] *Про затвердження* Порядку вжиття тимчасових надзвичайних заходів з подолання наслідків тривалого порушення нормальної роботи ринку електричної енергії : постанова Кабінету Міністрів України від 13.08.2014 р. № 372 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/372-2014

[19] *Про функціонування* паливно-енергетичного комплексу в особливий період : закон України від 02.11.2006 р. № 307-V [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/307-16

[20] *Про затвердження* Вимог до об'єктового плану взаємодії у разі вчинення диверсії : наказ Державного комітету ядерного регулювання України від 22.11.2010 р. № 163 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z1264-10

зичний захист, регулювання енергетичного ринку тощо), цілий комплекс проблем залишається неврегульованим.

Необхідно забезпечити врахування більш широкого кола загроз національній безпеці, забезпечити міжвідомчу координацію та узгодження систем управління при функціонуванні у різних режимах.

Тенденція до використання КІ як інструменту ведення гібридних війн зумовлює також необхідність удосконалення оборонної політики, зокрема щодо підвищення взаємодії між різними суб'єктами забезпечення національної безпеки, обізнаності силових структур щодо питань захисту КІ та її впливу на національну безпеку і стійкість країни.

ДО СТВОРЕННЯ ДЕРЖАВНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

БІРЮКОВ Дмитро Сергійович,
головний консультант НІСД

Нині захист критичної інфраструктури є одним із пріоритетів забезпечення національної безпеки і окремих розвинених країн, і їх об'єднань. І хоча вивчення зарубіжного досвіду свідчить про відсутність загальноприйнятої універсальної моделі організації системи захисту критичної інфраструктури (*далі* – КІ) (кожна країна будує таку систему залежно від національних особливостей), для України вкрай важливими є, по-перше, врахування фундаментальних принципів побудови системи захисту критичної інфраструктури, по-друге, практична реалізація кроків з побудови такої системи (наблизить нашу державу до нормативно-правових вимог та організаційних підходів країн – членів ЄС і НАТО). Необхідно зауважити, що ці кроки вже задекларовано у вітчизняних документах стратегічного рівня. Зокрема, в Стратегії національної безпеки України 2015 р.[21] окремим пунктом визначено забезпечення безпеки КІ, а поміж пріоритетів вирішення цього завдання названо і створення системи державного управління її безпекою.

Висвітленню питань впровадження захисту критичної інфраструктури в Україні присвячено *Зелену книгу*, відповідальність за розроблення якої відповідно до Річної національної програми співробітництва Україна – НАТО на 2015 рік покладено на НІСД[22]. Проект Зеленої

[21]Пункт 4.13 «Забезпечення безпеки критичної інфраструктури» Стратегії національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року №287/2015).

[22]Є одним з основних заходів, зазначених у п. 2.1.4 «Демократичний цивільний контроль над сектором безпеки і оборони України» Річної національної програми співробітництва Україна – НАТО на 2015 рік (затверджена Указом Президента України від 23 квітня 2015 р. № 238/2015).

книги було розроблено фахівцями НІСД та опрацьовано із залученням вітчизняних і зарубіжних експертів у сфері захисту КІ.

Потрібно підкреслити, що захист критичної інфраструктури – це надскладне завдання, пов'язане з необхідністю забезпечення міжвідомчої координації, врахування широкого спектра загроз національній безпеці та необхідністю функціонувати в різних режимах (зокрема, перехідних – до виникнення кризової ситуації). І тому, хоча в Україні окремі функції, притаманні захисту КІ, вже здійснюються в межах наявних систем цивільного захисту, боротьби з тероризмом, забезпечення кібербезпеки, фізичного захисту об'єктів ядерної енергетики, регулювання енергетичного ринку тощо, залишається невирішеною низка проблем стосовно координації на загальнодержавному рівні всього спектра заходів із забезпечення захисту критичної інфраструктури в Україні.

Порівняльний аналіз завдань Єдиної державної системи цивільного захисту[23], Єдиної системи запобігання, реагування та припинення терористичних актів і мінімізації їх наслідків[24] та Державної системи фізичного захисту[25] із завданнями, визначеними для системи захисту критичної інфраструктури, в Зеленій книзі вказує на наявність специфічних завдань системи захисту КІ (табл.). До таких завдань належать переважно ті, що стосуються попередження кризових ситуацій, пов'язаних із функціонуванням критичної інфраструктури, координацією та підтримкою прийняття рішень при забезпеченні захисту КІ.

Водночас низка завдань наявних державних систем виходить за межі захисту критичної інфраструктури, тому не можна говорити про поглинання чи реформування цих систем. Навпаки, створення нової системи захисту КІ поряд з наявними державними системами лише доповнить необхідні функції та завдяки взаємодії дозволить поліпшити на стратегічному рівні здатність загальної системи забезпечення національної безпеки.

Так, наприклад, протидія тероризму є широким напрямом дій, що передбачає, зокрема, фізичний захист об'єктів, на які можливим є здійснення терористичних актів (очевидно, частина цих об'єктів буде віднесена й до критичної інфраструктури). Проте боротьба з терористичною ідеологією або фінансуванням тероризму вже виходить за межі захисту критичної інфраструктури.

---

[23]Положення затверджене Постановою Кабінету Міністрів України № 11 від 9 січня 2014 р.

[24]Положення затверджене Постановою Кабінету Міністрів України № 1051 від 15 серпня 2007 р.

[25]Положення затверджене Постановою Кабінету Міністрів України № 1337 від 21 грудня 2011 р.

Таблиця

Порівняння завдань системи захисту КІ із завданнями інших наявних систем

Завдання системи захисту КІ[1]	Порівняння із завданнями інших систем		
	Єдина державна система цивільного захисту[2]	Єдина система запобігання, реагування та припинення терористичних актів і мінімізації їх наслідків[3]	Державна система фізичного захисту[4]
1. Загальна координація захисту КІ в Україні			
– створення та підтримка функціонування національного центру з управління в кризових ситуаціях та захисту критичної інфраструктури;	Відсутнє. Такого центру немає, а УІАСНС не має відповідного аналітично-інформаційного складника	Частково присутнє. Завдання АТЦ спрямовані на координацію дій щодо боротьби з тероризмом, запобігання, реагування і припинення терористичних актів	Частково присутнє. Поміж завдань системи вказуються створення та забезпечення функціонування єдиної системи захищеного зв'язку між органами державної влади та юридичними особами, до повноважень яких належить здійснення функцій обліку, контролю, фізичного захисту і протидії нападу на ядерні установки, об'єкти, призначені для поводження з радіоактивними відходами, іншими джерелами іонізуючого випромінювання, транспортні засоби, що перевозять радіоактивні матеріали
– формування пропозицій щодо вдосконалення нормативно-правової бази у сферах національної безпеки і оборони, пов'язаних із захистом КІ;	*Частково* присутнє (у сфері цивільного захисту)	*Частково* присутнє (у сфері боротьби з тероризмом), зокрема у спосіб «удосконалення організаційних засад міжвідомчої взаємодії суб'єктів боротьби з тероризмом»	*Частково* присутнє (нормативно-правове регулювання питань фізичного захисту ядерних установок, матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання). Держатомрегулювання узагальнює практику застосування законодавства з питань фізичного захисту, розробляє і в установленому порядку вносить на розгляд Кабінету Міністрів України пропозиції щодо вдосконалення такого законодавства[5]

Продовження табл.

Завдання системи захисту КІ[1]	Порівняння із завданнями інших систем		
	Єдина державна система цивільного захисту[2]	Єдина система запобігання, реагування та припинення терористичних актів і мінімізації їх наслідків[3]	Державна система фізичного захисту[4]
– здійснення оцінки загроз критичній інфраструктурі на національному рівні з урахуванням взаємозв'язків окремих об'єктів і секторів інфраструктури, впливу всіх видів загроз, оцінки ризиків на рівні і окремих регіонів, і держави загалом;	*Відсутнє.* Натомість здійснюється «5) опрацювання інформації про надзвичайні ситуації, видання інформаційних матеріалів з питань захисту населення і територій від наслідків надзвичайних ситуацій;» та «6) прогнозування і оцінка соціально-економічних наслідків надзвичайних ситуацій, визначення на основі прогнозу потреби в силах, засобах, матеріальних та фінансових ресурсах»	*Частково* присутнє (у сфері боротьби з тероризмом), зокрема у спосіб «пошуку та аналітичної обробки інформації про загрозу вчинення терористичних актів, джерел фінансування терористичної діяльності»	*Частково* присутнє (формується національна проектна загроза для ядерних установок і матеріалів). Держатомрегулювання бере участь в оцінюванні загрози вчинення диверсії, крадіжки, будь-якого іншого неправомірного вилучення радіоактивних матеріалів
– прийняття рішення та оповіщення щодо зміни режиму функціонування системи захисту критичної інфраструктури залежно від рівня загроз;	*Частково виконується.* Режими функціонування ЄДСЦЗ не збігаються з режимами функціонування, запропонованими для системи захисту КІ	*Частково виконується*	*Частково виконується.* Державна система фіззахисту функціонує в умовах: нормальне функціонування; підвищена готовність; функціонування у кризовій ситуації; відновлення нормального функціонування. Рішення про зміну умов функціонування системи приймає Держатомрегулювання на підставі інформації, поданої відповідними суб'єктами системи та іншими державними органами

– підготовка національного плану захисту КІ;	Не охоплює через де-юре відсутність такого плану		
– підготовка національної проектної загрози для КІ;	Не охоплює через відсутність такого механізму для всіх об'єктів КІ		*Частково* присутнє (формується національна проектна загроза для ядерних установок і матеріалів). Проектна загроза визначається на підставі результатів оцінки загрози вчинення диверсії, крадіжки або будь-якого іншого неправомірного вилучення радіоактивних матеріалів[6]
– координація зусиль усіх зацікавлених сторін (державних органів та місцевої влади, бізнесу й суспільства) щодо захисту КІ, зокрема з горизонтальною координацією операторів взаємозалежних та однотипних об'єктів;	*Не зазначається поміж основних завдань*	*Здійснюється* у сфері боротьби з тероризмом, зокрема у спосіб «забезпечення скоординованої роботи суб'єктів боротьби з тероризмом з організаціями і громадськими об'єднаннями у сфері захисту населення та потенційно уразливих об'єктів від терористичних посягань»; «налагодження взаємодії суб'єктів боротьби з тероризмом із недержавними суб'єктами охоронної діяльності у вирішенні завдань»; «запровадження механізму стимулювання фізичних і юридичних осіб до співпраці із суб'єктами боротьби з тероризмом»	*Не зазначається поміж основних завдань*, але Держатомрегулювання відповідно до своїх функцій у системі фізичного захисту[7] отримує в установленому порядку від відповідних державних органів інформацію про наявні загрози об'єктам системи та повідомляє в установленому порядку ліцензіатам про такі загрози

Продовження табл.

Завдання системи захисту КІ[1]	Порівняння із завданнями інших систем		
	Єдина державна система цивільного захисту[2]	Єдина система запобігання, реагування та припинення терористичних актів і мінімізації їх наслідків[3]	Державна система фізичного захисту[4]
– взаємодія та обмін інформацією з мережею ситуаційних (інформаційно-аналітичних) центрів у сфері безпеки і оборони;	*Не зазначається поміж основних завдань.* Мережі ситуаційних центрів фактично не існує		*Частково* присутнє Завданням системи визначено «організацію роботи з обміну інформацією про стан фізичного захисту та її збереження»
– підготовка державної цільової програми у сфері захисту КІ;	*Частково* присутнє: «4) виконання державних цільових програм, спрямованих на запобігання надзвичайним ситуаціям, забезпечення сталого функціонування підприємств, установ та організацій, зменшення можливих матеріальних втрат»	*Частково*, зокрема щодо підготовки, перепідготовки кадрів	*Частково (щодо фізичного захисту ядерних установок і матеріалів)* Держатомрегулювання організовує роботу з підготовки та виконання загальнодержавних, інших програм фізичного захисту, проведення наукових і науково-технічних досліджень у цій сфері
– формування комплексної науково-дослідної програми з питань захисту КІ;	*Не зазначається поміж основних завдань.* Частково виконується		*Частково виконується* Держатомрегулювання організовує в установленому порядку роботу з проведення науково-технічних досліджень у сфері фізичного захисту, контролює їх проведення, якість результатів досліджень і сприяє впровадженню таких результатів у практику

– здійснення взаємодії (контактна точка) зі структурами ЄС і державними органами країн – членів ЄС	*Виконується лише щодо питань цивільного захисту*	*Виконується лише щодо питань боротьби з тероризмом*	*Виконується Держатомрегулювання як регулятором у галузі ядерної енергетики*
2. Попередження кризових ситуацій, забезпечення готовності до дій у кризових ситуаціях, управління в умовах надзвичайних ситуацій, пов'язаних із функціонуванням критичної інфраструктури (об'єктами КІ), забезпечення відновлення функціонування КІ			
– вжиття наявних і формування нових заходів із попередження можливих кризових ситуацій, пов'язаних із функціонуванням КІ (її окремих секторів чи об'єктів);	*Частково здійснюється згідно з п. 2. завдань*: «забезпечення реалізації заходів щодо запобігання виникненню надзвичайних ситуацій», проте спрямовано виключно на запобігання надзвичайним ситуаціям на окремих об'єктах	Частково здійснюється щодо «прогнозування, виявлення та усунення терористичних загроз»	У Порядку функціонування державної системи фізичного захисту поміж принципів її функціонування (п. 4) названо «принцип запобігання вчиненню протиправних дій, згідно з яким забезпечується виявлення потенційних загроз щодо об'єктів системи та вжиття заходів для успішної протидії таким загрозам» [8]
– забезпечення готовності КІ, її здатності функціонувати в умовах кризової ситуації;	*Частково здійснюється згідно з п. 2. завдань*: «забезпечення готовності міністерств та інших центральних та місцевих органів виконавчої влади, органів місцевого самоврядування, підпорядкованих їм сил і засобів до дій, спрямованих на запобігання і реагування на надзвичайні ситуації», але стосується сил цивільного захисту	*Не вказано в переліку завдань*	*Частково здійснюється.* Затверджений Постановою Кабінету Міністрів України від 24 липня 2013 р. № 598 Державний план взаємодії центральних та місцевих органів виконавчої влади на випадок вчинення диверсій щодо ядерних установок, ядерних матеріалів, інших джерел іонізуючого випромінювання у процесі їх використання, зберігання або перевезення, а також щодо радіоактивних відходів у процесі поводження з ними

Продовження табл.

Завдання системи захисту КІ[1]	Порівняння із завданнями інших систем		
	Єдина державна система цивільного захисту[2]	Єдина система запобігання, реагування та припинення терористичних актів і мінімізації їх наслідків[3]	Державна система фізичного захисту[4]
– створення нових і вдосконалення наявних інструментів (нормативно-регламентуючих, організаційних, технологічних) попередження та управління в кризових ситуаціях, пов'язаних із функціонуванням КІ (її окремих секторів чи об'єктів);	*Частково* виконується: «забезпечення реалізації заходів щодо запобігання виникненню надзвичайних ситуацій»	*Не вказано в переліку завдань*	*Частково* присутнє. Держатомрегулювання узагальнює практику застосування законодавства з питань фізичного захисту, розробляє та в установленому порядку вносить на розгляд Кабінету Міністрів України пропозиції щодо вдосконалення такого законодавства
– підготовка в межах національної програми захисту КІ планів попередження кризових ситуацій, пов'язаних із функціонуванням критичної інфраструктури;	*Відсутнє*. Натомість розробляються плани реагування на надзвичайні ситуації	*Не вказано в переліку завдань*	*Частково* присутнє. Держатомрегулювання організовує в установленому законодавством порядку роботу з підготовки і виконання загальнодержавних, інших програм фізичного захисту, проведення наукових і науково-технічних досліджень у цій сфері

– забезпечення фізичного захисту об'єктів КІ, запобігання несанкціонованим діям (зокрема, терористичним актам) відносно об'єктів КІ, пом'якшення негативних наслідків і відновлення функціонування об'єктів КІ, якщо несанкціоновані дії таки мали місце;	*Частково* здійснюється (щодо пом'якшення негативних наслідків)	*Частково* здійснюється у спосіб «удосконалення систем та режимів охорони об'єктів можливих терористичних посягань, зокрема техногенно небезпечних об'єктів та спеціальних транспортних засобів, задіяних у перевезенні радіоактивних та інших небезпечних речовин»; «запобігання терористичним проявам, забезпечення безпеки об'єктів можливих терористичних посягань»	*Частково* здійснюється. Одним із завдань системи фізичного захисту визначено «*забезпечення захищеності ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання з урахуванням проектної загрози*». *Держатомрегулювання перевіряє діяльність суб'єктів системи фізичного захисту під час виконання ними завдань системи, у т.ч. діяльність зі створення й забезпечення функціонування єдиної системи захищеного зв'язку між органами державної влади та юридичними особами, до повноважень яких належить здійснення функцій обліку, контролю, фізичного захисту і протидії нападу на ядерні установки, об'єкти, призначені для поводження з радіоактивними відходами, іншими джерелами іонізуючого випромінювання, транспортні засоби, що перевозять радіоактивні матеріали*
– забезпечення захисту об'єктів КІ від кібератак, забезпечення захисту даних і технічної інформації, що містяться в системах управління технологічними процесами на об'єктах КІ, від несанкціонованого блокування та модифікації;	*Не належить до завдань*	*Частково* враховано щодо «забезпечення захисту даних, що містяться в системах управління технологічними процесами на техногенно небезпечних об'єктах, від несанкціонованого блокування та модифікації»	

Продовження табл.

Завдання системи захисту КІ[1]	Порівняння із завданнями інших систем		
	Єдина державна система цивільного захисту[2]	Єдина система запобігання, реагування та припинення терористичних актів і мінімізації їх наслідків[3]	Державна система фізичного захисту[4]
– забезпечення необхідного рівня експлуатаційної безпеки на об'єктах КІ, розроблення та впровадження інженерно-технічних заходів з підвищення безпеки КІ;	*Належить* «4) виконання державних цільових програм, спрямованих на запобігання надзвичайним ситуаціям, забезпечення сталого функціонування підприємств, установ та організацій, зменшення можливих матеріальних втрат». Виконується переважно для об'єктів підвищеної небезпеки	*Враховує*, зокрема, «забезпечення належного контролю за обліком вибухових речовин, у т.ч. тих, що зберігаються та використовуються на промислових підприємствах»	*Держатомрегулювання встановлює мінімально допустимі експлуатаційні характеристики систем фізичного захисту об'єктів системи, допустимий ризик вчинення диверсії щодо об'єктів системи залежно від їх категорій та можливих радіаційних наслідків вчинення диверсії*
– забезпечення стабільного функціонування КІ в умовах надзвичайних ситуацій та в особливий період;	*Частково* виконується «10) проведення рятувальних та інших невідкладних робіт щодо ліквідації наслідків надзвичайних ситуацій, організація життєзабезпечення постраждалого населення;»	*Не вказано в переліку завдань*	*Не розглядається як завдання системи фізичного захисту*

– формування матеріальних резервів, оцінка та інвентаризація ресурсів;	*Врахована* в п. 7 завдань « створення, раціональне збереження і використання резерву матеріальних та фінансових ресурсів, необхідних для запобігання і реагування на надзвичайні ситуації;»	*Враховано* щодо «забезпечення суб'єктів боротьби з тероризмом необхідною ресурсною базою»	*Не вказано в переліку завдань. Виконується суб'єктами системи*
– забезпечення конфіденційності інформації відповідно до встановлених законодавством вимог при обробленні даних про об'єкти КІ;	*Не вказано в переліку завдань*	*Частково здійснюється* у спосіб «забезпечення захисту даних, що містяться в системах управління технологічними процесами на техногенно небезпечних об'єктах, від несанкціонованого блокування та модифікації»	*Враховується.* З-поміж першочергових вимог фізичного захисту названо «створення умов для захисту інформації з обмеженим доступом»[9]
– забезпечення відновлення функціонування КІ в разі виникнення аварій/збоїв, вчинення зловмисних дій, що зашкодили її функціонуванню, або впливу природних явищ;	*Частково виконується* «10) проведення рятувальних та інших невідкладних робіт щодо ліквідації наслідків надзвичайних ситуацій, організація життєзабезпечення постраждалого населення»	*Не вказано в переліку завдань*	*Не вказано в переліку завдань*
3. Підтримка прийняття рішень щодо захисту КІ			
– моніторинг і виявлення можливих кризових ситуацій, пов'язаних із функціонуванням КІ;	*Не здійснюється для всіх секторів критичної інфраструктури*	*Частково* (щодо терористичних загроз)	*Здійснюється виключно для ядерних установок і матеріалів. Діє порядок міжвідомчої взаємодії*[10]

Продовження табл.

Завдання системи захисту КІ[1]	Порівняння із завданнями інших систем		
	Єдина державна система цивільного захисту[2]	Єдина система запобігання, реагування та припинення терористичних актів і мінімізації їх наслідків[3]	Державна система фізичного захисту[4]
– формування пропозицій щодо попередження загроз КІ;			*Здійснюється виключно для ядерних установок і матеріалів*
– встановлення та перегляд вимог до захисту об'єктів КІ в різних режимах функціонування;			
– ідентифікація об'єктів КІ; ведення автоматизованого реєстру КІ; збирання, узагальнення й аналіз даних щодо об'єктів КІ та їх функціонування;	*Частково* охоплює (лише щодо об'єктів підвищеної небезпеки та цивільного захисту)	*Частково* здійснюється (охоплює об'єкти можливих терористичних посягань) у спосіб «розроблення та затвердження критеріїв віднесення об'єктів (незалежно від форми власності) до переліку об'єктів можливих терористичних посягань»	
– забезпечення функціонування системи обміну інформацією, здійснення постійного моніторингу, аналізу та прогнозування загроз об'єктам КІ;	*Частково* охоплює (лише щодо об'єктів підвищеної небезпеки)	*Частково* охоплює (об'єкти можливих терористичних посягань)	*Здійснюється виключно для ядерних установок і матеріалів. Діє порядок міжвідомчої взаємодії*[11]

– виявлення та оцінка взаємозалежності між об'єктами КІ;	*Частково* враховано: «6) прогнозування і оцінка соціально-економічних наслідків надзвичайних ситуацій, визначення на основі прогнозу потреби в силах, засобах, матеріальних та фінансових ресурсах»	*Не вказано в переліку завдань*	*Не вказано в переліку завдань, не видно із функцій суб'єктів системи*[12]
– визначення та прогнозування об'ємів необхідних ресурсів для забезпечення захисту КІ;	*Частково* охоплює (лише щодо об'єктів підвищеної небезпеки)	*Частково* охоплює. Пов'язано винятково з терористичною загрозою	*Здійснюється виключно для ядерних установок і матеріалів*
– підтримка прийняття рішень щодо реагування на надзвичайні ситуації, пов'язані з безпекою та стійкістю КІ;	*Відсутнє*. УІАСНС не має відповідного аналітично-інформаційного складника	*Не вказано в переліку завдань*	
– аналіз ефективності організаційно-технічних засобів стосовно зниження ризиків життєдіяльності в умовах можливих і реальних загроз функціонуванню КІ	*Частково* охоплює: «6) прогнозування і оцінка соціально-економічних наслідків надзвичайних ситуацій, визначення на основі прогнозу потреби в силах, засобах, матеріальних та фінансових ресурсах»	*Не вказано в переліку завдань*	*Частково враховано у спосіб здійснення державної перевірки систем фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання та планів взаємодії у разі вчинення актів ядерного тероризму*

Продовження табл.

Завдання системи захисту КІ[1]	Порівняння із завданнями інших систем		
	Єдина державна система цивільного захисту[2]	Єдина система запобігання, реагування та припинення терористичних актів і мінімізації їх наслідків[3]	Державна система фізичного захисту[4]
4. Застосування механізмів регулювання та контролю за функціонуванням КІ, зокрема			
– здійснення раннього оповіщення (попередження про загрози) операторів об'єктів КІ та надання інформаційної, консультативної, експертної, технологічної допомоги операторам КІ, користувачам їх послуг (населенню) задля попередження, реагування, мінімізації можливого впливу загроз;	*Частково* враховує: «8) оповіщення населення про загрозу та виникнення надзвичайних ситуацій, своєчасне та достовірне інформування про фактичну обстановку і вжиті заходи»; водночас відсутня повноцінна взаємодія з операторами об'єктів КІ	*Не вказано в переліку завдань*	*Здійснюється виключно для ядерних установок і матеріалів. Діє порядок міжвідомчої взаємодії*[13]
– зміна режимів функціонування системи захисту КІ залежно від рівня загроз і правового стану;	*Так само, як і з прийняттям рішень та оповіщенням про зміну режиму (завдання з першої групи)*		

– запровадження автоматизованих систем раннього виявлення надзвичайних ситуацій та оповіщення про них;	*Частково* враховує: «8) оповіщення населення про загрозу та виникнення надзвичайних ситуацій, своєчасне та достовірне інформування про фактичну обстановку і вжиті заходи»	*Частково* враховано у спосіб «установлення сучасних систем безпеки, застосування засобів зовнішнього контролю (спостереження) та швидкого реагування на терористичні посягання на відповідних об'єктах»	*Враховано щодо виявлення та оцінки радіаційної обстановки*
– розроблення та впровадження стандартів, норм і регламентів захисту КІ;	*Не вказано в переліку завдань*	*Частково здійснюється* у спосіб «розроблення та впровадження стандартів, правил, технічних умов антитерористичної захищеності об'єктів можливих терористичних посягань, зокрема особливих правил антитерористичної безпеки;»	*Частково здійснюється щодо норм, правил і стандартів та умов ліцензій (дозволів) щодо забезпечення фізичного захисту*
– здійснення перевірок та оцінки захищеності об'єктів критичної інфраструктури;	*Не вказано в переліку завдань*	*Не вказано в переліку завдань*	*Відповідно до завдань системи «здійснюється державний нагляд та контроль за станом фізичного захисту ядерних об'єктів»*
– здійснення перевірок та оцінки інформаційної безпеки на об'єктах КІ;	*Не належить до завдань*	*Не належить до завдань*	*Частково здійснюється. Держатомрегулювання проводить державну експертизу проектів створення, реконструкції та технічного переоснащення систем фізичного захисту об'єктів системи, у т.ч. системи перевезень радіоактивних матеріалів*

Закінчення табл.

Завдання системи захисту КІ[1]	Порівняння із завданнями інших систем		
	Єдина державна система цивільного захисту[2]	Єдина система запобігання, реагування та припинення терористичних актів і мінімізації їх наслідків[3]	Державна система фізичного захисту[4]
– формування, облік та оновлення паспортів об'єктів КІ, а також карт ризику адміністративно-територіальних одиниць	*Частково виконується:* «5) опрацювання інформації про надзвичайні ситуації, видання інформаційних матеріалів з питань захисту населення і територій від наслідків надзвичайних ситуацій; 6) прогнозування і оцінка соціально-економічних наслідків надзвичайних ситуацій, визначення на основі прогнозу потреби в силах, засобах, матеріальних та фінансових ресурсах», а також реєстрування об'єктів підвищеної небезпеки	*Частково* здійснюється щодо «удосконалення систем та режимів охорони об'єктів можливих терористичних посягань, у тому числі техногенно небезпечних об'єктів та спеціальних транспортних засобів, задіяних у перевезенні радіоактивних та інших небезпечних речовин»	*Держатомрегулювання здійснює державний нагляд за дотриманням вимог законодавства з питань фізичного захисту й виконання ліцензійних умов, проводить в установленому порядку державну перевірку систем фізичного захисту об'єктів системи та планів взаємодії у разі вчинення диверсії*
5. Міжнародне співробітництво у сферах захисту КІ			
– забезпечення оцінки транскордонних впливів функціонування КІ та транскордонних загроз;	Частково здійснюється щодо надзвичайних ситуацій, пов'язаних з об'єктами підвищеної небезпеки	*Частково* охоплює (пов'язано винятково з терористичною загрозою)	*Держатомрегулювання здійснює співробітництво у сфері фізичного захисту з Міжнародним агентством з атомної енергії, іншими міжнародними організаціями та відповідними органами іноземних держав*

– обмін інформацією та ліпшим досвідом з питань захисту КІ;	Частково охоплює (лише щодо об'єктів підвищеної небезпеки)	Здійснюється суб'єктами боротьби з тероризмом, в концепції *виокремлено в окремий пункт «5. Міжнародне співробітництво з питань боротьби з тероризмом»*	
– участь України в європейських механізмах захисту КІ;	Частково охоплює в частині цивільного захисту		
– аналіз вимог нормативних документів ЄС та їх можливої імплементації в Україні			

[1]Запропоновано в підрозділі 5.1 Зеленої книги з питань захисту критичної інфраструктури в Україні (НІСД, 2015).
[2]Завдання (з посиланням на відповідні пункти) ЄДСЦЗ названо відповідно до Кодексу цивільного захисту України.
[3]Згідно з Концепцією боротьби з тероризмом (затверджена Указом Президента України від 25.04.2013 р. № 230/2013).
[4]Відповідно до Закону України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» (ст. 5-2).
[5,7,8,12]*Про затвердження* Порядку функціонування державної системи фізичного захисту : постанова Кабінету Міністрів України від 21.12.2011 р. № 1337 [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1337-2011-%D0%BF
[6]Відповідно до Закону України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» (ст. 5-1).
[9]Відповідно до Закону України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» (ст. 18).
[10,11,13]*Про затвердження* державного плану взаємодії центральних та місцевих органів виконавчої влади на випадок вчинення диверсій щодо ядерних установок, ядерних матеріалів, інших джерел іонізуючого випромінювання у процесі їх використання, зберігання або перевезення, а також щодо радіоактивних відходів у процесі поводження з ними : постанова Кабінету Міністрів України від 24.07.2013 р. № 598 [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/598-2013-%D0%BF

Не можна сказати, що вирішенню деяких окремих завдань (наприклад, 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 необхідно звернути увагу на завдання не об'єктового, а системного рівня. Саме недосконаліть заходів із комплексного управління захистом КІ в Україні спричинює необхідність вдосконалювати нормативні, організаційні й технологічні інструменти задля забезпечення безпеки та стійкості критичної інфраструктури.

Потрібно підкреслити важливість створення системи захисту КІ і в аспекті оцінки рівня забезпечення національної безпеки. Нині така оцінка є ретроспективною (здійснюється по факту, за значенням показників, наявністю інцидентів тощо). Такий підхід не дає можливості встановити зв'язок між чинниками, за якими оцінюється рівень (ефективність системи захисту національної безпеки), та об'єктами, стан яких переважно й визначає рівень показників. Крім того, оскільки не окремі об'єкти, а їх взаємне функціонування через взаємовплив визначає показники національної безпеки, необхідно враховувати такі зв'язки.

Аналіз критичної інфраструктури має стати елементом прогнозування та управління рівнем національної безпеки, визначення пріоритетів при забезпеченні національної безпеки. Крім того, оскільки критична інфраструктура є основою соціально-економічного зростання країни, її ґрунтовний аналіз дозволить дивитися в майбутнє і бачити свої переваги, зберігати ці точки зростання і зменшувати загрози для них.

Варто зауважити, що навіть у країнах – членах ЄС немає загальноприйнятої шаблонної моделі для системи захисту КІ[26]. Кожна країна вирішує таке завдання з огляду на власні характеристики, безпекову ситуацію та спроможність політичного керівництва здійснювати реформи в секторі безпеки і оборони. Посилаючись на досвід успішного функціонування Урядового центру з питань безпеки[27] (Республіка Польща), в Зеленій книзі як на одну з основних рекомендацій вказується на необхідність визначення (створення або призначення) орга-

---

[26]*Memorandum* on the results of the sixth Workshop on the Implementation and Application of the Directive 2008/114/EC / Joint Research Center, Institute for the Protection and Security of the Citizen. – 2011 [Електронний ресурс]. – Режим доступу: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC68759/reqno_jrc68759_6th_workshop_memo_final.pdf[1].pdf

[27]*Порядок* організації та режиму роботи Урядового центру з безпеки (польськ. мов.) [Електронний ресурс]. – Режим доступу: http://isap.sejm.gov.pl/DetailsServlet?id=WDU20110860471

ну, що відповідатиме за виконання завдань координації в системі захисту критичної інфраструктури (координатора). Такому органу може бути делеговано низку функцій організаційного характеру, нормативно-правового проектування, підтримки прийняття рішень та аналітичного забезпечення, організації взаємодії з операторами КІ.

На нашу думку, можна розглядати чотири найвірогідніші варіанти побудови системи, які потенційно можуть забезпечити виконання завдань (вказано в Зеленій книзі в підрозділі 5.1):

- варіант 1 – Координатор при РНБО України;
- варіант 2 – Координатор при Кабінеті Міністрів України;
- варіант 3 – Координатор – Міністерство внутрішніх справ України;
- варіант 4 – Координатор Антитерористичний центр при СБУ.

Можливу схему організації представлено на рис. 1.

З огляду на те, що нині частину завдань захисту КІ вже покладено на відповідні центральні органи виконавчої влади, сили, служби й під-

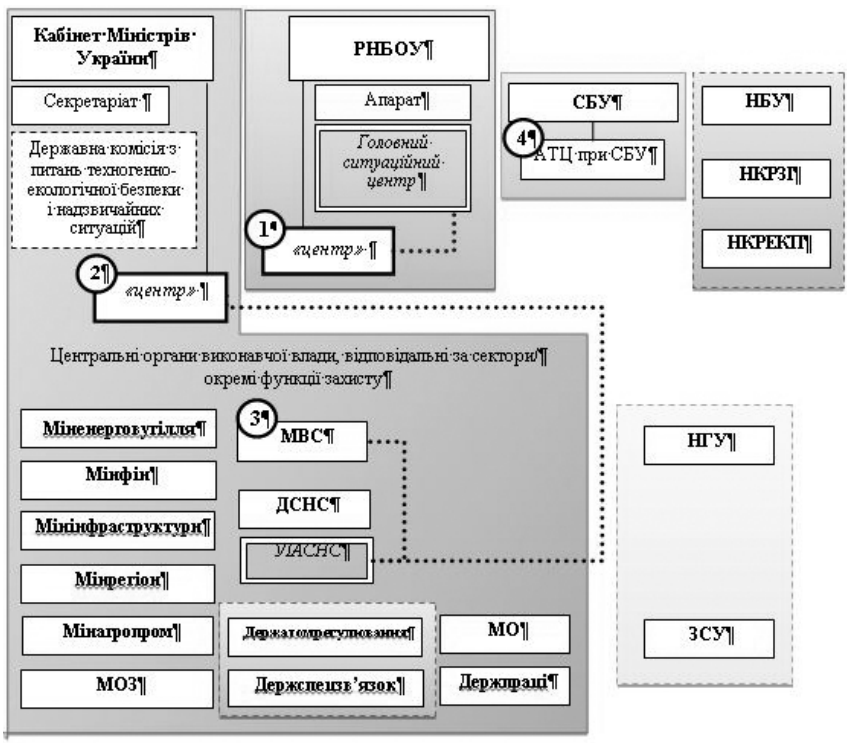

Рис. 1. Схема організаційної побудови системи захисту КІ для 4-х варіантів

розділи, підпорядковані їм, або вониздійснюються операторами тих об'єктів, що мають бути віднесені до КІ, всі чотири варіанти пропонують збереження за суб'єктами захисту критичної інфраструктури покладених на них функцій із забезпечення безпеки та охорони об'єктів.

Потрібно вказати на такі особливості варіантів побудови системи. У разі побудови системи за варіантом 1 координатор створюється при РНБОУ, а функції ситуаційного центру виконує Головний ситуаційний центр України як головний елемент мережі ситуаційних центрів.

За варіанта 2 при Кабінеті Міністрів України створюється робочий орган, на який покладаються функції координатора в системі захисту КІ, а також інформаційно-аналітичної підтримки діяльності Державної комісії з питань техногенно-екологічної безпеки та надзвичайних ситуацій, а функції ситуаційного центру виконує УІАСНС.

У разі побудови системи за варіантом 3 координатором призначається Міністерство внутрішніх справ України (в його структурі створюється підрозділ з питань захисту КІ, а УІАСНС використовується як ситуаційний центр).

За варіанту 4 основний фокус спрямований на терористичні й диверсійні загрози, а також загрози промислового шпіонажу та вчинення впливу через контроль над суб'єктами господарювання, які є критичною інфраструктурою. Організаційно четвертий варіант може бути побудований на базі Антитерористичного центру при СБУ.

У разі створення окремого органу – національного центру з управління в кризових ситуаціях і захисту критичної інфраструктури («центру») як робочого органу при РНБОУ (варіант 1) або при КМУ (варіант 2) – на нього покладається виконання таких функцій:

• формування пропозицій щодо вдосконалення нормативно-правової бази у сферах національної безпеки і оборони, пов'язаних із захистом КІ;

• оцінювання загроз КІ на національному рівні з урахуванням взаємозв'язків окремих об'єктів і секторів інфраструктури, впливу всіх видів загроз, оцінки ризиків і на рівні окремих об'єктів, і для регіонів та держави загалом;

• формування пропозицій щодо вжиття наявних і розроблення нових заходів з попередження можливих кризових ситуацій, пов'язаних із функціонуванням КІ (її окремих секторів чи об'єктів), а також управління в умовах кризових ситуацій;

• звернення із пропозицією щодо скликання засідань Державної надзвичайної комісії та підготовка проектів її рішень;

• прийняття рішення та оповіщення щодо зміни режиму функціонування системи захисту КІ залежно від рівня загроз, зміни правового стану (мирний час, надзвичайна ситуація, особливий період);

• підготовка Національного плану захисту критичної інфраструктури, розроблення планів захисту критичної інфраструктури;

• створення та підтримка функціонування (в режимі цілодобового чергування – «24/7») ситуаційного центру з управління/координації дій у кризових ситуаціях та захисту КІ, забезпечення його взаємодії з ситуаційними (інформаційно-аналітичними) центрами у сфері безпеки і оборони; забезпечення функціонування системи обміну інформацією, здійснення постійного моніторингу, аналізу та прогнозування загроз об'єктам КІ; підтримка прийняття рішень щодо реагування на надзвичайні ситуації, пов'язані із безпекою критичної інфраструктури;

• підготовка проекту державної цільової програми у сфері захисту критичної інфраструктури;

• формування із залученням НАНУ комплексної науково-дослідної програми з питань захисту КІ;

• здійснення взаємодії (контактна точка) зі структурами ЄС і державними органами країн – членів ЄС; аналіз вимог нормативних документів ЄС та їх можливої імплементації в Україні; забезпечення оцінки транскордонних впливів функціонування КІ і трансграничних загроз; обмін інформацією та ліпшим досвідом з питань захисту критичної інфраструктури;

• координація роботи з ідентифікації об'єктів КІ; ведення автоматизованого реєстру критичної інфраструктури; збір, узагальнення та аналіз даних щодо об'єктів КІ та їх функціонування;

• координація зусиль усіх зацікавлених сторін (державних органів і місцевої влади, бізнесу й суспільства) щодо захисту критичної інфраструктури, зокрема з горизонтальною координацією операторів взаємозалежних і однотипних об'єктів;

• координація роботи експертних/консультативних рад з питань захисту КІ (галузевих та орієнтованих на розгляд певних типів загроз);

• координація розроблення та впровадження стандартів, норм і регламентів захисту КІ;

• ініціювання перевірок забезпечення захисту КІ;

• формування рекомендацій щодо підвищення безпеки та стійкості об'єктів КІ, надання цих рекомендацій операторам.

На основі досвіду впровадження захисту КІ в країнах – членах ЄС і НАТО в Зеленій книзі запропоновано перелік секторів критичної інфраструктури. Фахівцями НІСД проаналізовано категорії об'єктів, які знайшли відображення у вітчизняній нормативно-правовій базі та можуть (певна частина з них) бути віднесені до об'єктів КІ в Україні[28]. У кожному із секторів КІ зазвичай визначається відповідальне

[28]*Бірюков Д. С.* Про доцільність та особливості визначення критичної інфраструктури в Україні : аналіт. зап. / Д. С. Бірюков [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/1026/

відомство (*далі* – ВВ), на яке буде покладено низку функцій (часто на практиці ці функції вже виконуються відомством) щодо захисту відповідних об'єктів КІ (див. Додаток Б із пропозицією щодо переліку секторів і відомств).

Різноманітні функції, пов'язані із захистом критичної інфраструктури виконують:

- Президент України;
- Верховна Рада України;
- Рада національної безпеки і оборони України;
- Кабінет Міністрів України;
- міністерства та інші центральні органи виконавчої влади;
- Служба безпеки України;
- Національний банк України (НБУ);
- Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКРЗІ); Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг (НКРЕКП);
- Збройні Сили України, Служба зовнішньої розвідки України, Державна прикордонна служба України та інші військові формування, створені відповідно до законів України;
- суди загальної юрисдикції;
- прокуратура України;
- місцеві державні адміністрації та органи місцевого самоврядування;
- оператори критичної інфраструктури;
- громадяни України та об'єднання громадян.

Крім виконання функцій захисту об'єктів КІ, що були визначені законодавством і покладені на ВВ у межах наявних державних систем, які є елементами загальної системи забезпечення національної безпеки України, передбачається доручити ВВ такі специфічні функції:

- підготовка (узагальнення) пропозицій щодо переліку об'єктів КІ, що віднесені до сфери компетенції;
- формування (узагальнення) пропозицій щодо вдосконалення нормативно-правової бази у сферах національної безпеки і оборони, пов'язаних із захистом об'єктів КІ (за сектором або загрозою);
- взаємодія через секторальний ситуаційний центр з відповідним підрозділом Центру захисту критичної інфраструктури; аналіз та оцінка загроз об'єктам (і на об'єктах) КІ в секторі;
- участь у роботі та стимулювання роботи галузевих (або орієнтованих на розгляд певних типів загроз) експертних/консультативних рад з питань захисту КІ;
- участь у підготовці Національного плану дій із захисту критичної інфраструктури, розроблення секторальних планів захисту КІ;

• формування пропозицій щодо проекту державної цільової програми у сфері захисту КІ;

• здійснення перевірок забезпечення захисту КІ;

• участь у розробленні та впровадженні стандартів, норм і регламентів захисту КІ.

Започаткування системи захисту критичної інфраструктури має бути здійснено на основі прийняття закону України, який має, зокрема, врегулювати організаційно-інституційні питання:

• щодо визначення суб'єктів системи захисту КІ та їх функцій, зокрема утворення національного центру з управління в кризових ситуаціях і захисту критичної інфраструктури;

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

• щодо запровадження порядку зміни режимів функціонування системи захисту критичної інфраструктури залежно від визначеного рівня загроз;

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

Залежно від варіанта побудови системи захисту КІ відповідні підзаконні акти мають затверджуватися указами Президента України або постановами Кабінету Міністрів України.

Висновок

У межах реформування сектору безпеки і оборони України актуальним завданням є створення системи захисту критичної інфраструктури. Потрібно ініціювати процес створення такої системи. Це може бути здійснено у спосіб розгляду на засіданні РНБОУ зазначеного питання, прийняття й ухвалення відповідного рішення Ради, в якому буде визначено органи державної влади, відповідальні за виконання першочергових кроків з утворення системи захисту критичної інфраструктури в Україні.

CRITICAL INFRASTRUCTURE PROTECTION – ROMANIAN CONTRIBUTIONS AND EXPERIENCES

Dr. Liviu MUREŞAN,
Alexandru GEORGESCU
EURISC Foundation, Romania

Critical Infrastructure Protection (CIP) is emerging as an important framework for understanding and ensuring societal security in the context of important interdependencies between critical systems such as energy

and transport infrastructure, each with their own risks, vulnerabilities and threats. Romania is developing a competitive CIP framework, in accordance with Europeans standards, that recognizes not only National Critical Infrastructures, but also European Critical Infrastructures with transborder dimensions. The specific characteristics of Romania's Critical infrastructure and the challenges it faces in ensuring their identification, designation and protection are all relevant to Ukraine's future efforts in this field.

Introduction

The aim of this article is to provide an overview of Critical Infrastructure Protection (CIP), a framework of security thinking which has seen significant development in Western countries and in the most notable emerging economies. Afterwards, the Romanian efforts in this field will be presented, keeping in mind the specifics of both the Romanian Critical Infrastructures (CI) and the characteristics of the security environment in which they operate. The authors hope to underline both the importance of this field for Ukrainian security and future economic development (which are intertwined when it comes to CI) and the value of potentially translating Romanian experiences into useful insights for the future development of a Ukrainian CIP framework.

Critical Infrastructures and their protection

Modern societies are highly dependent on the continuous operation of critical infrastructures that ensure the supply of essential goods and services. These include amongst others the supply of energy in all its forms, drinking water supply, information and communication technologies or waste disposal. Disruptions may have rapid repercussions for the population and the basis of its livelihood, and can affect other critical infrastructures through a domino effect termed «cascading disruptions»[29]. For instance, a power blackout will also disrupt the water supply, telecommunications, and rail transport. Cities, the very engines of economic, social and political development, represent agglomerations of critical infrastructures which are easily disrupted, especially with regards to energy dependencies. This leads to potentially existential threats, such as food insecurity, health issues, the maintenance of public order and peace, the proper coordination in case of emergency situations and so on. Today's critical infrastructures are large-scale sociotechnical systems, comprised of multiple components, involving various stakeholders, technologies, policies and social factors.

Infrastructures are accounted to be critical for several reasons:

• Singularity within the frame of infrastructures of a system or process;

[29] *Rinaldi S. M.* Identifying, understanding, and analyzing critical infrastructure interdependencies IEEE / S. Rinaldi, J. Peerenboom, T. Kelly // Control Systems Magazine. – 2001. – № 21(6), P. 11–25.

• Their vital importance as a material or virtual (net-like) support in the functioning of systems and the unfolding of processes – economic, social, political, informational, military etc.;

• Important, non-replaceable role that they play in the stability, reliability, safety, functionality and especially in the security of systems;

• Increased vulnerability to direct threats, as well as to threats targeting the systems these infrastructures are a part of;

• Special sensitivity in case of variation of the underlying environmental conditions (in a broad sense) and especially in case of sudden changes of the situation.

CIP provides a comprehensive framework for managing the key infrastructures, assets and resources on which we depend at local, national, regional and global levels. Various actors, mostly governmental but increasingly private ones (such as multinational companies), have pursued an independent development of this field, generating solutions of a technical, organizational and strategic nature.

Rapid development of the sector has enhanced our understanding of the depth to which critical infrastructures are interconnected and, therefore, the potential dangers that disruptions (intentional or unintentional, natural or man-made, sudden or gradual) in a single area pose to the entire system-of-systems emerging in modern societies. CIP is based on risk analyses that take into account a comprehensive threat spectrum and prescribes security measures which include all aspects of integral risk management. In the most modern CIP philosophies, a principle of subsidiarity is at work, wherein Operators, Local and National Authorities are responsible for the protection of CI. Finally, proportionality must be maintained in designing protection measures, in order to ensure the best results with the least investment of scarce resources. These protection measures aim at strengthening resilience.

There are numerous models and systems for assessing the interdependencies between CI. One such model recognizes four types of dependency (physical, geographical, informational and logical)[30]. The Romanian National Critical Infrastructure Protection Strategy focuses on a variation of this, where dependencies are physical, logical/informational, inter-regional and inter-sectorial. Another sees infrastructures as being in a production chain, and identifies upstream, downstream and lateral dependencies[31]. Concepts have been developed to assess infrastructure risk, by identifying

[30] *Gheorghe Adrian V.* Critical Infrastructures: Ubiquity of Digitalization and Risks of Interdependent Critical Infrastructures : IRGC-ETH Document / Adrian V. Gheorghe, Markus Schläpfer.– Zürich. – 2004. – June.

[31] *Baker George H.* A Vulnerability Assessment Methodology for Critical Infrastructure Sites / George H. Baker. – 2005. – April [Електронний ресурс]. – Режим доступу: http://works.bepress.com/george_h_baker/2

complexity, survivability, dependability, uncertainty and policies[32]. Criteria for vulnerability have also been identified such as exposure to risk, sensitivity to risk and adaptive capacity to a hazard[33]. These have been expanded upon to include concepts such as resilience, robustness, fragility[34], fragility and antifragility[35] (where the strength of a system increases through exposure to small stressors) and others. The US National Research Council, in its 2009 publication «Sustainable critical infrastructure system – a framework for meeting 21st century imperatives», described a model of interdependency analysis based on a set of five well-developed criteria – physical, functional, security, flexibility and unpredictability[36]. So, research in this field is constantly advancing the state of the art in terms of coming to grips with the inherent complexity of the system-of-systems.

The European Union's Programme for Critical Infrastructure Protection coalesced around initial efforts at codifying strategic thought on European Energy Security, followed by the security of the European transport infrastructure. The resulting Recommendation, Directives, Standards and research imperatives were accompanied by an expansion of EPCIP to include numerous other infrastructures. The table below illustrates both the expansion of the EPCIP, a rough division into components and the fact that critical energy infrastructures stand at the forefront of the infrastructure taxonomy, by virtue of being a primary target of dependence by most other systems.

The Romanian framework for CIP

The Romanian framework for Critical Infrastructure Protection is designed to meet not just its National CI protection mission, but also the European CIP imperative, in a manner that is as compatible as possible with the CIP programs of other EU Member States, especially neighboring ones, while meeting and exceeding the expectations laid out in relevant EU legislation. Romania recognizes the following CI categories, which are roughly analogous to EU categories – energy, transport, ICT, National Security, administration, food, water, health, chemical and nuclear industry, space and research, with finance being the latest addition.

---

[32]*Stapelberg Rudolph.* Infrastructure Systems Interdependencies and Risk Informed Decision Making / Rudolph Stapelberg // Journal of Systemics, Cybernetics and Informatics / International Institute of Informatics and Cybernetics. – 2008. – № 6(5), P. 21–27.

[33]Idem.

[34]*Hokstad Per.* Risk and Interdependencies in Critical Infrastructures / Per Hokstad, Ingrid B. Utne, Jørn Vatn // Springer Series in Reliability Engineering, Springer. – Trondheim (Norway), 2012. – P. 16–18.

[35]*Johnson John.* Antifragility Analysis and Measurement Framework for Systems of Systems / John Johnson, Adrian Gheorghe // International Journal of Disaster Risk Science. – 2013. – № 4 (4). – P. 159–168.

[36]*Sustainable* critical infrastructure system – a framework for meeting 21st century imperatives / D. Nash [et al.] ; National Research Council, The National Academies Press. – 2009.

Table 1

The list of CI Sectors and belonging subsectors

Sector	Service or Product
I. Energy	1. Production of oil and gas, refinery, treatment and storage including pipelines
	2. Production of electric energy
	3. Energy, gas and oil transport
	4. Energy, gas and oil distribution
II. Information and Communication Technology	5. Information and network systems
	6. Command, automation and instrumentation systems
	7. Mobile and land telecommunication services
	8. Navigation and radio communication services
	9. Satellite communication services
	10. Broadcasting services
III. Water Supply	11. Drinking water supply
	12. Water quality control
	13. Dam building and water quantity control
IV. Food Supply	14. Food supply, food safety, security and protection
V. Health	15. Medical support and hospital services
	16. Drugs, serums, vaccines, and pharmaceutical products
	17. Bio laboratories and bio agents
VI. Finance	18. Payment services / related structures
	19. Governmental financial systems
VII. Defence, Public Order, National	20. Country defence, public order and national security
	21. Integrated management of borders
VIII. Administration	22. Government
	23. Armed forces
	24. Administration and services
	25. Emergency services
IX. Transport	26. Road Transport
	27. Railways
	28. Sea, river and ocean transport
	29. Air transport
X. Chemicals and Nuclear Energy	30. Production, processing and storage of chemical and nuclear substances
	31. Dangerous chemical substances pipes
XI. Space	32. Air traffic
	33. Outer Space

A key aspect to remember about Romanian CIP efforts is the paradox of having, on paper, a competitive and well thought out system which is also integrating the state of the art in this field with regards to identifying and designating new CI, while operating under severe resource constraints which undermine the effectiveness of such a system and thereby reduces the ultimate resilience of Romanian CI.

The Romanian CIP system is the product of an internal development which integrates the relevant EU framework, but is mindful of Romanian CI characteristics, its national specificities and its challenging security environment. Romania is not just a passive beneficiary of EU developments in the field, but has also begun to contribute directly to the further development of the EPCIP framework – Romanian experts have worked on the Security Liaison Officer project for use in future European legislation, which codified the attributes, responsibilities, competencies and training for the SLO embedded in corporate or governmental security departments[37] .

Romania can find much in common with Ukraine when it comes to infrastructure and specifics of the security environment. Due to communist development policies, Romania has an imbalance of certain infrastructures (especially heavy industry and energy refining assets), which are not well positioned for sustainable exploitation. The passage of time and a lack of resources for upgrades and maintenance mean that many infrastructures are suffering from various levels of decay and technological obsolescence, leading to a significant potential for spontaneous disruption. In a holistic sense, there is a dangerous imbalance between the stages of development and transition of the Romanian society and economy. Just to give an example from the field of energy, the push towards green solutions at EU levels and the financial incentives associated with such developments have led to a rapid development of a subsidized renewable energy sector which has placed a strain on the Romanian critical energy infrastructure system, through an increased number of intermittent providers of energy, requiring ever more complex grid balancing operations.

Moreover, the challenging security environment of Romania exhibits threats from natural phenomena and increasing regularity of extreme weather patterns, but also significant geopolitical risk, compounded by Romania's participation in antiterrorist coalitions and peacekeeping forces. The recent period has also revealed Romania's security exposure to asymmetric risks, such as deliberate cessation of resource and information flows, the threat of frozen conflicts, trans-border criminal organization activities and threats from human migration patterns. Meanwhile, Romanian secu-

[37]*Security* Liaison Officer Project 2014 : Final Report / European Commission, Directorate-General Home Affairs [Електронний ресурс]. – Режим доступу: http://www.coseritylab.it/News/Voci/2014/6/25_SLO_Project_Final_Conference_files/SLO_FinalReport.pdf

rity, prestige and international goodwill towards it depends also on adequately protecting the regional and international critical infrastructures which transit through its territory, and on which other states are critically dependent, from energy connection to commercial transport corridors.

Below is a graph on the informational and decisional circuit on CI protection, highlighting the role of public authorities, specialized institutions, and the stakeholder who actually operate the Critical Infrastructure. This is a generic model that is also applicable to the Energy Critical Infrastructure subdomain.

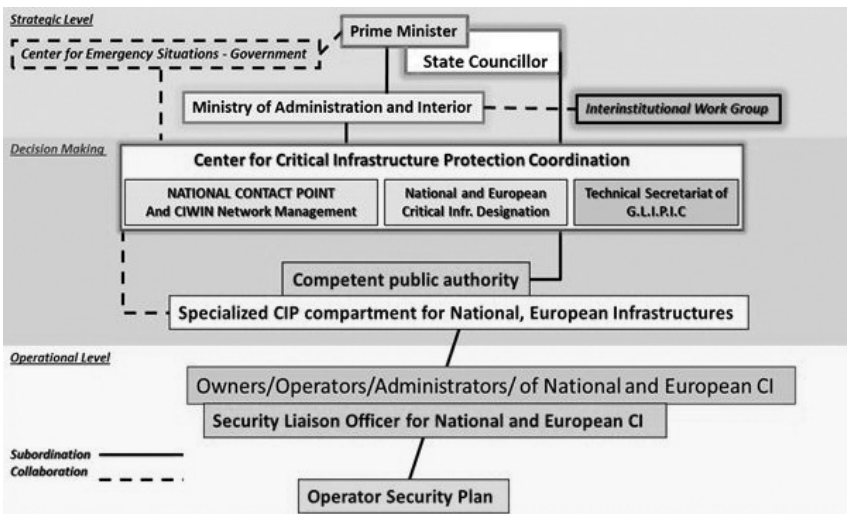

Fig. 1. Simplified layout of Romanian CIP information and decision circuit

A few notable ideas should be taken from the table. The first is the recognition of an abundance of stakeholders, from private and public companies to government agencies and ministries, requiring a connecting agency and authority to provide a holistic view. The second is the presence of elements of European connectivity, to allow for the sharing of information and the coordination with partners in other EU and NATO Member States and in the EU and NATO institutions themselves. The third is the inevitable concentration of a host of functions regarding information gathering, compliance verification and activities coordination in a single body or a few bodies, which themselves become administrative critical infrastructures for the whole process (administration being a recognized EPCIP category). This means that decision makers should be aware of having creates a new disruption point and a source of new risks and vulnerabilities. Resilience, in a

certain sense, is less of a destination and more of a journey and permanent balancing act, where not just the change in environmental factors produces new risks, vulnerabilities and threats, but the actions of security decision makers themselves, in the pursuit of security from known threats.

In Romania, over 1.000 individual infrastructures have been designated as critical and added to a classified list, which entails special responsibilities on the part of the owner/operator/administrator. Central to Romanian and European CIP efforts is the Operator's Security Plan (OPS), which includes identification of vulnerabilities, descriptions of existing or future security measures and procedures, permanent measures and gradual measures to be instituted with each new alert level etc. Within 9 months of the designation of a new CI element, the owner/operator/administrator must develop OPS in line with the applicable legislation (Annex 3 of the Emergency Government Order 98 from 03.11.2010) and present it for approval and then periodic revision and renewal (ever two years, or whenever circumstances warrant it). Here too, European regulations and directives supersede National legislation pending harmonization.

Below is a graph outlining the information and decision flow in case of a generic crisis or an emergency situation. The specifics of the incident, especially regarding geographical concentration of the effects of a crisis, will determine what bodies take which measures. Since critical infrastructure disruptions are prone to triggering cascading disruption events, it is likely that further resources and authorities in other areas will have to be mobilized, as well as sector specific crisis response resources.

Romanian CIP legislative framework

Like that of all EU Member States, the Romanian legislation in these fields must be harmonized with European legislation, while its mechanisms, organizations and competent authorities must be able to function smoothly within the wider EPCIP and its mechanisms, as well as any other CI related initiative that is set into motion. It is interesting to note that Romanian has CI-specific legislation, in addition to security legislation which governs certain aspects of CI security without directly mentioning them. Some of the most important entries into the legislative framework for CIP protection in Romania and, implicitly, for ECI protection, are:

• Emergency Government Ordnance no. 98 of 03.11.2010, regarding the identification, designation and protection of CI (Official Monitor no. 757 from 12.11.2010);

• Government Decision no. 1.110 from 03.11.2010, regarding the components, responsibilities, attributes and organization of the Inter-Institutional Working Group for CIP (Official Monitor no. 757 from 12.11.2010);

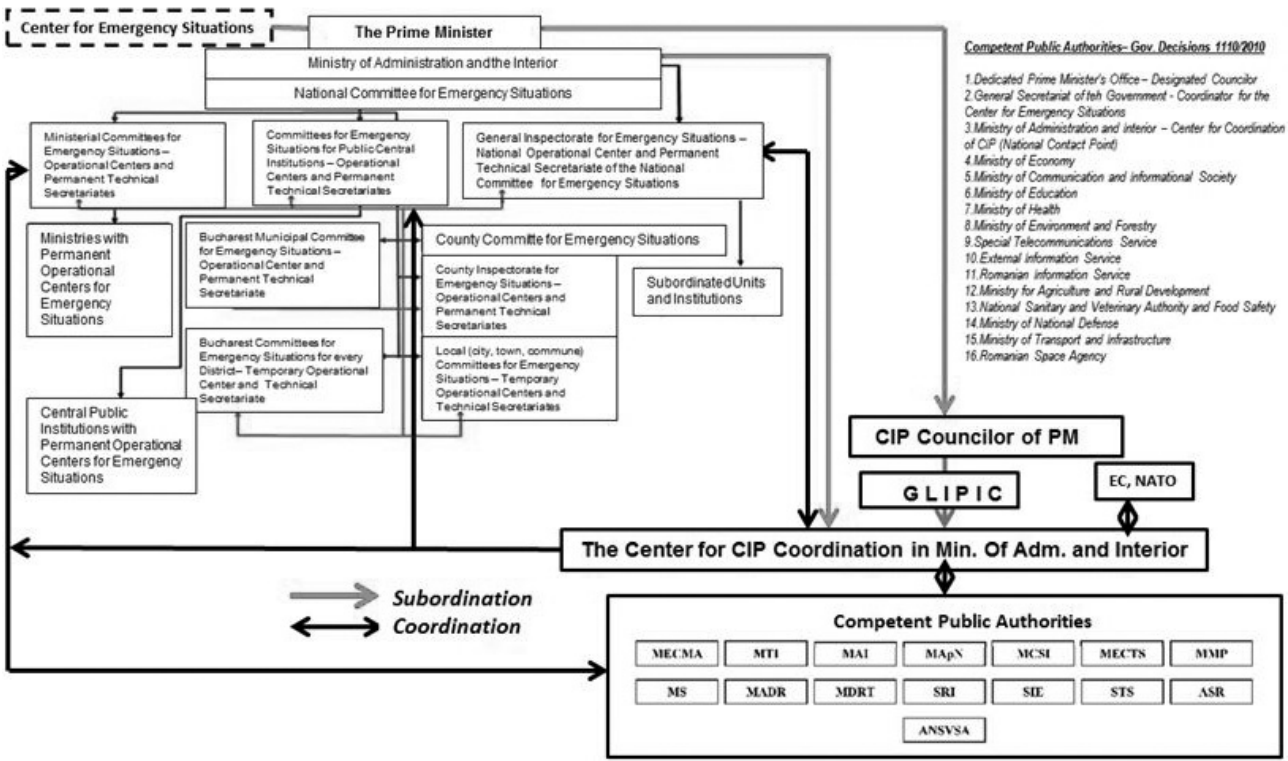

Fig. 2. In depth presentation
of organizational chart for CIP emergency situations

• Law no. 18 from 11.05.2011, for the approval of EGO no. 98 of 03.11.2010, regarding the identification, designation and protection of CI (Official Monitor no. 183 from 16.05.2011 – starting date: 19.05.2011);

• Prime Minister Decision no. 42 from 28.05.2011, regarding the description of the CIP specific Counselor within his own Office (Official Monitor no. 216 from 29.05.2011); and Prime Minister Decision no. 53 from 02.05.2011, regarding the components, responsibilities, attributes and organization of the Inter-Institutional Working Group for CIP, as well as its Regulations for functioning (Official Monitor no. 301 from 02.05.2011);

• Government Decision no. 718 from 31.07.2011, National Strategy for Critical Infrastructure Protection (Official Monitor no. 555 from 04.08.2011);

• Government Decision no. 1154 from 16.11.2011 for the approval of critical thresholds and methodologies for the inter-sectorial criteria which are used to identify National Critical Infrastructures;

• Government Decision no. 1198 from 04.12.2012 regarding the designation of National Critical Infrastructures.

• Other entries establish specific standards for companies in general, that are applicable to critical infrastructures, such as:

• Law no.333/2003 republished in 2014 and Government Decision no.1010/2004 on the protection of persons, valuables, goods and sites;

• Law no.182/2002, Government Decision no.585/2002, Government Decision no.781/2002 which contributed to the protection of classified information and preventing and combating terrorism;

• Government Decision no.547/2005, Law no 481/2004 which established the National Strategy for Civil Protection and further regulated the management of crises and emergency situations;

• Government Decision no.642/2005 which added to the management of crises and emergency situations in general;

• Law no.307/2006, on protecting against fires.

Meanwhile, there have been steady developments in the field of functional European institutions and mechanisms governing CI issues, especially in the field of energy security and critical energy infrastructure security[38]. The Department of Homeland Security quotes a figure of 80–85 % of US critical infrastructures being owned and operated by private companies, though it has not made such a study public for reasons of security[39]. One of the most notable of these is CIWIN (European Critical Infrastructure Warning Information Network), initiated under COM(2008) 676 and functional since 2013.

[38] *Critical* infrastructure and key resources [Електронний ресурс]. – Режим доступу: https://www.ise.gov/mission-partners/critical-infrastructure-and-key-resources

[39] *Hedges Chris.* The Most Brazen Corporate Power Grab in American History / Chris Hedges [Електронний ресурс]. – Режим доступу: http://www.opednews.com/articles/1/The-Most-Brazen-Corporate-by-Chris-Hedges-American-Hypocrisy_Americans-For-Prosperity_Corporate-Citizenship_Corporate-Crime-151107-882.html

The CIWIN network is a protected and public Internet based information and communication system owned by the European Commission, dedicated to facilitating the exchange of information between recognised and authenticated members of the EU Critical Infrastructure Protection community. In Romania, the National Contact Point is the Center for Critical Infrastructure Protection Coordination. Another initiative was the E.R.N.C.I.P. (European Reference Network for Critical Infrastructure Protection) is a platform for information on experimental and testing facilities in Critical Infrastructure Protection research and development.

The Third Energy Package in 2009 established the European Agency for the Cooperation of Energy Regulators (ACER) as a body with final decision capability. At the same time, a number of hybrid organizations were created with varying levels of European input to support the liberalization of European energy markets and aid the smoothing of the regulatory landscape in conjunction with the main actors in the field, including private ones: the Council of European Energy Regulators (CEER), the European Network of Transmission System Operators for Electricity (ENTSO-E), the European Network of Transmission System Operators for Gas (ENTSO-G), the European Regulators' Group for Electricity and Gas (ERGEG) etc.

Case Study – New frontiers in risks – The private and foreign element in Romanian CI

A clear trend that was signaled by American security actors is the growing importance of private entities in CIP, through their ownership of designated CI. The Department of Homeland Security quotes a figure of 80–85 % of US critical infrastructures being owned and operated by private companies, though it has not made such a study public for reasons of security . The situation in the European Union is similar, with estimates of around 70 % of CI being controlled by companies, though each country has its own such profile. There are numerous reasons for this trend to continue, some of which will be cited beneath, but an emerging one is the effect of international free trade treaties or other projects driven by lobbying from special interest groups imposing economic policies in favor of privatizations and allowance, even prioritization, of (foreign) corporate interests. The upcoming Trade in Services Act (TiSA) in the United States is one such development, as could be the Trans-Atlantic Trade and Investment Partnership (TTIP)[40].

[40] *Hedges Chris.* The Most Brazen Corporate Power Grab in American History / Chris Hedges [Електронний ресурс]. – Режим доступу: http://www.opednews.com/articles/1/The-Most-Brazen-Corporate-by-Chris-Hedges-American-Hypocrisy_Americans-For-Prosperity_Corporate-Citizenship_Corporate-Crime-151107-882.html

This presents an interesting challenge. For one, the CI development needs of a society for the provision of critical goods and services is more and more reliant on private capital and private development efforts, especially to avoid malinvestment and find the right investment mix that will ensure sustainability. However, in general, private companies and foreign (state owned) companies view security as a cost affecting their profitability, and are apt to minimize their expenditure in the field, even at the risk of diminishing the goodwill of the host state and incurring losses in case of a negative event. A system-of-systems will only be as strong as its weakest link, meaning that a heterogeneous approach towards security on the part of each system component operator is a recipe for disruption, which is where the role of state authorities as clearing houses of information, enforcers of standards and disseminators of best practices comes into play. There is also the exception, where a very security conscious company improves the security profile of the country it operates in by exceeding local standards of prudence and preparedness.

The Romanian authorities must also contend with a large foreign presence in the CI sectors such as energy and agriculture that will only increase, a result of multiple factors such as the privatization of state assets, the need to attract capital investment from outside the borders, the need for technology transfers, the presence of significant internal resource potential (energy, agriculture) in comparison with the rest of the region and so on. Future infrastructure investment projects, regardless of specifics, will most likely contain an important foreign element providing capital, technology, intermediate financing and possibly also ownership. From the perspective of critical infrastructure protection, the involvement of foreign companies, while beneficial in a strictly economic sense, given Romania's needs, is also a source of concern. While decision makers may eventually consider otherwise, this concern does not yet warrant special restrictions on foreign investment and ownership, which would be problematic from an EU regulatory perspective, but they must be acknowledged by the decision makers and their supporting security specialists. It must also be reflected in the legal and organizational frameworks for Romanian security, in general, and critical infrastructure protection, in particular. Some of these concerns are:

• The possibility of disinvestment and withdrawal from Romania, should underlying economic conditions at home, in Europe or in Romania make continued operations unprofitable or untenable;

• The possibility of insufficient investment in the critical infrastructure affecting the security of said infrastructure and of the wider system-of-systems;

• The foreign companies may have upper management (foreign or Romanian) which is less responsive to the security needs and standards expressed by the competent Romanian authorities, being physically removed from Romania and primarily concerned with respecting legislation in their home country. Moreover, proper communication between the competent authori-

ties and the owners/operators/administrators of critical infrastructures is a critical component of CIP activities which is the concern of the current Romanian push for developing, adopting and enhancing Liaison Security Officer legislation, Operator Security Plan legislation, National Contact Point for European Critical Infrastructure Protection and various security standards;

• The foreign companies may, directly or indirectly, be influenced by third parties with non-profit and non-sector concerns, whose interests may be detrimental to those of Romania. Such means of covert undermining of a state is part of the panoply of hybrid warfare, a concept which has gained significant real world exposure with the geopolitical upheavals of the past few years. Taking the example of the energy sector, there are numerous countries present in Romania – Austria, Hungary, Germany, Kazakhstan, Russia, France, Italy, the Czech Republic, the United States, Azerbaijan, Turkmenistan and soon enough also China, through negotiations for the building of the future Romanian nuclear reactors and of the Rovinari thermal power plant. Some companies perform greenfield investments, while others acquire a stake in an existing Romanian critical energy infrastructure or energy champion, such as the Kazakhstani acquisition of Rompetrol. In the near future, the withdrawal of Italian company ENEL from the Romanian energy market may provide a useful case study for the power such companies have over Romanian energy consumers.

Continuous improvement in CIP efforts is key

Romania must not rest on whatever laurels it has earned, but view its CIP efforts as a continuous effort requiring continuous improvement. As research in the field expands, new avenues of security thinking open up, such as space security and dependence on foreign-owned satellite systems. A few key areas have been identified for improving the Romanian CIP efforts, in addition to the usual calls for allocating more resources for security efforts and realigning outmoded organizations and CIP management tools to new standards. One is the establishment of a better dialogue with civil society stakeholders (think tanks, professional associations, NGOs) to benefit from their accumulated expertise. The SLO project mentioned in a previous section was the result of cooperation with a Romanian professional association of CIP experts, the Romanian Association for the Promotion of Critical Infrastructure and Services Protection, which has partnerships with similar organizations throughout the EU. Such organizations, including Academia and other civil society and business groups, are vital for offering policy research and advisory capabilities, for creating certified training programs for security experts and decision makers and for narrowing the skills and knowledge gap on CIP (and Security in general) present in certain state institutions, where non-experts weigh in on security issues.

Given the characteristics of Romanian CI, it is important to prioritize

not only security of existing infrastructure, but the development of a more robust and resilient infrastructure system-of-systems. Security should be viewed not as a cost, but as an important investment in insuring business continuity and quality of life, especially with the rise of terrorist actions against important infrastructures, not just population concentrations. With proper management and development, it is even possible for security investments to become self-sustaining, by generating innovative and competitive products for a security-as-a-service type of industry. This has been identified as key for the sustainability of security expenditure and for economic growth in the findings of the European Security Research and Innovation Forum[41].

In Romania, private companies, but also state agencies and institutions may contribute to the development of CIP specific models and instruments. One such example is the Military Equipment and Technologies Research Agency (METRA) of the Ministry of Defense, whose research may also be applicable to CIP (sensors, unmanned vehicles, cyberdefense, security procedures and products for NBC defense etc.). The «pipelines» for the research of such institutions to be prototyped and developed into a product for wide dissemination to potential beneficiaries or for export or licensing (generating a profit center and economies of scale which aid in local security efforts) is not very well developed.

Lastly, international cooperation for CIP efforts does not end in Brussels. Other international organizations have shown an interest in CIP, both as a natural extension of their interest in development and security, as well as a way of remaining relevant players in a rapidly evolving security paradigm. NATO, for instance, has been developing CIP policies for Member State Cooperation, especially for energy security and cyber security[42].

Conclusion

Critical Infrastructure Protection has become an invaluable tool for understanding and ensuring the security of a state and the underlying systems necessary for the prosperity of its citizens. Romania is a useful model for Ukraine in creating a CIP framework that not only serves National needs, but also takes into account a responsibility for positive impact on regional security through the safeguarding of regional critical infrastructures. It also underlines the limitations of such a model in the context of resource penury and inconsistencies in infrastructure maintenance and development. More-

[41] *Security* Industry Policy – Action Plan for an innovative and competitive Security Industry : SWD(2012) 233 final [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0417:FIN:EN:PDF

[42] *Good* Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace / Organization for Security and Co-operation in Europe. – 2013 [Електронний ресурс]. – Режим доступу: http://www.osce.org/atu/103500?download=true

over, interesting developments are highlighted, such as the growing importance of private companies as operators/owners/administrators of critical infrastructure and the contradictions inherent in the rising foreign element in the critical infrastructure landscape. Ultimately, a country is only as safe and as prosperous as its infrastructures will allow.

МЕРЕЖА РОЗПОДІЛЕНИХ СИТУАЦІЙНИХ ЦЕНТРІВ ЯК ІНФОРМАЦІЙНО-АНАЛІТИЧНА ТА ОРГАНІЗАЦІЙНА ОСНОВА УПРАВЛІННЯ ЗАХИСТОМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Морозов Анатолій Олексійович,
директор Інституту проблем
математичних машин і систем НАНУ;
Білоконь Володимир Миколайович ІПММС;
Вишневський Віталій В'ячеславович, ІПММС;
Железняк Марк Йосипович, ІПММС

Євроінтеграційні намагання України та нові виклики щодо загроз національній безпеці України змусили урядовців, науковців і представників інших сфер суспільства звернутися до позитивного досвіду управління критичною інфраструктурою, що практикується в Сполучених Штатах і європейських країнах. Створивши дієву систему управління із захисту критичної інфраструктури, зазначені країни вдало протистоять і попереджують терористичні атаки, акти кіберзлочинності, оперативно діють у напрямі ліквідації наслідків надзвичайних ситуацій техногенного та природного характеру тощо. Аналіз масштабних надзвичайних ситуацій, що виникали в Україні та у світі, свідчить про актуальність створення такої системи для нашої держави.

Важливим кроком в опрацюванні наукових основ щодо захисту критичної інфраструктури стала Зелена книга з питань захисту критичної інфраструктури в Україні (*далі* – Зелена книга), до розроблення якої Національний інститут стратегічних досліджень долучив вітчизняних та іноземних спеціалістів. Перші обговорення Зеленої книги засвідчили високий рівень зацікавленості центральних органів виконавчої влади до вивчення позитивного зарубіжного досвіду та усвідомленість необхідності створення аналогічної системи в Україні. Дуже знаково, що в Зеленій книзі запропоновано створити *національний центр* з управління в кризових ситуаціях та захисту критичної інфраструктури, який, зокрема, виконуватиме функцію ситуаційного центру і взаємодіятиме у *мережі ситуаційних центрів*, розподілених між об'єктами критичної інфраструктури та відповідальними держав-

ними установами, і має стати інформаційно-аналітичною й організаційною основою із захисту критичної інфраструктури.

Історія розвитку ситуаційних центрів в Україні сягає минулого століття, коли найбільша катастрофа людської цивілізації – аварія на Чорнобильській АЕС – змусила державних діячів, науковців та інших осіб, задіяних у ліквідації наслідків цієї катастрофи, застосувати (чи не вперше в історії радянського управління) т.зв. ситуаційне управління[43], що здійснювалося в межах діяльності оперативного штабу, створеного на зразок сучасного ситуаційного центру.

Під технологією колективного формування рішень в умовах функціонування ситуаційного центру мається на увазі послідовність людино-машинних процедур (з англ. HMI – *human-machine interface*) взаємодії між особами, що беруть участь у процесі колективного обговорення варіантів рішення, й системою в процесі підготовки та проведення наради[44].

Концептуальні положення ситуаційного управління, розвинені як продовження поступу системного підходу, базуються на ідеї, що наявні методи й управлінські прийоми не можуть бути застосовані з однаковим успіхом у різних ситуаціях, які виникають у діяльності підприємств[45]. Цю тезу з успіхом можна апроксимувати на діяльність держави загалом.

Сучасна зовнішньополітична й соціально-економічна ситуація в Україні формує низку нових викликів, що спричинюють необхідність реформування системи дотримання національної безпеки і оборони та перегляду підходів щодо створення ефективної державної системи кризового реагування на основі методології ситуаційного управління, автоматизації та інформаційного наповнення процесу управління.

До таких викликів належить насамперед анексія Російською Федерацією Криму й частини територій Донецької та Луганської областей. Нинішня зона проведення АТО є об'єктом пильної й постійної уваги рятувальних служб, адже незаконні та самопроголошені «республіки» щодня здійснюють там воєнно-диверсійну й терористичну діяльність, що призводить до загибелі чи травмування людей, знищення чи пошкодження важливих об'єктів критичної інфраструктури, завданню

---

[43]Ситуаційне управління стало несподіваною альтернативою ручному управлінню, яке на той час переважало.

[44]*Морозов А. А.* Ситуационные центры информационные технологии будущего (Новая информационная технология) / А. А. Морозов, В. А. Ященко. – К. : Изд-во СП «Интертехнодрук», 2008. – 332 с.

[45]*Ситуаційні* центри: теорія і практика : зб. статей / За ред. А. О. Морозова, Г. Є. Кузьменко, В. А. Литвинова. К. : Видавництво СП «Інтертехнодрук», 2009. – 346 с.; Полянська А. С. Роль менеджменту знань у ситуаційному управлінні на підприємстві А. С. Полянська // Ефективність функціонування та економічного розвитку підприємства. Стратегія економічного розвитку України. – 2014 р. – № 34.

прямої та непоправної шкоди навколишньому природному середовищу. На жаль, агресія Російської Федерації не вичерпується лише зоною АТО, а загрожує постійною потенційною небезпекою вчинення терористичних актів на всій території України. Готовність об'єктів критичної інфраструктури до попередження та оперативної локалізації несподіваних терористичних атак перевіряється ворожими диверсійними групами, на жаль, майже щодобово.

Ще одним потужним викликом для системи кризового реагування виявилася низка пожеж протягом 2015 р., що набули статусу надзвичайних ситуацій (*далі* – НС) загальнодержавного значення. Прикладом такої НС стала пожежа на базі нафтопродуктів мережі заправок БСРМ у Васильківському районі Київської області, що призвела до загибелі п'яти рятувальників і завдала колосальних економічних збитків і власникам нафтобази, і державі Україна, а також непоправної шкоди здоров'ю населення та навколишньому середовищу. На нашу думку, можна дійти висновків, що вказана пожежа виникла через таке:

• високий рівень корупції і в центральних, і в місцевих органах державної влади (в цьому випадку ГУ ДСНС у Київській області), що призвела до повної відсутності контролю стосовно запобігання порушенням правил протипожежної безпеки на пожежонебезпечних об'єктах;

• злочинне й свідоме порушення правил протипожежної безпеки власниками (орендарями) зазначеної нафтобази з метою отримання якомога більших прибутків та особистого збагачення;

• інформаційна, організаційна, технічна та кадрова неготовність рятувальної служби до оперативної локалізації НС такого масштабу.

Не менш небезпечним викликом для людства є глобальна проблема зміни клімату, свідченням чого є значні лісові пожежі, що виникали протягом останніх трьох років у США, Росії, інших країнах світу і в Україні, а також масштабні загоряння торфу. Збільшення тривалості засушливих фаз протягом літньо-осіннього періоду року, високі температурні показники та інші чинники стали причиною виникнення пожеж, які іноді набували форми стихійного лиха. Однак зміна клімату має й інші форми вираження: люди, а особливо система кризового реагування, мають бути готові до бур, великих злив, катастрофічних паводків на водних об'єктах, підтоплень, ураганів, смерчів тощо, ймовірність яких зростає через зазначені зміни клімату. Підвищення рівня Світового океану та зменшення території суші – це проблема, що стоїть на порозі людської цивілізації та загрожує, зокрема, й українцям.

Крім зазначених викликів, чи не найнебезпечнішим є людський чинник. Війна на сході України, низка воєнних конфліктів на Близькому Сході, загострення зовнішньополітичної ситуації у світі через агресивну поведінку Російської Федерації спричинили значний міграційний потік

біженців і в Україні, й у світі. Інформація зі ЗМІ про щоденні вбивства (загибель чи травмування) в районі АТО, вчинення диверсій в інших регіонах України, вимушене переселення та адаптацію понад мільйона українців до нових умов призводять до звикання та притупляють у людей відчуття небезпеки, що стає причиною байдужості, неуважності та ігнорування правил виробничої та/чи індивідуальної безпеки. Нині перед країнами світу і перед Україною зокрема постала необхідність формування нової психології «безпекової поведінки» і окремої людини, і людства загалом, що передбачає вироблення системи знань, проведення постійних навчань населення щодо правил поведінки в тій чи іншій ситуації, побудованих за принципом давно забутих і, на жаль, втрачених навчань із цивільної оборони, що проводилися за радянських часів, коли СРСР готувався до потенційної ядерної атаки противника. Україна, крім того, повинна інтегруватися у систему спільної європейської безпеки, побудувати надійну системи захисту критичної інфраструктури.

Технологічний розвиток людства змінив наше уявлення про можливості автоматичних інформаційно-аналітичних систем, що стали головним механізмом забезпечення дієвості управління та оцінки його ефективності.

Сучасні ситуаційні центри (*далі* – СЦ) як автоматичні інформаційно-аналітичні системи управління в розвинених країнах призначені для інформаційно-аналітичного забезпечення діяльності контролю сфер національної безпеки, оцінки можливого розвитку подій і підтримки прийняття рішень. Вони мають виявляти потенційні загрози, прогнозувати стан національної безпеки з використанням методів оцінки ризиків у спосіб економіко-математичного, імітаційного, когнітивного та геопросторового моделювання, застосування геоінформаційних технологій просторового прогнозування, моделювання та запобігання виникненню надзвичайних ситуацій, що загрожують об'єктам критичної інфраструктури. Національний ситуаційний центр, створення якого запропоновано в Зеленій книзі як інформаційно-аналітичного та організаційного механізму створення системи захисту критичної інфраструктури, є доцільним та логічним і має розглядатися як осередок розвитку єдиної державної мережі розподілених ситуаційних центрів критичної інфраструктури України.

СЦ як механізм державного управління в Україні вперше згадується в 1994 р., коли Розпорядженням Президента України було започатковано створення СЦ при Президентові України; функції замовника СЦ було покладено на Секретаріат Ради національної безпеки при Президентові України. Однак, крім затвердження концепції створення вказаного центру, в Україні на той час, на жаль, жодних заходів не було вжито: створення СЦ залишилося технічним проектом, реалізацію якого потім було зупинено.

У XXI ст. нові виклики національної безпеки та альтернативи соціально-економічного розвитку на тлі активного використання СЦ економічно розвиненими країнами світу поставили Україну перед необхідністю знову звернути увагу на заснування СЦ. Згідно з Указом Президента України «Про Стратегію сталого розвитку «Україна–2020» від 12 січня 2015 р. № 5/2015 Рада національної безпеки і оборони України має відігравати провідну роль у створенні ефективної державної системи кризового реагування, а формування мережі ситуаційних центрів центральних органів виконавчої влади України планується як основа організаційно-технічної та інформаційно-наукової підтримки її діяльності. Розпорядженням Кабінету Міністрів України від 04 березня 2015 р. № 213 затверджено План заходів з виконання Програми діяльності Кабінету Міністрів України та Стратегії сталого розвитку «Україна–2020» у 2015 р., яким передбачено (див. п. 3 Плану) «Створення ефективної державної системи кризового реагування (мережі ситуаційних центрів центральних органів виконавчої влади) за провідної ролі Ради національної безпеки і оборони України». Зокрема до 30 листопада 2015 р. передбачено розроблення та подання Кабінетові Міністрів України пропозицій щодо концепції створення ефективної державної системи кризового реагування (мережі ситуаційних центрів центральних органів виконавчої влади) та плану заходів щодо реалізації зазначеної концепції[46]. Постановою Кабінету Міністрів України «Про затвердження переліку пріоритетних напрямів наукових досліджень і науково методичних розробок на період до 2015 року» від 07 вересня 2011 р. № 942 створення та організацію роботи СЦ визначено як пріоритетний напрям розвитку наукових досліджень.

На сьогодні в Україні в окремих органах державної влади є кілька центрів та інформаційно-аналітичних систем, що виконують або мали б виконувати ті чи інші функції, дещо схожі на функціональні можливості СЦ. До них варто віднести:

• Головний ситуаційний центр при РНБО України (офіційно відкритий 16 січня 2015 р. у межах проведення Президентом України наради з питань військово-стратегічного планування).

• Антитерористичний центр при Службі безпеки України, що здійснює координацію діяльності суб'єктів боротьби з тероризмом щодо запобігання, попередження та припинення терористичних актів[47];

---

[46]Пропозиції щодо проектів Концепції та Плану заходів підготовлені Міноборони та надіслані до Кабінету Міністрів України (лист від 06.08.2015 № 220/221) та Апарату Ради національної безпеки та оборони України (лист від 10.08.2015 № 220/226).

[47]*Антитерористичний* центр при Службі безпеки України [Електронний ресурс]. – Режим доступу: http://www.sbu.gov.ua/sbu/control/uk/publish/article?art_id=98861&cat_id=101375

• СЦ Головного командного центру Збройних Сил України, призначений для забезпечення ефективної діяльності вищих посадових осіб Збройних Сил України, керівного та оперативного складу центрального апарату Міністерства оборони України та Генерального штабу Збройних Сил України[48];

• Урядова інформаційно-аналітична система з питань надзвичайних ситуацій, що започатковувалася як кризовий центр у складі Центру інформаційних ресурсів Кабінеті Міністрів України, однак, на жаль, процес створення цієї системи не завершено й досі[49].

Необхідність створення та підтримки функціонування відомчих ситуаційних центрів підтверджує досвід галузі ядерної енергетики. Так, НАЕК «Енергоатом» планує запровадити нову систему радіаційного моніторингу РОДОС (*RODOS – Real-time On-line Decision Support System*), що діє в низці країн – членів ЄС, створити Центр прогнозування наслідків радіаційних аварій (включає математичні моделі та бази даних для прогнозування й оцінки наслідків можливих радіаційних аварій, а також планування невідкладних і довгострокових контрзаходів з використанням даних систем радіаційного моніторингу), автоматичну метеорологічну станцію та обчислювальний центр поблизу Запорізької АЕС[50].

Прототип СЦ було створено в Мінприроди як державне підприємство «Центр еколого-експертної аналітики», що певний час виконувало функції інформаційної аналітичної системи з охорони навколишнього природного середовища, однак розвиток вказаної системи було повністю припинено після створення національного геопорталу з охорони заповідних територій[51].

Проект створення ситуаційного центру стратегічного рівня було розроблено в 2012 р. Державним космічним агентством України. Він передбачає створення Інформаційно-аналітичного (ситуаційного) центру при Кабінеті Міністрів України з використанням космічних технологій. Такий центр має стати основою урядової інформаційно-аналітичної системи для підтримки прийняття рішень із використанням геопросторових інформаційних технологій і дистанційного зон-

---

[48]*Морозов А. О.* Шлях від АСУП до ситуаційних центрів / А. О. Морозов, Г. Є. Кузьменко // Математичні машини і системи. – 2008. – № 3.

[49]*Про створення* Урядової інформаційно-аналітичної системи з питань надзвичайних ситуацій : постанова Кабінету Міністрів України від 16 грудня 1999 р. № 2303 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua

[50]*На Запорізькій* АЕС професійне свято відзначили співробітники гідрометеорологічної служби [Електронний ресурс]. – Режим доступу: http://www.energoatom.kiev.ua/ua/press/nngc/40717-na_zaporzkyi_aes_profesyine_svyato_vdznachili_spvrobtniki_gdrometeorologchno_slujbi/

[51]*Система* моніторингу / Національний геопортал [Електронний ресурс]. – Режим доступу: http://menr.gov.ua/index.php/geoportal

дування Землі. Зазначене агентство у 2014 р. поновило свої зусилля щодо започаткування створення Національного ситуаційного центру з названими функціями на базі вже створених технічних і програмних можливостей ситуаційного центру Апарату РНБО України.

Однак перераховані подоби ситуаційних центрів, створені в державних органах України, або не працюють, або працюють не на повну (проектну) потужність.

Здається, що невдачі, які спіткають Україну на шляху запровадження ситуаційного управління та ситуаційних центрів, лежать лише в площині фінансового забезпечення, адже створення технічного та програмного комплексу сучасного ситуаційного центру, націленого на вирішення завдань державного управління, є досить дорогим. Проте, як свідчить досвід використання інформаційних систем в Україні, фінансові аспекти створення таких систем відходять на другий план через неготовність системи державного управління до сучасних методів інформаційно-технічного, комунікативного, візуалізованого та науково-експертного супроводження процесу управління.

Державні установи та організації часто готові на витрати, пов'язані із закупівлею сучасного технічного обладнання та програмного забезпечення спрямованих на створення СЦ, але, на жаль, вони не готові до сталого організаційного забезпечення роботи певного організаційного підрозділу, створеного в межах чинної штатної структури даної установи або ж на засадах аутсорсингу чи аутстафінгу. Дійсно, в умовах жорстких фінансових обмежень і скорочення штатної чисельності державних установ першими, хто розглядається на предмет скорочень, стають співробітники ситуаційних центрів. Адже «керівники» наскільки звикли до ручного управління, що не бачать потреби утримувати необхідну чисельність співробітників СЦ або державне підприємство, створене при певній установі.

Ще гірша ситуація з використанням т.зв. малих експертних груп (*далі* – МЕГ), які є основою для прийняття рішень у межах ситуаційного управління, адже лише експерти можуть визначити оптимальні параметри для прогнозування або моделювання тієї чи іншої ситуації, а також правильно трактувати отримані результати. Використання таких МЕГ є невигідним для установ та організацій з кількох причин:

• формування МЕГ супроводжується досить трудомістким пошуком та визначенням фахової придатності експерта з тих чи інших питань;

• невизначеність фінансового врегулювання роботи таких МЕГ у межах державної установи;

• щодо готовності деяких керівників до альтернативної думки експерта на ситуацію, яка склалася.

Для поліпшення ситуації щодо МЕГ необхідно створити на рівні Кабінету Міністрів України банк даних експертів (науковців) за різними

сферами щодо забезпечення національної безпеки та захисту критичної інфраструктури, а також затвердити на рівні Кабінету Міністрів України положення про порядок залучення експертів (науковців) до роботи МЕГ у межах діяльності державних установ та організацій.

Однак найбільшою проблемою є відсутність в системі національної освіти середньої та вищої ланки викладання елементарних основ з використання сучасних програмних продуктів у практиці господарювання та управління. Більшість державних службовців, що працюють у системі виконавчої влади України, не мають елементарних знань щодо використання інформаційно-аналітичних систем, тому свідомо уникають їх впровадження у повсякденну роботу. Необхідно на базі Національної академії державного управління при Президентові України розробити й запровадити для державних службовців навчальний курс «Упровадження сучасних інформаційно-аналітичних систем та автоматизованих систем управління в практику державного управління». Сучасна реформа у сфері впровадження електронного врядування в Україні має стати мірилом здатності органів державного управління до переходу на вищий рівень управління – ситуаційного управління на основі автоматизованого інформаційно-аналітичного забезпечення.

Усі зазначені проблеми було вирішено в межах створення Головного ситуаційного центру при РНБО України (*далі* – ГСЦ РНБО України), що проектувався за прототипом сучасного СЦ на базі найновішого програмно-технічного забезпечення протягом 2012–2013 рр. Однак і йому притаманні всі названі проблеми щодо організаційного забезпечення та роботи МЕГ.

Разом з тим у межах вказаного СЦ було створено програмно-технічний комплекс, зібрано всі необхідні технічні модулі СЦ, розроблено та впроваджено першу чергу інформаційного, програмного й математичного забезпечення.

Реалізовані на базі ГСЦ РНБО України можливості ситуаційного управління є унікальними на території України і навіть у сучасній формі (реалізовано лише І етап робіт із трьох запланованих) уможливлюють кардинальні зміни в управлінні соціально-економічним розвитком і країни загалом, і її окремих регіонів. Станом на сьогодні в межах цього СЦ реалізовано такі функції: (1) формування інтегрованого сховища даних з питань національної безпеки із диверсифікованих джерел інформації[52], (2) моніторинг та аналіз сфер стану національної безпеки, (3) їх моделювання та прогнозування, (4) підтримка прийняття управлінських рішень у межах аналізу геоінформаційної ситуації, геопросторовий аналіз і картографічне моделювання (5) збір

[52]У систему введено понад 200 джерел інформації загальним обсягом близько 2500 Гбайт, що містять понад 30 млн різноманітних показників.

та оброблення неструктурованої інформації, (6) управління нормативно-довідковою інформацією, (7) автоматична підготовка регламентних звітів та оглядів.

Зазначені переваги роблять СЦ окупним протягом найкоротшого строку його експлуатації, адже він є незамінним під час аналізу експортно-імпортних операцій у межах інтеграції України в ЄС, планування зовнішньоекономічної діяльності держави, моделювання соціально-економічної відбудови та напрацювання концепцій альтернативного економічного розвитку інфраструктури, зокрема Донецької та Луганської областей тощо. СЦ вже зараз дозволяє значно посилити оперативність і достовірність прийняття управлінських рішень у сфері забезпечення обороноздатності України, зокрема оцінки тактико-оперативної обстановки в районі проведення антитерористичної операції.

ГСЦ РНБО України було створено за всіма канонами заснування та організації діяльності ситуаційного центру, наявними в розвинених державах світу. Тому мають місце значні сподівання щодо можливої його трансформації в Національний ситуаційний центр при Президентові України, який би став основою мережі розподілених СЦ, спрямованих на забезпечення національної безпеки та захисту критичної інфраструктури.

Діяльність кожного з названих наявних центрів (систем) передбачає вирішення конкретних відомчих завдань із залученням різноманітних технічних і програмних продуктів, які можуть суттєво відрізнятися від однієї установи до іншої; відсутність уніфікованих методологічних підходів і регламентів взаємодії ускладнює їх об'єднання в єдину мережу. Налагодження ефективної взаємодії та інформаційної їх сумісності на основі єдиних регламентів з метою ефективного використання державних ресурсів, зокрема коштів держаного бюджету, може бути здійсненим лише в межах створення єдиної державної мережі розподілених ситуаційних центрів (*далі* – ЄДМРСЦ).

Створення ЄДМРСЦ відбуватиметься на основі всебічного аналізу інформації, що надходитиме від об'єктів критичної інфраструктури та з урахуванням новітніх досягнень у сфері ситуаційних технологій, спрямованих на вдосконалення стратегічного й регіонального планування, основ забезпечення національної безпеки завдяки суттєвому підвищенню достовірності вхідної інформації, наукової обґрунтованості, прозорості та оперативності процесу формування й виконання завдань державного розвитку. Завдяки впровадженню ЄДМРСЦ прогнозування соціально-економічного, територіально-просторового та інноваційного розвитку держави з використанням імітаційного й математичного моделювання, геопросторових і супутникових даних стане невід'ємним складником державного управління у сфері захисту критичної інфраструктури.

Забезпечення функціонування ЄДМРСЦ у державних органах вимагає комплексного організаційно-технічного підходу та розв'язання завдань щодо міжвідомчої координації та інформаційної взаємодії, розроблення відповідної нормативної бази, організації фінансового, кадрового й експертного супроводження, впровадження сучасного інформаційного і технічного забезпечення.

На сьогодні відсутня державна установа, яка б охоплювала в межах своєї компетенції всі види діяльності об'єктів критичної інфраструктури та забезпечувала б їх захист. Саме тому є доцільним присвоєння ГСЦ РНБО України статусу Національного ситуаційного центру (*далі* – НСЦ) та виведення його на міжвідомчий рівень. Низка міністерств та інших державних установ, що відповідають за захист критичної інфраструктури могли б бути співзасновниками НСЦ і забезпечувати його інформаційне навантаження. Координацію та дотримання єдиних уніфікованих методологічних підходів міг би здійснювати Апарат РНБО України, а штат НСЦ працював би на базі Апарату РНБО України на засадах аутсорсингу.

Вдалим прикладом можливостей використання НСЦ може бути така потенційна надзвичайна ситуація природного характеру, як екстремально високі рівні повеней на каскаді Дніпровських водосховищ і напрацювання сценаріїв реагування на них для потенційно небезпечних об'єктів (*далі* – ПНО), що перебувають у можливій зоні затоплення. Зазначимо, що всі наведені нижче можливості моделювання та геоінформаційної візуалізації повністю адаптовані на геоінформаційній системі ГСЦ РНБО України та можуть бути задіяні негайно.

Так, спеціалістами Інституту проблем математичних машин і систем НАНУ (*далі* – ІПММС, Інститут) на базі власного модельного ситуаційного центру розроблено в географічно розподіленому вигляді візуалізацію засобами ГІС наборів сценарних характеристик наслідків надзвичайних ситуацій поблизу ПНО для населення й забудов. Зазначені сценарні характеристики та приклади візуалізації було встановлено й адаптовано для віддаленої ГІС, у даному випадку для ГІС, встановленої в межах програмного забезпечення СЦ Апарату РНБО України. Спеціалістами надано рекомендації щодо зон впровадження контрзаходів, розрахунки яких проводяться методами математичного моделювання[53] на прикладі природних надзвичайних ситуації – затоплень міської та приміської забудови м. Києва на заплаві р. Дніпро в умовах екстремальних повеней і техногенних надзвичайних ситуацій руйнування греблі Київської ГЕС та радіаційних аварій на Рівненський та Запорізький АЕС. Адже ні в кого не викликає сумнівів, що

[53]Числову модель COASTOX-UN було розроблено спеціалістами ІПММС у 2008 р.

вказані АЕС будуть віднесені до об'єктів критичної інфраструктури України.

Рівень води в районі м. Києва влітку за відсутності паводків визначається підпором води Канівської ГЕС, для якої нормальний підпірний рівень води становить 91,5 м за т.зв. балтійською системою висот (*далі* – БС). У 2004 р. найбагатоводніше водопілля за останні 20 років при максимальній відмітці поблизу ГС»Київ» у 93,5 м (БС) істотних затоплень не викликало. Найбільші повені у ІІ половині ХХ ст. 1970 і 1979 рр. стали причиною значних затоплень в околицях м. Києва, особливо сильним впливом відзначилося водопілля 1970 р., яке затопило частину Подолу, район Корчуватого, острови Труханів і Гідропарк, а також частину сіл Гнідин і Вишеньки Бориспільського району[54]. Дані про найвищі паводки минулих років на р. Дніпро в районі м. Києва представлені в табл.

Таблиця

Фактичні дані про найвищі паводки минулих років на Дніпрі в районі Києва

Рік	Максимальні витрати води, м3/сек.	Максимальний рівень води від нульового гідрологічного посту м. Київ, м	Максимальний рівень води, м (БС)
1931	23100	10,73	97,73
1970	18500	9,80	96,80
1979	10500	8,39	95,39
2004	5100	6,50	93,50

Розрахунки було зроблено для двох сценаріїв – «Екстремальні повені» та «Руйнування дамби Київської ГЕС». Розраховані сценарії затоплень продемонстрували можливість оперативного прогнозування наслідків повеней для будь-якого наступного року й уможливили розрахунки оцінки потенційної ефективності щодо протидії затопленням проектів нового будівництва в річкових заплавах Дніпра та інших річок, а також виявлення зон, що потребують додаткового протиповеневого захисту.

Розраховані сценарії радіаційних аварій на об'єктах критичної інфраструктури продемонстрували можливість оперативного прогнозування наслідків радіаційних аварій та використання ситуаційного моделювання для розрахунку ризиків для населення в зонах впливу українських АЕС у випадках тяжких ядерних аварій з урахуванням

[54] *Бойко В. М.* Особливості формування весняного стоку Дніпра та моделювання зони затоплення у межах м. Києва на основі сучасної гідролого-гідродинамічної моделі / В. М. Бойко, Є. О. Євдін, М. Й. Железняк, П. С. Коломієць, О. О. Іщук // Гідрологія, гідрохімія, гідроекологія : період. наук. зб. – 2012 .– Т. 1(26). – С. 55–63.

географічних особливостей місцевості, розподілу населення та метеорологічної обстановки в період аварії[55].

Висновки

Ситуаційні центри як інформаційні технології майбутнього є унікальним шансом для розвитку системи державного управління в Україні та запровадження ситуаційного управління. СЦ є системою управління, що поєднує людський інтелект, інформаційні технології, сучасні програмно-технічні засоби й засоби моделювання в процесі прийняття державними органами рішень стосовно розв'язання комплексних проблем у всіх сферах державної діяльності в цілому, й зокрема з метою захисту критичної інфраструктури, дотримання національних інтересів і забезпечення національної безпеки.

Розбудова СЦ в окремих органах державної влади України та їх об'єднання в єдину розподілену мережу надасть змогу налагодити надсучасний інформаційний обмін та взаємодію між осередками такої мережі. Отже, вагомим чинником, що сприятиме суттєвому поліпшенню державного управління може стати ефективне функціонування Єдиної державної мережі розподілених ситуаційних центрів (*далі* – ЄДМРСЦ) у державних органах, які діють за єдиними регламентами взаємодії, що спрямовується, зокрема, на здійснення достовірної оцінки наявних та ймовірних загроз і ризиків у сферах національної безпеки та соціально-економічного розвитку.

З огляду на значний досвід ІПММС у сфері розроблення автоматизованих інформаційних систем, зокрема й ГСЦ РНБО України, на Національний інститут стратегічних досліджень необхідно покласти функції центру науково-технічного супроводження процесу подальшого вдосконалення ГСЦ РНБО України й доручити розроблення концепції та уніфікованої методології створення єдиної державної мережі ситуаційних центрів державних органів влади України, що працюють під керівництвом ГСЦ РНБО України.

Напрацювання науковців ІПММС демонструють необхідність різнорівневого втручання в межах ситуаційного управління захистом об'єктів критичної інфраструктури. Адже очевидно, що повінь сценарію 1931 р. потребує оперативного втручання не лише Мінприроди, ДСНС, Держводагентства тощо, а й РНБО України і Президента України. Ситуаційне управління щодо запобігання надзвичайних ситуацій на об'єктах критичної інфраструктури та ліквідації їх на-

[55]*Бойко О. В.* Прогнозування розповсюдження радіонуклідів в річкових басейнах в системі підтримки прийняття рішень під час радіаційних аварій JRODOS / О. В. Бойко, М. Й. Железняк // Екологічна безпека та природокористування ; зб. наук. пр. / Київ. нац. ун-т буд-ва і архіт., НАН України, Ін-т телекомунікацій і глобального інформ. простору. – К. – 2012. – Вип. 9. – С. 27–39.

слідків для повеней за сценарієм 2004 р. буде врегульовано в межах спільної робочої групи Мінприроди, ДСНС, Держводагентства. Однак у випадку і того, й іншого сценарію, обов'язковим має бути попереднє прогнозне ситуаційне моделювання, геоінформаційна візуалізація можливих затоплень, розрахунок можливих ризиків для населення та об'єктів критичної інфраструктури з метою забезпечення високого рівня готовності на випадок підтвердження прогнозованого сценарію надзвичайної ситуації природного характеру.

Вказані програмно-технічні засоби ситуаційного управління мають бути реалізовані не лише в СЦ Апарату РНБО України, а й у зазначених центральних органах виконавчої влади, та на основі єдиних методологічних підходів об'єднані в мережу розподілених ситуаційних центрів, яку в подальшому необхідно трансформувати в ЄДМРСЦ.

ЗАГРОЗИ КРИТИЧНІЙ ІНФРАСТРУКТУРІ ТА ОЦІНКА ЇЇ «КРИТИЧНОСТІ»

Бобро Дмитро Геннадійович,
відділ енергетичної та техногенної безпеки НІСД

Проблеми забезпечення безпеки критичної інфраструктури

Ключовими у цьому дослідженні є терміни «критична інфраструктура» та «загроза».

В Україні термін «критична інфраструктура» (*далі* – КІ) неодноразово використовувався в нормативно-правових документах, зокрема й у новій редакції Стратегії національної безпеки України, затвердженій Указом Президента України від 26 травня 2015 року №287/2015, проте його визначення досі відсутнє в чинному законодавстві.

Сучасне поняття критичної інфраструктури включає в себе ті об'єкти та системи, які є життєво важливими для безпеки держави, суспільства та людини. У першу чергу, це системи життєзабезпечення – передусім транспорт, енерго-, водо- та теплопостачання, основні системи зв'язку і комунікацій, а також банківсько-фінансовий сектор. Дестабілізація, не кажучи вже про колапс цих систем, обертається важкими або навіть катастрофічними наслідками для суспільства, економіки і держави. Сюди можна додати також особливо небезпечні виробництва, такі як хімічне, біологічне і атомне, аварії на яких (викликані будь-якими причинами) теж можуть обернутися катастрофічними наслідками.

Проект Зеленої книги з питань захисту критичної інфраструктури в Україні, розроблений Національним інститутом стратегічних дослід-

жень у 2015 році, пропонує наступне визначення: «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 та забезпечення національної безпеки». Надалі під терміном «критична інфраструктура» розумітимуть саме таке його визначення.

Іншим ключовим терміном у цій роботі є термін «загроза».

Законом України «Про основи національної безпеки України» надане наступне визначення загроз національній безпеці: «наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України». Надалі під загрозами в контексті захисту критичної інфраструктури будемо розуміти наявні та потенційно можливі явища та чинники, що створюють небезпеку сталому функціонуванню об'єктів критичної інфраструктури та можуть призвести до негативних наслідків.

Як правило, у національних законодавствах загрози КІ розділяють на три основні категорії, виходячи з характеру їх походження: надзвичайні ситуації природного характеру; надзвичайні ситуації техногенного характеру; зловмисні дії, зокрема, зловмисні дії груп або окремих осіб, таких як терористи, злочинці і диверсанти.

Особливо небезпечними вважаються комбіновані загрози та загрози, реалізація яких може призвести до катастрофічних і різноманітних каскадних ефектів («ефекту доміно») внаслідок взаємозалежності елементів КІ.

Слід зазначити, що після подій 11 вересня 2001 року безпека критичної інфраструктури у США була зосереджена на захисті від загроз терористичного типу (*one hazard strategy*). Але через нездатність ефективно протистояти наслідкам ураганів Катріна і Ріта у 2005 році уряд США повернувся до стратегії захисту від двох або декількох найбільш ймовірних загроз, включаючи природні лиха і техногенні аварії (*multiple hazard strategy*)[56].

У провідних країнах світу виходять із необхідності забезпечення захисту критичної інфраструктури від усіх видів загроз (*all hazards approach*).

Говорячи про захист КІ, виникає питання не лише «від чого захищатися», але й який елемент чи «що захищати»: фізичний (об'єкт) чи функціональний (функцію)? Слід зазначити, що захист цих елементів КІ має відмінності, оскільки щодо об'єктів він спрямований, у пер-

[56]*Степанова Е.* Терроризм как угроза критической инфраструктуре / Е. Степанова [Електронний ресурс]. – Режим доступу: http://www.estepanova.net/Stepanova2010SvMysl.pdf

шу чергу, на зниження загрози (запобігання та упередження загроз), зниження вразливості об'єктів, а також мінімізацію наслідків, а щодо функцій – ще й на скоріше їх відновлення. Не слід забувати й про захист такого елементу КІ, як люди (персонал, аварійні команди тощо).

Щодо захисту об'єктів КІ, то розуміння неможливості забезпечити однаково високий рівень захисту всієї критичної інфраструктури від всіх можливих загроз призвів до розвитку підходу, який зосереджений на вибірковому захисті конкретного об'єкта КІ від обмеженого набору відомих та відносно прогнозованих загроз з наданням пріоритету тій або іншій інфраструктурі залежно від ступеня її «критичності». Проте постає питання, як оцінити цей ступінь?

І тут слід перейти від загроз до ризиків. Саме ризик може виступити головною мірою «критичності» КІ.

Довідково: існують різні визначення «ризику»: ймовірні частота та величина втрат (збитків) – метод оцінки кіберзагроз *FAIR*; поєднання ймовірності нанесення шкоди внаслідок того, що визначена загроза реалізована через наявність вразливості – державний російський стандарт ГОСТ Р 52448-2005.

У нашій оцінці будемо виходити з розуміння ризику як кількісно виражених очікуваних наслідків (втрат/збитків), що отримані упродовж певного періоду часу для певного типу суб'єктів (держави, суспільства і людей, бізнесу), та які можуть мати місце в результаті реалізації певного набору загроз.

Досвід реагування на надзвичайні ситуації природного та техногенного характеру, аналіз їх наслідків дозволяють достатньо легко провести ранжування КІ відносно цих загроз інфраструктурі за їх ризиками (ймовірними наслідками). Аналогічно, може бути проведене ранжування КІ і за терористичною загрозою. Проте далеко не вся критична для суспільства і держави інфраструктура представляє інтерес для терористів як мішень, удар по якій може забезпечити їм досягнення власних цілей.

Тероризм як загроза критичній інфраструктурі

Хоча теракти та інші зловмисні атаки входять до числа серйозних загроз критичній інфраструктурі, вони не є настільки поширеними, як технологічні аварії або природні катаклізми.

Так, за даними *Global Terrorism Database*[57], критична інфраструктура ставала об'єктом нападу для порівняно невеликої кількості терактів (до 10-15 %), у той час, як основна кількість терактів була направлена проти людей та військових об'єктів. Такий вибір терористів можна по-

[57]*Global* Terrorism Database [Електронний ресурс]. – Режим доступу: http://www.start.umd.edu/gtd/

яснити тим, що більшість ключових об'єктів КІ, удари по яких можуть мати дійсно катастрофічні наслідки, зовсім не є незахищеними мішенями, у той час як скупчення людей у громадських місцях вразливі до терористичних атак.

Проте терористичні загрози КІ навряд чи можна вважати перебільшеними через наступні чинники:

• по-перше, разом із прямою дією на КІ, цілеспрямований вибір терористів, направлений на завдання максимальної шкоди, зазвичай тягне за собою вторинні наслідки – каскад порушень в роботі інших об'єктів КІ;

• по-друге, на відміну від терактів ні технологічні, ні природні катаклізми не є заздалегідь спланованими спробами домогтися максимальної дії на суспільство, спеціально розрахованого на його дестабілізацію; для терористів же цей вторинний ефект дестабілізації навіть важливіший;

• по-третє, терористи можуть намагатися отримати контроль над ключовими вузлами інфраструктури, що надалі призведе до ще більшої дестабілізації;

• по-четверте, зростаюче розмаїття вразливих об'єктів КІ суттєво ускладнює визначення найбільш імовірних мішеней для терактів та проведення відповідних антитерористичних заходів;

• по-п'яте, заходи з посилення безпеки на одних об'єктах КІ (наприклад, на АЕС), водночас підвищують ймовірність переключення терористів на інші, менш захищені та більш вразливі цілі (наприклад, на ТЕЦ, що за умов низьких температур може дати не менш значущий дестабілізуючий ефект).

Загалом же для усвідомлення привабливості об'єктів КІ для терористичних атак слід розуміти, чим мотивуються терористи у своєму виборі об'єкта для нападу. Ці мотиви можуть бути дуже різними. Найбільш характерними з них є:

• намагання викликати масову загибель людей;

• нанести економічну (екологічну, суспільно-політичну тощо) шкоду;

• викликати тривогу та невпевненість;

• отримати широкий суспільно-політичний резонанс.

Загалом, все це зводиться до намірів терористів щодо суспільно-політичної дестабілізації та можливості впливу на ситуацію в окремій країні чи групі країн. Саме дестабілізуючий ефект і є головною метою та мірилом успіху теракту.

Що ж до об'єктів терористичних атак на КІ, то найбільш вразливою мішенню є перетинання місць масового скупчення людей з інфраструктурою загального використання, перш за все транспортною, системами водо-, тепло- та енергопостачання, телекомунікаціями, а в зоні конфліктів – об'єктами енергетичної інфраструктури, перш за все

тими, які мають велику протяжність (трубопроводи, газові та нафтові родовища, лінії електропередач тощо), повноцінний фізичний захист яких дуже важко забезпечити.

Можна констатувати, що в умовах ведення гібридної війни в Україні одну із найбільших загроз для критичної інфраструктури представляють дії диверсійних груп терористичних організацій. Саме тому оцінка терористичної загрози є важливим елементом розбудови системи захисту КІ.

Аналіз загроз зловмисних дій щодо об'єктів КІ (методичний підхід)

Загрози для об'єктів КІ оцінюються із застосуванням різноманітних методик, в основі яких лежить загальна методологія оцінки ризиків[58]. Для оцінки досягнення цілей захисту цих об'єктів можна застосовувати детерміністичні та імовірнісні методи, а також їхнє сполучення, що, наприклад, передбачено рекомендаціями МАГАТЕ[59] та нормативно-правовими актами України стосовно захисту ядерних матеріалів та ядерних установок. Аналогічні підходи передбачені й у США[60].

Враховуючи те, що прояв загроз несанкціонованих дій можна розглядати як випадкову і нечасту подію, для кількісної оцінки загроз можна застосовувати ймовірнісні методи, розуміючи поняття ризику як кількісної міри реалізації загроз для держави загалом та окремим об'єктам КІ зокрема.

Сукупний ризик як кількісна міра загрози для держави. Для виключення різночитань далі ризик r_i від i-тої події $a_i(\tau)$визначимо як добуток частоти реалізації окремої події, що здійснилася за проміжок часу τ, на наслідки l_i від цієї події:

$$r_i = a_i(\tau)\, l_i \qquad (1)$$

Щодо терористичної загрози конкретизуємо формулу 1, представивши частоту у виді двох множників:

$$a_i(\tau) = b_i(\tau)p_{i,} \qquad (2)$$

де $b_i(\tau)$ – оцінка частоти прояву намірів порушників щодо об'єктів фізичного захисту;

p_i – імовірність досягнення цілей порушників за умови прояву намірів, тобто частка від усіх протиправних дій, які привели до наслідків l_i.

---

[58] *Risk* assessment methodologies for critical infrastructure protection. Part I: a state of the art / G.Giannopoulos, R.Filippini, M. Schimmer. – Luxembourg: Joint Research Centre of Institute for the Protection and Security of the Citizen, 2012. – 70 p.

[59] *INSAG*-25 [Електронний ресурс]. – Режим доступу: http://www-pub.iaea.org/MTCD/publications/PDF/Pub1499r_web.pdf

[60] *Physical* protection of plants and materials (10 CFR part 73), U.S. NRC, 8.10.2003.

Як видно з формули (2), якщо наслідки виражені в одних одиницях виміру для всіх розглянутих подій, то можливе підсумовування ризиків за всіма подіями. Тоді для *k*-об'єкта ризик R_k можна виразити у виді суми:

$$R_k = \sum_{i=1}^{i=I(k)} b_{ik}(\tau) p_{ik} l_{ik} \qquad (3)$$

де підсумовування ведеться за всіма загрозами для об'єкта k обсягом $I(k)$.

Ризик для держави, що має K об'єктів, є:

$$R = \sum_{k=1}^{k=K} R_k \qquad (4)$$

Зробимо кілька зауважень щодо застосування оцінок ризиків.

Визначення частот подій

На рівні держави необхідно застосовувати загальне поняття проектної загрози, яка конкретизує властивості та характеристики потенційних внутрішніх і/або зовнішніх порушників та обумовлює вимоги до системи фізичного захисту.

При визначенні ризику використовується оцінка частоти прояву намірів порушників щодо конкретного об'єкта. Якщо для K об'єктів у державі за час τ зафіксовано $N_i(\tau)$ намірів вчинити i-ту дію, то оцінка середньої частоти $b_i(\tau)$ може бути визначена за формулою:

$$b_i(\tau) = \frac{N_i(\tau) K_{li}}{K\tau} \qquad (5)$$

де $K_{li} \geq 1$ – оцінений коефіцієнт пропуску i-того типу подій.

Розмірність величини $b_i(\tau)$ може бути прийнята 1/(рік·об'єкт). Ця розмірність застосовується в нормативних документах і часто невірно називається імовірністю[61].

Відзначимо, що проміжок часу τ, з одного боку, має бути доволі великим для того, щоб статистична похибка оцінки зводилася до мінімуму за рахунок збільшення числа подій і, з другого боку, обмеженим періодом, у якому не відбувалося істотних змін у рівні терористичної загрози.

Безумовно, що не всі загрози можуть характеризуватися за співвідношенням (5), у якому $N_i(\tau) \geq 1$. Для не втілених у державі подій можуть застосовуватися методи порівняння з аналогами іноземних країн, експертні оцінки тощо. Зокрема, якщо імовірність подій розподілена за за-

[61] *Гордон Б. Г.* Об использовании понятия риска в различных отраслях промышленности / Б. Г. Гордон // Вестник Госатомнадзора России. – 2003. – № 1

коном Пуассона і за період спостережень τ над *K* об'єктами не відбулося жодної події, то можна стверджувати, що така реалізація можлива з довірчою імовірністю 0,95, якщо прийняти $b_i(\tau) \approx 0{,}05/(\tau K)$ (див. роботу[62]).

Оцінка імовірності досягнення цілей порушників

Виходячи з прийнятих підходів, імовірність досягнення цілей порушників можна представити в наступному виді:

$$pi = (1 - P_{Ii} P_{Ni}), \tag{6}$$

де P_{Ii} – імовірність своєчасного виявлення (перехоплення) порушників;
P_{Ni} – імовірність нейтралізації порушників.

Наслідки загроз

Розглядаючи наслідки реалізованих загроз, слід відмітити, що у деяких національних законодавствах вже при визначенні терміну «критична інфраструктура» акцент зміщено з об'єкта КІ на функції та послуги, якими вони забезпечують. Однак наслідки полягають не лише в припиненні чи обмеженні функцій із життєзабезпечення, які надаються об'єктами КІ, але стосуються й інших втрат, які можна звести у наступні основні групи: шкода здоров'ю і життю людей; економічний збиток (розмір економічних втрат); екологічні наслідки (вплив на населення та навколишнє природне середовище); політичні збитки (суспільна тривога, втрата впевненості в дієздатності влади, зниження авторитету влади, порушення державного управління тощо); нацбезпека (зниження боєздатності збройних сил тощо). При цьому для кожної категорії втрат є своя шкала важкості наслідків.

Звернемося далі до розгляду розмірності втрат (наслідків). Для можливості обліку втрат різного характеру в одній функції ризику можна використовувати нормовані втрати; тобто замість абсолютної величини втрат вводяться відносні втрати, які визначаються для кожної групи подій з однаковою розмірністю втрат:

$$l_{0i} = \frac{l_i}{l_{max}} \tag{7}$$

де l_{max} – втрати від реалізації події з максимальним збитком.

Довідково: *подібний підхід використовується при оцінці втрат від подій, пов'язаних з ядерними матеріалами (шкала нормованих втрат від 0,1 для незначних кількостей ядерного матеріалу до 1,0 для ядерного вибухового пристрою)*[63].

---

[62] *Клемин А.И.* Инженерные вероятностные расчеты при проектировании ядерных реакторов / А. И. Клемин. – М. : Атомиздат, 1973.

[63] *Рекомендации* курса обучения методам физической защиты, SNL, 2001 г.

Такий підхід не виключає застосування експертної оцінки втрат для кожної події. Та інтегрованим показником втрат найбільш об'єктивно виступають людські та/чи економічні втрати. Подібний підхід використовується при класифікації надзвичайних ситуацій в Україні, де основними чинниками для визначення рівня НС виступає масштаб НС, кількість людей, які постраждали або загинули, та обсяги збитків[64]. Аналогічний підхід на директивному рівні закріплений і в ЄС[65].

Не вдаючись до числових розрахунків, можна сказати, що ризик терористичного нападу на об'єкт КІ буде тим більшим, чим більша його вразливість щодо конкретної загрози і чим важчі наслідки у випадку реалізації загрози.

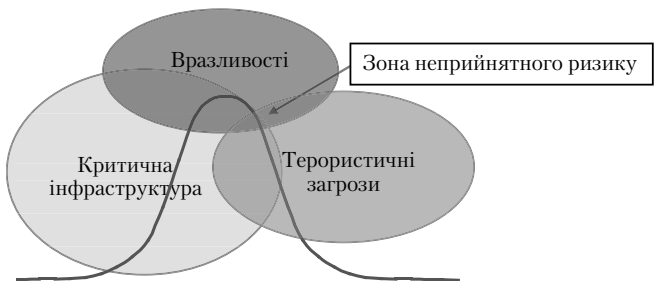

Рис.1. Візуальне представлення зони неприйнятного ризику для КІ держави

Фактор невизначеності у процесі оцінки терористичних загроз. Слід зазначити, що наведений «класичний» методологічний підхід до оцінки терористичних загроз та ризиків не завжди є таким, що може бути реалізованим на практиці. При цьому, якщо для певних категорій подій можна отримати їхні ймовірнісні характеристики (точніше, частоти подій, які можна вирахувати за даними, що зберігаються у вже згаданій базі даних *Global Terrorism Database*[66] чи базі даних американської неурядової неприбуткової дослідної організації *RAND*[67], а щодо кібератак, наприклад, у Депозитарії безпекових інцидентів у промисловості[68]), то для

[64]*Про затвердження* Порядку класифікації надзвичайних ситуацій за їх рівнем : постанова Кабінету Міністрів України від 24.032004 р. № 368 [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/368-2004-%D0%BF

[65]*On the identification* and designation of European critical infrastructures and the assessment of the need to improve their protection : council Directive 2008/114/EC [Електронний ресурс]. – Режим доступу: http://eurlex.europa.eu

[66]*Global* Terrorism Database [Електронний ресурс]. – Режим доступу: http://www.start.umd.edu/gtd/

[67]*RAND* Database of Worldwide Terrorism Incidents[Електронний ресурс]. – Режим доступу: http://www.rand.org/nsrd/projects/terrorism-incidents.html

[68]*The Repository* of Industrial Security Incidents [Електронний ресурс]. – Режим доступу: http://www.risidata.com/

інших подій можна зробити лише припущення щодо їх частоти. Тобто, для процесу оцінки терористичних ризиків характерна суттєва невизначеність, найбільший внесок в яку дає етап оцінки терористичної загрози.

Дійсно, якщо для оцінки наслідків терористичних актів можуть бути використані вже розроблені моделі та розрахунки для природних та техногенних надзвичайних ситуацій, то для оцінки загроз це зробити неможливо, адже вона базується на інформації про цілі, мотиви та можливості терористів. І якщо можливості та тактика дій терористів ще можуть бути більш-менш адекватно передбачені, то який об'єкт КІ стане ціллю – оцінити можна дуже приблизно[69].

Слід зазначити, що пошуку об'єктивної складової щодо визначення терористичної загрози завжди приділялася підвищена увага. Однією з таких об'єктивних складових можна вважати привабливість об'єкта КІ, яка залежить від його значущості та доступності. Зокрема, спроба кількісно оцінити привабливість об'єкта КІ для терористів та визначити методологічні підходи щодо ранжування об'єктів за терористичною загрозою була зроблена в роботі[70].

Фактично результати подібних досліджень свідчать, що складова у формулі (2) – $b_i(\tau)$ (оцінка частоти прояву намірів порушників щодо об'єктів фізичного захисту) не може бути коректно розрахована на основі статистичних даних за формулою (5), оскільки її складові не є незалежними, а похідними від доступності (вразливості) та значущості об'єкта (масштабів наслідків у розрізі досягнення суспільно-політичної дестабілізації). Загалом це може призводити до помилок в оцінці терористичних загроз і, відповідно, до системної недо- або переоцінки загроз.

Мапа оцінки терористичних ризиків і загроз. Слід зазначити, що галузі-лідери у сфері оцінки загроз і ризиків (фізична ядерна безпека та авіаційна безпека, кібербезпека) використовують методологічно схожі підходи. Розглянемо їх детальніше.

Авіаційна безпека

У глобальній заяві Міжнародної організації цивільної авіації (ІКАО від *англ. ICAO – International Civil Aviation Organization*) про контекст ризику[71] наводиться опис картини ризику для авіаційної без-

---

[69]*Henry H.* Willis...[et al.], «Estimating Terrorism Risk», 2005, RAND Corporation, Santa-Monica, CA, U.S.

[70]*Радаев Н., Бочков А.* Оценка террористической угрозы для объекта [Електронний ресурс]. – Режим доступу: http://mx1.algoritm.org/arch/77/77_3.pdf

[71]*Глобальное* заявление ИКАО о контексте риска (RCS) [Електронний ресурс]. – Режим доступу: http://www.icao.int/Meetings/avsecconf/Documents/Risk%20Context%20Statement/Risk%20Context%20Statement%20-%20Abridged%20Version.Published.RU.pdf

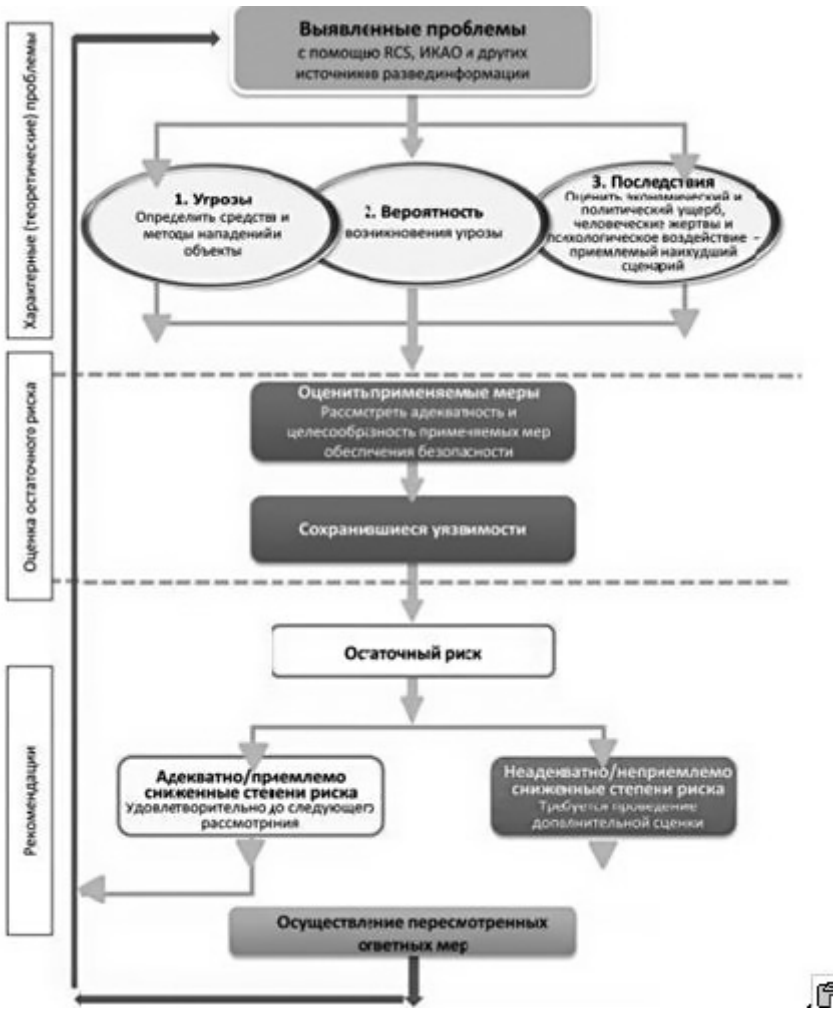

Рис. 2. Мапа процесу оцінки «авіаційних» ризиків

пеки. На основі методики, розробленої Робочою групою із загроз та ризиків (*WGTR*) Групи експертів ІКАО з авіаційної безпеки (*AVSEC*), представлена мапа процесу оцінки ризику, яка включає виявлення характерних проблем, оцінку залишкового ризику та підготовку рекомендацій. Оцінка ризику – це процес, у ході якого ризики оцінюються шляхом визначення: 1) загрози для конкретного об'єкта, а також засо-

бів та методів можливого нападу, 2) ймовірності виникнення загрози, 3) наслідків нападу, 4) вразливостей та 5) залишкового ризику. Узагальнена мапа процесу аналізу «авіаційних» ризиків наведена на рис. 2.

Кібербезпека

У сфері ІТ розроблена та широко впроваджується низка методик оцінки загроз та ризиків, зокрема:

• Методологія оцінки ризиків Національного Інституту Стандартів та Технологій США (*National Institute of Standards and Technology – NIST*);

• Методологія аналізу факторів ризиків інформаційних технологій (*Factor Analysis of Information Risk – FAIR*);

• Методологія пропорційного аналізу ризиків (*MESARI*);

• Метод оцінки операційно критичних загроз, активів та вразливостей (*Operationally critical threats, assets and vulnerability evaluation – OCTAVE*);

• Методологія аналізу інформаційних ризиків Міжнародного Форуму з інформаційної безпеки (*Information Risk Analysis Methodology – IRAM*).

Всі ці методики зводяться до оцінки активів, загроз цим активам, оцінки вразливості активів та можливих наслідків, а також розробки та впровадження контрзаходів.

Фізична ядерна безпека

Відповідно до рекомендацій МАГАТЕ в Україні розроблена та діє система фізичного захисту ядерних установок та ядерних матеріалів. Узагальнена мапа процесу аналізу «ядерних» ризиків наведена на рис. 3.

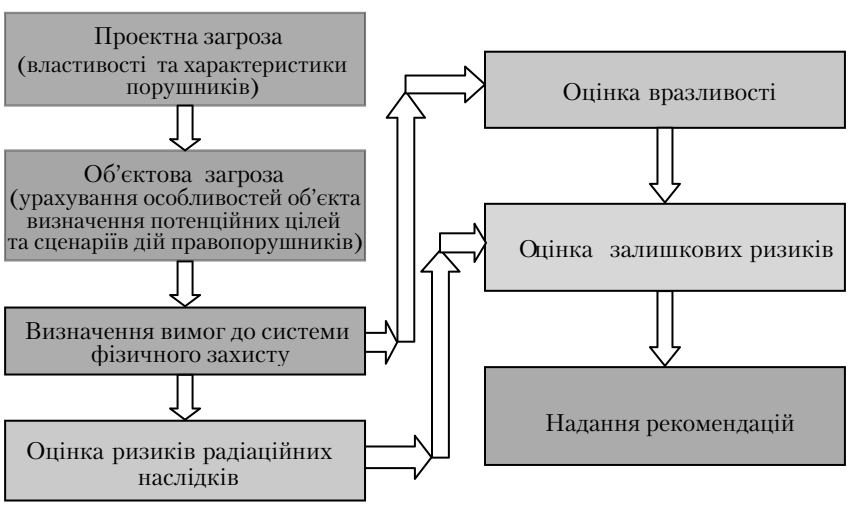

Рис. 3. Узагальнена мапа процесу аналізу «ядерних» ризиків

Методики HAZOP та HAZAN. Серед інших методик, що використовуються для аналізу ризиків, слід згадати методики HAZOP (*HAZard and Operability study* – Аналіз небезпек і експлуатаційної надійності) і *HAZAN* (*HAZard Analyses*). Узагальнена мапа процесу аналізу ризиків за методикою *HAZAN* наведена на рис. 4.

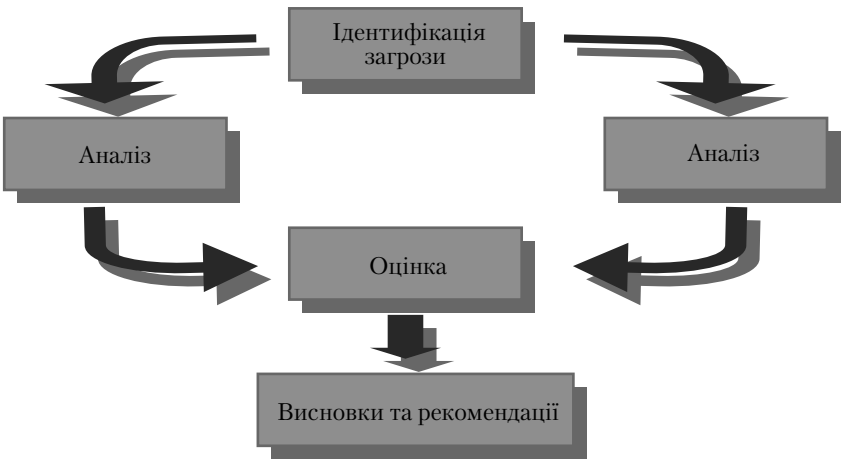

Рис. 4. Методика аналізу ризиків *HAZAN*

Загальний підхід до оцінки ризиків та захисту КІ

Загальний підхід до оцінки ризиків об'єктів КІ включає:

• ідентифікацію та класифікацію загроз, оцінку частоти кожної загрози;

• оцінку вразливостей (до кожного типу подій/атак),

• оцінку наслідків (для обґрунтованого найгіршого сценарію).

При цьому потрібне врахування численних взаємозалежностей КІ[72].

Загалом все це укладається в поняття «моделі загроз», яка включає:

• опис можливих загроз КІ, їх джерел, засобів, що використовуються, методів реалізації (для терористичної загрози – «модель порушника»);

• опис об'єктів, придатних для реалізації загроз, вразливостей цих об'єктів до загроз, що аналізуються;

• опис можливих втрат, масштабу потенційної шкоди.

Слід зазначити, що таке моделювання ризику на системному рівні сприяє не лише ідентифікації потенційних небезпек (у т.ч. відмов обладнання), але й більш глибокому розумінню устрою та функціону-

[72]*Lewis T.G.* Critical infrastructure protection in homeland security: defending a networked nation / T.G. Lewis // John Wiley & Sons, Inc., 2006. – 474 p.

вання об'єкта/системи КІ, виявленню «слабких ланок» у системі, загалом адекватному ранжуванню ризиків.

Слід враховувати, що достовірно кількісно оцінити терористичну загрозу конкретному об'єкту КІ у більшості випадків неможливо. Проте на основі розвідувальної інформації, історичного аналізу та експертних оцінок можна адекватно якісно її оцінити. Саме так оцінюються ризики авіаційній безпеці, коли ймовірність загрози та вразливість об'єкта оцінюють за 5-бальною шкалою від «НИЗЬКОЇ» до «ВИСОКОЇ», а наслідки – від «НЕЗНАЧНИХ» до «ЗНАЧНИХ».

Подібний підхід використовується в оцінці загроз кібербезпеці[73]. Приклад оцінки ризику на основі методики *FAIR* в залежності від вразливості об'єкта КІ та рівня (частоти) загрози для середнього рівня наслідків, наведений на рис. 5.

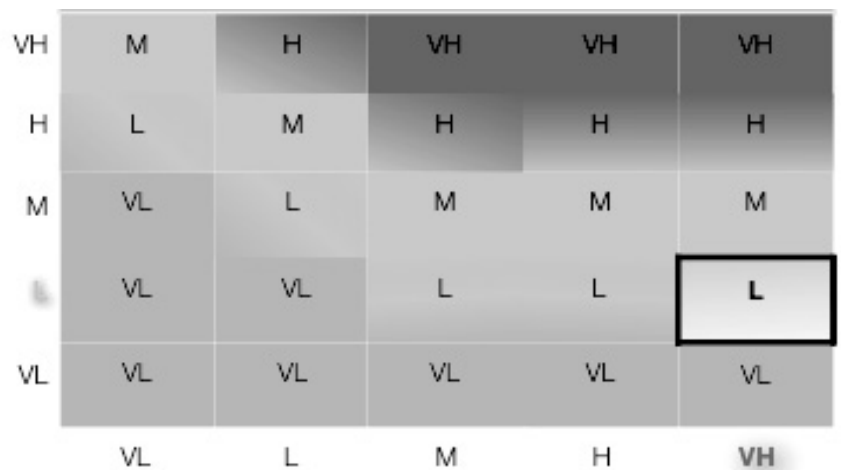

Рис. 5. Приклад оцінки ризику за методикою *FAIR*

Як свідчать результати використання методу Дельфі, у разі залучення до експертної оцінки компетентних у справі людей, отримана усереднена оцінка буде точною не менше, ніж на 80 %. При цьому, якщо провести декілька раундів оцінки, попередньо ознайомивши експертів з результатами попередніх раундів, то достовірність оцінки буде ще вищою.

Водночас якісна експертна оцінка вимагає чіткого розуміння експертами усіх термінів, що використовуються, та процесів, що аналізу-

[73] *Jack A. Jones* An Introduction to Factor Analysis of Information Risk (FAIR) [Електронний ресурс]. – Режим доступу: http://riskmanagementinsight.com/media/documents/FAIR_Introduction.pdf

ються, обґрунтування та розуміння шкал, що застосовуються для оцінки загроз, вразливостей та наслідків. При цьому найбільшу похибку дає не різниця у кваліфікації експертів та можливість впливу одних експертів на інших, а психологія сприйняття ризику. Так, люди (і експерти тут не є виключенням) перебільшують одні ризики та недооцінюють інші, зокрема:

• люди перебільшують ризики, що загрожують їм особисто (або їх дітям), які справляють глибоке враження, широко обговорюються, відбуваються рідко (наприклад, авіакатастрофи), несуть мало зрозумілу дію (наприклад, для більшості людей – радіація), нові та незнайомі, неочікувані тощо;

• люди недооцінюють ризики, що не привертають увагу, є звичними, повсякденними, загрожують іншим, не загрожують безпосередньо, не викликають морального неприйняття, широко не обговорюються тощо.

Водночас ризики, які мали місце в житті експерта (особливо недавно чи були пов'язані зі смертельною небезпекою), для нього часто мають більшу вагу, ніж ті, з якими він ніколи не зіштовхувався. А звідси виникає його зашореність та налаштованість на боротьбу з минулими типами загроз, ніж здатність передбачити їх нові типи.

Іншим проблемним питанням є адекватна оцінка експертами обсягів витрат, які знадобляться для нейтралізації ризиків.

У будь-якому разі слід пам'ятати, що оцінка ризику – це «моментальний знімок», який має регулярно переглядатися.

Результатом подібної узагальненої експертної оцінки ризиків та загроз КІ, наприклад у США, є визначення 5-и ступенів готовності: червона (вища), помаранчева (висока), жовта (підвищена), блакитна (можлива) та зелена (низька).

Виходячи з розуміння основних складових ризику, можна визначити й основні шляхи управління ризиками КІ:

• зниження рівня загроз (наприклад, перехопленням порушників до завдання ними удару, посилення охорони кордонів тощо);

• зниження вразливості об'єкта КІ (створення системи фізичного захисту, яка здатна протистояти правопорушникам);

• мінімізація можливої шкоди (захист населення тощо);

• підвищення стійкості об'єкта (забезпечення технічної надійності та можливості якнайшвидшого відновлення функцій КІ).

Фактично, з одного боку, потрібно закрити вікно вразливості – адаптувати систему фізичного захисту об'єктів КІ до чинних загроз (рис. 6.), а з другого – на державному рівні мати розвинену систему запобігання і реагування на надзвичайні ситуації та передбачити заходи з відновлення функцій цих об'єктів (у т.ч. за рахунок резервування та диверсифікації).

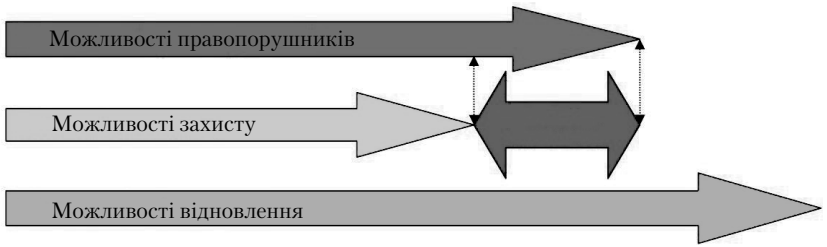

Рис. 6. Вікно вразливості об'єкта КІ щодо чинних загроз

При цьому слід враховувати, що головна проблема полягає у встановленні реалістичного балансу між плануванням заходів, спрямованих на зменшення ризиків КІ, та доступними для їх реалізації ресурсами. Інколи доцільніше концентруватися на можливості відновлення втрачених функцій за рахунок диверсифікації, ніж намагатися створити з об'єкта КІ «неприступну фортецю».

Саме з погляду управління ризиками та встановлення адекватного балансу між заходами із захисту КІ та наявними ресурсами всю інфраструктуру можна розбити на чотири групи, перші три з яких охоплять ту інфраструктуру, що розцінюється як критична за наслідками її впливу на життєзабезпечення через втрату/пошкодження або аварії, викликані будь-якими чинниками: природними або техногенними НС, та/або зловмисними діями:

1 група – великі об'єкти інфраструктури, заходи з відновлення яких вимагають значних ресурсів та часу, на яких має бути створена адекватна загрозам система фізичного захисту (наприклад, АЕС); відповідальність за захист цієї КІ має консолідовано нести держава та оператори (рис. 7);

2 група – об'єкти інфраструктури, на яких потрібно реалізувати як заходи з фізичного захисту, так і передбачити можливість скорішого відновлення функцій за рахунок диверсифікації та резервів (наприклад, крупні нафтобази, підземні сховища газу, мостові переходи тощо); відповідальність за захист цієї КІ має нести держава та оператори на основі державно-приватного партнерства;

3 група – об'єкти інфраструктури, на яких основним способом захисту є забезпечення скорішого відновлення функцій за рахунок диверсифікації та резервів (наприклад, теплові електроцентралі тощо); відповідальність за захист цієї КІ в першу чергу мають нести оператори, а держава мусить забезпечити наявність умов для диверсифікації та резервування;

4 група – об'єкти інфраструктури, які не відносяться до критичної, безпосередній захист яких є відповідальністю суто оператора.

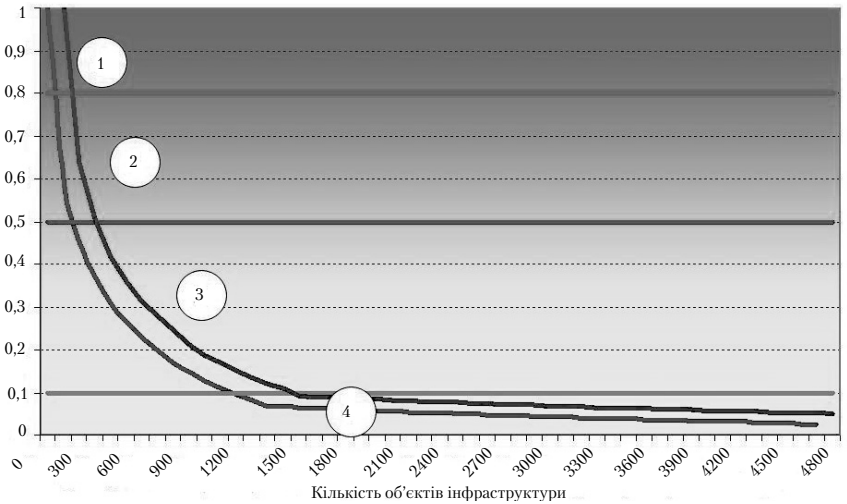

Рис. 7. Розподіл об'єктів інфраструктури за їх критичною важливістю

Довідково: *у США остаточний список об'єктів, які розглядалися як критичні на національному рівні, містив 1700 позицій з бази даних, в яку було внесено близько 33 тис. об'єктів. Для кожного з них були проведені оцінки ризиків, що стало основою для підготовки планів із захисту КІ в США*[74].

Захист КІ в Україні

У державі функціонують Єдина державна система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків, Єдина державна система запобігання і реагування на надзвичайні ситуації техногенного та природного характеру, що трансформована у Єдину державну систему цивільного захисту населення і територій, Державна система фізичного захисту (остання стосується лише питань використання ядерної енергії).

Якщо розглянути функції цих держаних систем, то стане зрозуміло, де саме вони перетинаються. Повертаючись до категорій загроз (надзвичайні ситуації природного та техногенного характеру, зловмисні дії), очевидно, що система цивільного захисту, яка опікується захистом населення та територій від негативних наслідків НС, подоланням їх наслідків (зона 1 на рис. 8) хоча і діє по всій країні, проте із захистом

[74] *Critical* infrastructure and key assets: definition and identification. – Congressional research service, RL32631, October, 2004.

критичної інфраструктури пересікається лише частково (зони 4 та 7 на рис. 8), оскільки не опікується питаннями стійкості об'єктів КІ та можливістю скорішого відновлення функцій КІ; аналогічно система антитерористичного захисту, яка опікується захистом особи, держави і суспільства від тероризму (зона 2 на рис. 8), включно із системою фізичного захисту через ті ж причини із захистом критичної інфраструктури пересікається лише частково (зони 5 та 7 на рис.8).

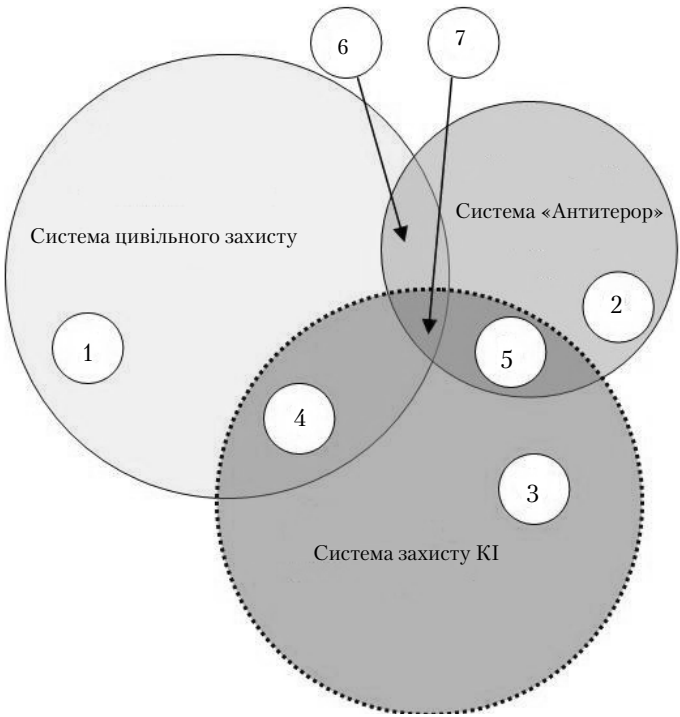

Рис. 8

Метою системи захисту КІ має стати гарантування спроможності інфраструктури виконувати передбачені функції, а запобігання шкоди населенню й довкіллю від настання надзвичайних ситуацій повинно лишатися головним завданням системи цивільного захисту; завдання боротьби з тероризмом – головним завданням державної системи запобігання, реагування і припинення терористичних актів і мінімізації їх наслідків.

При цьому заходи із захисту КІ будуть адекватними лише в контексті загального підвищення стійкості (*resilience*) КІ до будь-яких впливів, незалежно від їх походження. Тобто, йдеться не лише про

спроможність «витримати удар», але й про здатність швидкого відновлення функцій. Фактично потрібно створити систему, яка поєднує застосування глибоко ешелонованого захисту (*defense-in-depth*), фізичного і технологічного, з достатньою забезпеченістю резервними потужностями та ресурсами, їх диверсифікованістю. При цьому, якщо для окремих об'єктів КІ (зони 5 та 7 на рис. 8) наголос має бути зроблений на заходах з фізичного захисту (наприклад, в ядерній енергетиці), то для інших об'єктів (зона 4 на рис. 8) – на забезпеченні технічної стійкості та надійності (наприклад, системи берегоукріплення, протипаводкові системи), а загалом для об'єктів КІ (зона 3 на рис. 8) – на забезпеченні загальної стійкості КІ, її диверсифікації та резервуванні (наприклад, енерго-, тепло- та водопостачання, системи телекомунікації, побудовані за мережевим принципом «від багатьох до багатьох», тощо), розбудові КІ на основі мережевого принципу децентралізації.

Що роблять держави світу на цьому напрямі?

• Розробляють нормативну базу та регулярно її переглядають.

• Визначають координуючий орган (наприклад, у США це Департамент (міністерство) внутрішньої безпеки – *The Department of Homeland Security* (МВБ), до складу якого увійшли 22 федеральних агентства та відомства[75]).

• Розробляють методологічні підходи, формують перелік КІ, оцінюють загрози й ризики КІ, розробляють плани реагування, регулярно оцінюють їх ефективність (наприклад, у США цим опікується Національний центр аналізу та імітаційного моделювання інфраструктури МВБ).

Цікавим є підхід для ранжування об'єктів військово-промислового комплексу у США – модель визначення пріоритетності (*The Asset Prioritization Model*)[76]. Усі об'єкти оцінюються за 16-ма факторами, яким присвоєні вагові коефіцієнти від 16 до 1, з діапазоном оцінок «важливості» об'єкта від 1 до 3 (інколи 5), та розраховується сумарний індекс їх «ризикованості». Ці чинники враховують вплив на великосерійні програми виробництва, бойові можливості (значущість продукції), фінансові можливості компанії, економічну живучість, можливості відновлення, кількість населення, що проживає поряд, супутні втрати від враження речовинами, які використовувалися при атаці, та інші. Цікавим є й те, що у 2007 році найбільш критичними визнані об'єкти, на яких виконуються великосерійні програми виробництва

[75]*Цыгичко В.Н.* Обеспечение безопасности критических инфраструктур в США (аналитический обзор) / В.Н.Цыгичко, Г.Л.Смолян, Д.С.Черешкин„// Труды ИСА РАН.– 2006, т. 27.

[76]*Баранник А.* Организация обеспечения безопасности критической инфраструктуры в США / А. Баранник, С. Клементьев // Зарубежное военное обозрение. – 2009. – № 8. – С.3–10.

для ВПК, хоча раніше такими об'єктами вважалися ті, які мають найбільший вплив на сучасні бойові можливості.

- Забезпечують підготовку кваліфікованих кадрів у сфері захисту КІ.
- Організовують обмін інформацією та кращими практиками.
- Розвивають державно-приватне партнерство.

Проект Зеленої книги з питань захисту критичної інфраструктури в Україні, розроблений Національним інститутом стратегічних досліджень у 2015 році, можна вважати першим системним кроком на шляху розбудови в Україні системи захисту КІ.

Висновки та рекомендації

1. Застосування методів оцінки ризиків на державному рівні дозволить мати кількісні, а для терористичних загроз – адекватні якісні оцінки очікуваної небезпеки у випадках реалізації загроз критичній інфраструктурі. Це дасть можливість одержати необхідний баланс між вимогами забезпечення захисту КІ і наявних ресурсів – зокрема визначити пріоритетність захисту об'єктів, вимоги до систем фізичного захисту, до резервування тощо.

2. На основі проведеного аналізу логічною є розбудова системи захисту критичної інфраструктури за двома напрямами, а саме: системи аналізу ризиків, рівня загроз та вразливості КІ та системи реагування на можливе припинення критичною інфраструктурою виконання своїх функцій.

Фактично має йтися про створення системи захисту КІ, яка поєднує застосування глибоко ешелонованого захисту (як фізичного, так і технологічного) ключових об'єктів з достатньою забезпеченістю інфраструктури резервними потужностями та ресурсами, їх диверсифікованістю, що дозволить у разі реалізації загроз критичній інфраструктурі швидко відновити втрачені функції із життєзабезпечення. Роль держави у розбудові системи захисту КІ полягає у створенні «правил гри», формуванні культури управління ризиками на основі спільних зусиль громадян, суспільства, бізнесу та держави.

ОЦІНКА ГЕОЛОГІЧНИХ ЗАГРОЗ ДЛЯ БЕЗПЕКИ ФУНКЦІОНУВАННЯ МАГІСТРАЛЬНИХ ГАЗОПРОВОДІВ В УКРАЇНІ

ІВАНЮТА Сергій Петрович,
головний консультант, НІСД

З огляду на постійне зростання потреб у виробництві та споживанні природного газу, безпечне й безперебійне функціонування системи магістральних газопроводів має стратегічне значення не лише для

багатьох галузей економіки та життєдіяльності населення країни, а й для національної безпеки держави.

Українська газотранспортна система є однією з найпотужніших у світі. Її пропускна спроможність на вході сягає 287,7 млрд м^3/рік, на виході в напрямку європейських країн – 151,4 млрд м^3/рік. ГТС України тісно пов'язана із системами газогонів сусідніх держав – Російської Федерації, Білорусі, Польщі, Румунії, Молдови, Угорщини, Словаччини, й через них інтегрована в загальноєвропейську газову мережу[77]. Довжина магістральних газопроводів української ГТС та їх відгалужень становить 38,6 тис. км. ГТС налічує 1 458 газорозподільних станцій.

Транзитне транспортування газу територією України в 2014 р. зменшилося майже на 25 %, з 86,1 млрд м^3 у 2013 р. до 62,2 млрд м^3 у 2014 р. Через скорочення попиту на внутрішньому ринку[78] суттєво зменшився і обсяг транспортування газу українським споживачам. У 2014 р. він становив близько 40 млрд м^3.

Зазначені чинники додатково посилюються тим, що протягом останніх 20 років на значній частині території України відбувається регіональна активізація екзогенних геологічних процесів (*далі* – ЕГП) при комплексній дії техногенних і природних чинників, що призводить до збільшення кількості надзвичайних ситуацій (*далі* – НС) різного характеру з негативними наслідками для населення та навколишнього середовища[79]. При цьому найбільшу загрозу для життєдіяльності населення та господарських об'єктів при випереджальному розвитку регіонального підтоплення земель становлять зниження міцності та просідання лесових ґрунтів, формування техногенних водоносних горизонтів у промислово-міських агломераціях, активізація карстово-суфозійних процесів.

Небезпека від цих процесів значно зростає в місцях дислокації потенційно небезпечних об'єктів, що відрізняються підвищеною чутливістю до зниження інженерно-геологічної стійкості техногенно-геологічних систем (*далі* – ТГС) «техногенний об'єкт-геологічне середовище»[80]. В умовах порушення рівноваги ТГС активізація ЕГП на території промислових майданчиків, залізничних колій, нафто-,

[77] *Річний* звіт НАК «Нафтогаз України» за 2014 рік [Електронний ресурс]. – Режим доступу: http://naftogaz-europe.com/ua

[78] *Річний* звіт НАК «Нафтогаз України» за 2014 рік [Електронний ресурс]. – Режим доступу: http://naftogaz-europe.com/ua

[79] *Національна* доповідь про стан техногенної та природної безпеки в Україні у 2006 р. – К. : ДП «Чорнобильінтерінформ», 2007. – 236 с.

[80] *Yakovlev Y. A.* The geological aspects of environmental systems monitoring the geological medium of Ukraine : Technical Report 21/ Y. A. Yakovlev ; UNESCO Regional Office for Science and Technology for Europe. – 1995 – P. 184–191.; *Биченок М. М.* Про вплив екзогенних геологічних процесів на рівень техногенних ризиків життєдіяльності / М. М. Биченок, С. П. Іванюта, Є. О. Яковлєв : зб. наук. пр. Українського державного геологорозвідувального інституту. – К. : УкрДГРІ, 2006. – № 1. – С. 85–91.

газопроводів тощо може спричинити виникнення НС переважно інженерно-геологічного походження зі значними негативними наслідками для життєдіяльності населення та об'єктів господарювання, що перебувають у зонах впливу цих об'єктів, або функціонування яких безпосередньо пов'язане з ними. Зазначені чинники зумовлюють необхідність уточнення змін інженерно-геологічних умов та підвищення рівня безпеки функціонування об'єктів критичної інфраструктури, зокрема газопроводів, нафтопроводів, а також уточнення прогнозу рівня загроз для них з боку ЕГП, оскільки площинний характер вияву цих процесів може викликати додаткові деформації відповідальних конструктивних елементів і призводити до аварійних відмов обладнання[81].

Оцінка геологічних загроз для безпеки функціонування магістральних газопроводів. Останніми роками підтоплення території України має прогресуючий характер і стійку тенденцією до активізації на регіональному рівні з постійним збільшенням площ підтоплення[82]. За даними МНС і Державної геологічної служби Мінприроди України найнесприятливіші умови з підтоплення територій склалися, насамперед, у південних і східних регіонах, де середній приріст підтоплення становить до 300 км^2/рік. За наявними даними, з 1982 р. відбулося подвоєння площ земель на регіональному рівні та у промислово-міських агломераціях.

Також варто звернути увагу на закономірний зв'язок між розвитком підтоплення земель та активізацією внаслідок цього більшості небезпечних ЕГП. Якщо регіональне підтоплення протягом останніх років розвивається в достатньо сталому просторово-часовому режимі (подвоєння площ підтоплення протягом 20–25 років), то активізація в його зонах більшості небезпечних ЕГП має ймовірнісно-ритмічний характер із зростанням кількості виявів переважно в роки з підвищеним рівнем опадів (3–4, 7–13, 26–34 років). Потрібно також зауважити, що найбільш комплексного впливу підтоплення зазнають території в межах міст і селищ України, загальна площа яких складає близько 3 % площі території держави, але в них зосереджено до 70 % населення, що суттєво підвищує (до 10–100 разів) вплив підтоплення на безпеку життєдіяльності.

За даними Державної геологічної служби та МНС України, на 38 % території держави поширені породи, в яких можуть відбуватися процеси

---

[81] *Биченок М. М.* Про комплексне оцінювання ризиків життєдіяльності у потенційно небезпечних регіонах / М. М. Биченок, С. П. Іванюта, Є. О. Яковлєв // Екологія і Ресурси: Зб. наук. пр. Інституту проблем національної безпеки. – К. : ІПНБ, 2007. – № 17. – С. 33–41.

[82] *Регіональні* інженерно-геологічні умови території України : інформ. бюл. / М. Г. Демчишин, Л. М. Климчик, Л. М. Красноок [та ін.] ; гол. ред. Є. О. Яковлєв. – К. : ДІГФ «Геоінформ» Держгеолслужби Мінприроди, 1997. – Вип. 1. – 92 с.

і природного, і техногенно активізованого карстоутворення, а на 24 % території карст може безпосередньо впливати на господарську діяльність[83].

За даними МНС і Державної геологічної служби України, за допомогою ГІС-технологій здійснено просторову оцінку актуальних геологічних загроз стосовно частки довжини магістральних газопроводів на потенційно небезпечних територіях. Результати оцінки свідчать, що на територіях імовірного вияву карсту розміщено до 59,1 % довжини газопроводів, на територіях імовірного вияву підтоплення – до 21,5 %, на територіях імовірного вияву зсувів – до 13 % довжини магістральних газопроводів. Більш докладну інформацію щодо загроз ЕГП для магістральних газопроводів на території адміністративних областей України наведено в таблиці.

Аналіз таблиці дозволяє виявити найнебезпечніші регіони стосовно частки довжини газопроводів, що перебувають під загрозою підтоплення й карсту, а також здійснити ранжирування адміністративних областей України за цими критеріями.

Отримані дані свідчать, що найбільша загроза від підтоплення для магістральних газопроводів за критерієм частки їх довжини існує на території Чернігівської, Чернівецької, Волинської, Полтавської областей, оскільки понад 50 % довжини газопроводів у них розташовано на територіях імовірного вияву підтоплення. Крім того, на території Чернігівської області газопроводи майже по всій довжині перебувають у зонах можливої активізації підтоплення.

Аналіз карстових загроз для магістральних газопроводів на рівні адміністративних областей України свідчить, що в більшості з них (14) понад 60 % довжини газопроводів перебувають на територіях можливого вияву карсту. Найбільша небезпека від карстових загроз для магістральних газопроводів існує насамперед на території Чернівецької, Волинської, Миколаївської, Луганської, Рівненської, Тернопільської, Донецької, Харківської, Львівської областей, у яких понад 80 % довжини газопроводів проходять потенційно небезпечними територіями.

Висновки

Забезпечення безпеки функціонування об'єктів критичної інфраструктури, зокрема магістральних газопроводів, є досить важливим і складним завданням, практичне вирішення якого потребує виявлення та оцінки найбільш імовірних загроз для розроблення адекватних захисних і попереджувальних заходів. Поміж таких загроз суттєве значення мають небезпечні ЕГП, насамперед підтоплення та карст.

---

[83] *Рудько Г.И.* Оползни и другие геодинамические процессы горноскладчатых областей Украины (Крым, Карпаты) / Г. И. Рудько, И. Ф. Ерыш. – К. : «Задруга», 2006. – 623 с.

Таблиця

Загрози від ЕГП для безпеки функціонування магістральних газопроводів в адміністративних областях України

Адміністративні області	Площа, тис. км^2	Ураженість території, тис. км^2		Частка довжини газопроводів на уражених територіях, %	
		карст	підтоплення	карст	підтоплення
АР Крим	27,0	13,2	4,43	72,8	21,4
Вінницька	26,2	5,4	0,054	15,3	0,0
Волинська	20,2	17,4	13,91	100,0	80,1
Дніпропетровська	31,9	7,1	7,3	38,6	22,9
Донецька	26,5	18,5	7,67	92,3	18,5
Житомирська	29,9	0,0	20,13	0,0	0,0
Закарпатська	12,8	0,8	3,02	0,0	43,6
Запорізька	27,2	7,5	3,2	0,0	0,0
Івано-Франківська	13,9	5,0	0,008	68,0	0,0
Київська	28,9	0,0	8,1	0,0	20,0
Кіровоградська	24,6	0,4	0,142	0,0	9,3
Луганська	26,7	26,6	0,164	100,0	2,1
Львівська	21,8	12,7	0,218	83,0	8,3
Миколаївська	24,6	17,4	10,672	100,0	24,5
Одеська	33,3	5,3	9,975	73,4	16,5
Полтавська	28,8	0,3	8,5	76,8	56,2
Рівненська	20,1	16,1	12,8	100,0	0,0
Сумська	23,8	10,0	0,423	7,4	3,0
Тернопільська	13,8	13,1	0,0	93,5	0,0
Харківська	31,4	10,8	3,02	85,0	14,4
Херсонська	28,5	15,2	7,79	31,5	45,4
Хмельницька	20,6	13,5	0,014	42,2	0,0
Черкаська	20,9	0,0	0,08	0,0	14,2
Чернівецька	8,1	3,8	0,4	100,0	80,6
Чернігівська	31,9	4,2	4,4	66,4	100,0
Загалом	**603,4**	**227,8**	**126,42**	**59,1**	**21,5**

Останні дослідження МНС і Державної геологічної служби України свідчать про значне зростання техногенних навантажень на верхню зону геологічного середовища, регіональний розвиток зсувних і карстових процесів, а також про випереджальний характер розвитку підтоплення в деяких регіонах держави.

На тлі техногенних змін геологічного середовища та впливу глобальних змін клімату відбувається збільшення навантажень на відповідальні конструктивні елементи ЛЕП і газопроводів. Вказані чинники значно підсилюються додатковими технічними, спричиненими закриттям шахт, а також підтопленням міст і селищ у південних та східних областях України. З огляду на площинний характер розвитку ЕГП, в таких умовах особливо уразливими стають потенційно небезпечні об'єкти, розташовані в зонах зосередження проявів карсту, зсувів і підтоплення.

Наведене зумовлює необхідність проведення більш ґрунтовних досліджень комплексного впливу ЕГП на безпеку функціонування магістральних газопроводів на території України з урахуванням імовірності вияву цих процесів у місцях спорудження нових чи реконструкції існуючих систем. Обмежений обсяг наявних ресурсів захисту визначає необхідність їх використання для нейтралізації загроз на найбільш пріоритетних напрямках і територіях. Отримані в даній роботі результати зосереджують увагу на тих регіонах України, які потребують першочергової комплексної оцінки загроз від ЕГП для функціонування магістральних газопроводів.

CRITICAL INFRASTRUCTURE ADVANCED RESEARCH – SPACE SECURITY FOR BUSINESS CONTINUITY AND QUALITY OF LIFE

GEORGESCU Alexanru,
EURISC Foundation,
Romania

Space systems have become key components of critical infrastructure systems, playing a key role in vital components such as command, control and coordination capabilities, data gathering, positioning and so on. They have become such important applications for enabling the proper and safe functioning of terrestrial critical infrastructures, that we can even describe them as critical space infrastructures. The present article will present the arguments in favor of this conclusion, underline the myriad ways in which space systems differ from terrestrial systems when it comes to risk management and briefly introduce specific threats.

Finally, the article will present a non-spacefaring country's view on space systems reliance, underscoring the unique challenges associated with this dependence.

Introduction

Beginning with the launch of the first artificial satellite, Sputnik, the spacefaring nations of the world have managed to launch an impressive array of specialized objects into space, each of them with its own capabilities and objectives. This rate accelerated once private companies began to invest in space development, mainly by launching commercial satellites in close proximity orbits. Space systems are a key enabler for a widening spectrum of applications.

Over time, our increasingly globalized economies and societies have become dependent on the valuable services that these satellites and other space installations provide, from inexpensive, constant and instantaneous communications with worldwide coverage, to navigation systems, remote sensing, threat assessment and early warning. This dependence transcends national borders, even though the assets themselves are considered to still be under the jurisdiction of their countries of origin. We are also entering into a phase of greater private actor involvement and initiative, with cheaper launch solutions and less expensive systems, and with a gradual development of a legislative and institutional framework that is conducive to commercial operations by risk-averse private actors. It can be expected that the range of services provided by space based systems, as well as their numbers and complexity, is likely to grow, compounding the global dependency on their smooth operation.

With this in mind, space systems should be recognized as critical infrastructures that affect quality of life and business throughout the world and at all levels, from local, to national, regional, continental and, ultimately, global levels. States are beginning to recognize the opportunities afforded and vulnerabilities engendered by space infrastructures, which is why more and more are taking the first steps, often in a cooperative fashion, to establish a presence in such activities, along with the formulation and dissemination of good practices, customs, standards, laws and guidelines that should govern human activity in space.

These efforts are still in an early stage, with nowhere near the same level of acceptance, depth and breadth of similar legal and administrative frameworks on Earth, for instance in maritime law.

This is especially important in close proximity to Earth, which is the focus of most human activity and where the vast orbital space has begun to feel more crowded, with ever increasing numbers of assets, missions and debris from earlier activity. This is a truly international environment, with

dynamics that defy national borders and warrant a truly global stewardship of what can be described as the new «commons» of mankind.

Critical Space Infrastructures

Critical Infrastructure Protection (CIP) is a set of disciplines and philosophies that, together, make up a framework that recognizes the critical nature of infrastructures, as well as their extensive interdependences. The materialization of risks is not easily prevented or its effects contained, and disruptions tend to propagate throughout the system-of-systems, triggering cascading failures in the provision of critical goods and services. So far, CIP has been applied at national level, with an increasing development in regional organizations, such as the EU and NATO, but only for terrestrial infrastructures. Space systems were relegated to a marginal position, compared with more existential systems facings severe threats, like energy, food, water and health.

The criticality of space systems can no longer be ignored, and there is also the realization of the heavy dependence of previously mentioned critical infrastructures on space infrastructures, which provide command and control capabilities, information gathering, emergency response support and so on. For this reason, CIP precepts should be applied to critical space infrastructures (CSI) as well, identifying threats, mitigating vulnerabilities and minimizing disruptions. However, policy and decision makers should not just transpose CIP from terrestrial to space systems, as this would ignore the risks inherent in the heavy interconnections between the two. Rather, space systems should be integrated in existing CIP frameworks with the full realization of their importance, triggering developments in the fundamentals of critical infrastructure protection efforts around the world.

Timid progress has already been registered in building the legislative and institutional framework for critical space systems protection and development. The UN's Committee on the Peaceful Uses of Outer Space conducts varied research and regularly makes policy recommendations to member states regarding threats, opportunities and the implementation of new standards for achieving economic and security synergies. The United States, itself, is also an advanced actor, with the EU trailing not far behind. In the establishment and development of the European Programme for Critical Infrastructure Protection (EPCIP), space security has been present from the very beginning. Space was mentioned as one of the eleven critical infrastructures in Directive 114/2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, and was subsequently mentioned in EU documents on preparedness for cyber-attacks (COM (2009) 149 and

COM (2011) 163), space and cyber infrastructures being intimately linked to each other.

Furthermore, space development and security was given special attention in COM(2011) 152 – «Towards a space strategy for the European Union that benefits its citizens» and COM(2011) 808 – Horizon 2020 – The Framework Programme for Research and Innovation.

Specific Space Threats

CSI are faced with a wide range of extraordinary threats, man-made and natural, as well as accidental or premeditated. The environment in which they operate is one of the harshest known to man, filled with kinetic threats, harmful radiation and variations in temperature. Before proceeding with a brief description of the risks which are, to a certain extent, unique to CSI, we must also point out the fact that, due to characteristics of modern technology, of positioning in space and of the economic limitation to space activity, all of the services that SCI render for humanity are performed by a limited pool of fragile space assets. According to the Union of Concerned Scientists' collaborative database on space systems, the millions of consumers and billions of beneficiaries of space capabilities are reliant on just 1.300 space systems[84], which must cater to very different needs. The table below (table) shows a breakdown of space systems by type and by originating countries.

Table

Number of satellites by country of origin, orbit and type

	Criteria											
	Country				Orbit				Type (for US only)			
	United States	Russia	China	Other	LEO	MEO	Elliptical	GEO	Civil	Commercial	Government	Military
Number of satellites	549	131	142	483	696	87	41	481	21	250	126	152
Total in the group	1305				1305				549			

This concentration of service capacity leads to unique opportunities for space economic development in the future, but also to the possibility of serious disruptions from the most random and limited occurrences. For in-

[84] *Union* of Concerned Scientists [Електронний ресурс]. – Режим доступу: http://www.ucsusa.org/nuclear-weapons/space-weapons

stance, the premier global navigation system, the American GPS constellation, only contains 30 satellites for servicing billions of service requests. Incipient networks or regional ones, like Galileo, become operational with only a few units in orbit, compounding the risks of disruption, which is somewhat mitigated by being the first Global Navigation Satellite System (GNSS) that can interface with both the American GPS and the Russian GLONASS systems, in addition to the various ground station amplifiers. Weather satellites are similarly burdened, and just as important. The main vanguard of Earth's early warning system against solar flares is one NASA probe (Advanced Composition Explorer, which can provide warnings of events 15–45 minutes beforehand), and the only human habitat currently in space and with scientific capabilities is the International Space Station. Redundancy is difficult to achieve, replacement is time consuming and threats are omnipresent, which makes our dependence on these infrastructures even more worrying.

Directed threats against space infrastructures used to be a hallmark of science fiction, however the United States ran satellite obliteration tests in the 1985 and, as recently as 2007, China used a missile to destroy the FengYun-1C meteorological satellite, weighing 750 kg and at an altitude of 865 km, generating, by NORAD estimates, 2316 golf ball sized pieces of debris[85]. Even more worrying is the fact that one does not need expensive conventional attack methods to impact CSI operations. Cyber-attacks have one of the lowest costs to damage ratio among unconventional warfare methods, since a skilled individual with a laptop and an uplink is almost untraceable and can disrupt satellite operations, falsify or steal data and even destroy the satellite. Even if the assets are secure against interference, the links with their respective ground stations are not, and suitable jammers are easily manufactured and sold with other applications in mind[86].

As to the threats that are unique to SCI, the two most dangerous are random collisions with debris and space weather.

To put the space debris issue into perspective, most human activity is concentrated in a thin layer of orbital space surrounding the Earth, where decades of launches, accidents, collisions and carelessness have produced over hundreds of thousands of objects larger than a centimetre hurtling through space at 8 km/s. Even millimetre sized objects are extremely dangerous. While most do eventually re-enter the Earth's atmosphere, it usually requires a very low orbit or an inordinate amount of time. Orbital

[85] *Center* for Space Standards and Innovation. Chinese ASAT Test. Retrieved from http://www.centerforspace.com/asat/

[86] *Gheorghe A. V.* Risk and vulnerability games. The anti-satellite weaponry (ASAT) / A. V. Gheorghe, D. V. Vamanu // International Journal on Critical Infrastructures. –2007. – Vol. 3. – N. ¾. – P. 457–470.

space, in this regard, is one of the least regenerative environments known to man, and there have been fears, such as the Kessler Syndrome proposition[87], of debris density becoming so high, that one final collision produces a cascade effect of other collisions, rendering Low Earth Orbit into a dangerous or even uninhabitable minefield. A revealing incident took place on the 10th of February 2009 when an American commercial satellite collided with a Russian military one 789 km of the Taymyr Peninsula in Siberia. The speed of collision was 11,7 km/s, and the number of new, detectable, debris generated by the incident numbers 2140[88], with thousands more being too small for tracing. It was the first random collision between satellites at hyper speeds, although there had been other incidents in the past. The Russian satellite was a 950 kg, nuclear-powered military satellite called Kosmos-225, which was launched in 1993 and deactivated in 1995. The American one weighed 560 kg, had been active since 1997, and was link number 33 in the Iridium Corporation communication network which contained 66 units[89]. A representative from Iridium stated that they received 400 weekly close proximity warnings, issued when an Iridium satellite is within 5 km of another satellite, and Iridium 33 was scheduled to bypass the Russian relic by 584 metres[90].

The challenges faced in overcoming debris are considerable, ranging from technical to legal, since most of the elements of the debris field are generated by human activity and, in a variant of the «tragedy of the commons», there is little incentive to cover the costs of cleaning up or ensuring that inactive assets are deorbited. In 1978, when the first reports on the debris field were commissioned, NASA specialist Donald Kessler (who coined the term Kessler Syndrome) found that 42% of existing debris was generated by 19 US launches or explosions[91]. Even more worrying is the threat that the debris field may become the object of kinetic terrorism or deterrence games in the vein of Cold War mutually assured destruction doctrines[92], a view expressed by the RAND Corporation.

The «cosmic weather system» is the other equal opportunity threat to CSI. It is unrelated to terrestrial weather patterns, which are confined

---

[87]*Long Austin.* Deterrence: From Cold War to Long War. Retrieved from http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG636.pdf

[88]*National* Aeronautics and Space Administration. Retrieved from http://www.orbitaldebris.jsc.nasa.gov/newsletter/pdfs/ODQNv13i2.pdf

[89]*Weeden B.* Billiards in Space / B. Weeden. Retrieved from http://www.thespacereview.com/article/1314/1

[90]*Kelso T. S.* Iridium 33/Cosmos 2251 Collision / T. S. Kelso. Retrieved from http://celestrak.com/events/collision.asp

[91]*Kessler D. J.* The Kessler Syndrome / D. J. Kessler. Retrieved from http://webpages.charter.net/dkessler/files/KesSym.html

[92]*Long A.* Deterrence: From Cold War to Long War / A. Long. Retrieved from http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG636.pdf

to Earth's atmosphere. Unlike extreme Earth weather, which disproportionately impacts the populations of poor countries, space weather impacts rich countries above all others, since they are the biggest consumers of services provided by CSI and they derive the greatest economic added value from employing them in the economy.

Space weather, as a threat to CSI, is primarily made up of the high speed ejections of plasma from the Sun, which experiences periodic solar flares on a seemingly 12 year cycle. In humanity's brief history with post-modern industrialism, there has never been a truly destructive solar flare event. In its industrial history, however, we have the example of the Carrington event, the largest ever recorded, which, in 1859, lead to auroras manifesting at the Equator, measurement devices becoming erratic and world telegraph network being heavily damaged, with service interruptions[93].

Smaller events left six million inhabitants of the Canadian province of Quebec without electricity for several hours, and many planes grounded or rerouted[94]. In this respect, solar weather, while an existential threat for space borne assets, can also lead to disruptions of services and significant damage at terrestrial level. In 2003, which was another peak of solar activity, alongside power disruptions on the ground, orbital activity was seriously affected – 59 % of scientific missions were interrupted, astronauts had to take refuge in specially shielded areas of the ISS, and a number of satellites were lost[95].

The US National Academy of Sciences (NAS) released a report that estimated damages for a Carrington Event occurring in such a way that it strikes the US in full at 2 trillion dollars in the first year for the US alone, and recovery times between four and ten years[96], without also counting damages to electricity grids in Europe, lost economic opportunity and so on. Other key terrestrial infrastructures are disrupted, mostly as a result of the loss of electricity and communications.

Future events could exploit weak links in infrastructure systems to inflict even greater damage, with the NAS estimating that, due to vulnerable transformer stations, over 130 million consumers in the US alone would be

---

[93]*Extreme* Space Weather: Impacts on Engineered Systems and Infrastructure / Royal Academy of Engineering. – P. 18. Retrieved from http://www.raeng.org.uk/publications/reports/space-weather-full-report

[94]I bid.

[95]*Butt Y. M.* The EMP threat: fact, fiction and response / Y. M. Butt. Retrieved from http://www.thespacereview.com/article/1553/1

[96]*Severe* Space Weather Events: Understanding their Economic and Societal Impact / National Research Council of the National Academies. – 2008. Retrieved from http://lasp.colorado.edu/home/wp-content/uploads/2011/07/lowres-Severe-Space-Weather-FINAL.pdf

deprived electricity for more than a few hours[97], maybe even weeks, with effects not just on technical systems, but also on public trust, public order and national defence.

Space systems play a vital role in researching these phenomena and warning against them, with various probes containing measuring devices that warn of incoming radiation storm fronts, in addition to the specialised systems already in place, like the Solar and Heliospheric Observatory[98]. In addition to their proven usefulness in governing terrestrial risks, space systems are the main line of defence against space threats, not just to themselves, but to terrestrial infrastructures, making them an integral part of CIP efforts and not just their recipient.

The small country conundrum

The issues surrounding dependence on space systems are compounded in the case of non-spacefaring nations exhibiting these critical connections. Since the prosperity and technological advancement of every nation is growing more dependent on space systems, it stands to reasons that not only the big players, such as the US, Russia, the EU and emerging powers, such as India and China, are going to be consumers of space services, but also smaller countries.

These countries may find the resources to perform space related research and development, but they will not be able to field the number of space systems required to meet their specific needs. Many of them, like Romania, have no space systems of their own, even though the Romanian Space Agency is a full member of the European Space Agency, the second Eastern European nation to gain this position.

In this case, countries such as Romania find themselves dependent on space systems for advancements such as weather monitoring, precision agriculture, environmental protection, communications and various other areas, but their access to these space systems is mediated by foreign companies and other entities who own and operate these space systems and who are headquartered in other states, whose laws and sovereignty they must respect. The space systems are considered to be under the jurisdiction of the state that owns them or exercises authority over the owning company. The thread is going to become much more complicated as private companies become an increasingly important part of human

[97] *Severe* Space Weather Events: Understanding their Economic and Societal Impact / National Research Council of the National Academies. – 2008. Retrieved from http://lasp.colorado.edu/home/wp-content/uploads/2011/07/lowres-Severe-Space-Weather-FINAL.pdf

[98] *Hapgood M.* Space weather. Its impact on Earth and implications for Business / M. Hapgood, A. Thomson. Retrieved from https://www.lloyds.com/~/media/lloyds/reports/360/360%20space%20weather/7311_lloyds_360_space%20weather_03.pdf

activity in space. Already, a private company can access private financing to build a satellite which will be launched by another private company and operated by another, providing services to private and state actors. If countries such as the United States fret about the governmental reliance on private assets (such as the fact that 90 % of US military communications pass through civilian owned satellites which are neither hardened nor shielded from threats like military satellites are, presumably), then what should Romania and other countries conclude about their own positions?

In various crises situations, these countries may find themselves outbid for access to scarce capacity for the provisioning of critical services, outmanoeuvred for compelling companies to keep their interests in mind (since the company is not headquartered in the respective country) or simply the inadvertent victim of policies imposed by another state, especially with regards to dual use systems. For instance, the premier GNSS, the American GPS, is still a military system and the US Military reserves the right to terminate access or degrade service quality to any user, including allied nations and businesses and individuals headquartered there, should it decide that opaque criteria for emergency situations have been met.

These challenges, like most of the ones comprising risk governance, require not just technical acumen to be addressed, but also political and organizational efforts.

One option would be to simply forego the benefits of space services that cannot be replaced by ground systems under the country's control. This might spur innovation, but it can also lead to productivity stagnation and worsening quality of life, as well as compounding the numerous risks that the use of space systems as security tools are trying to address (natural disasters, extreme weather phenomena etc.).

The second option is to steadily become a spacefaring nation and establish at least critical reserves of space capabilities provisioning, if not outright independence. The possibilities are growing with the development of nanosatellites, modular satellites, high altitude platforms (flying or balloon drones), more affordable launch costs and arrangements for secondary payloads, but also the very important rise of new business models for accessing space information. For instance, the ESA's Copernicus/GMES Program will launch a constellation of Earth Observation satellites, whose output, to a certain quality, will be made available free of charge to users[99]. Other programs, designed by international institutions for use in address-

[99] *Free* access to Copernicus satellite data. Retrieved from http://www.esa.int/Our_Activities/Observing_the_Earth/Copernicus/Free_access_to_Copernicus_Sentinel_satellite_data

ing specific issues in developing countries, can also be a model for affordable access to space.

The third option is to become involved in the continuing evolution of the international legal and administrative framework for managing space activities and to use their influence to positively impact the security and sustainability of the provision of space services. For instance, the UN Committee on the Peaceful Uses of Outer Space develops technical recommendations, including for issues such as minimizing the amount of new space debris created during launches or at the end of a satellite's useful life. Institutions such as the International Telecommunications Union handle the distribution of the frequency spectrum to avoid satellites accidentally jamming each other through proximity (called frequency fratricide by the UK Ministry of Defence's Center for Development, Concepts and Doctrine[100]). Meanwhile, the Galileo GNSS project of the ESA is specifically designed with the input of partner nations and lacks any provision whatsoever for limiting the legitimate access of users to its services, reducing the uncertainties of the provision of critical positioning, synchronization and navigation services[101].

Conclusion

It is this realisation, of the central role that space systems play in conducting, as well as securing, economic, social and political affairs, that warrants their inclusion among critical infrastructures. Furthermore, rather than using their extra-terrestrial nature and uniquely challenging security environment to justify a separate framework for their risk governance, CSI, as well as terrestrial infrastructures, would benefit most if countries, companies and international organizations integrate them in their overarching CIP efforts and strategies. There is an important role here to play even for non-spacefaring nations, who are, nevertheless, critically dependent on the functioning of space systems. CSI function at near-global levels, which render their criticality even more apparent, as there is no hope of regional containment of disruption effects or of certain risks, such as deliberate threats to their integrity. In the end, we are only as secure and as prosperous as all of our critical infrastructures will allow, including various space systems.

Acknowledgement

The insights expressed during this article were gleaned from a research project named «Space Systems as Critical Infrastructure» led by the Ro-

[100] *Space:* Dependencies, Vulnerabilities and Threats / Ministry of Defence (MoD). Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33689/20120313mne7_space_vulnerabilites.pdf

[101] *European* Space Agency. Retrieved from http://www.esa.int/Our_Activities/Navigation/Galileo_and_EGNOS accessed. – 05.12.2015.

manian Space Agency, with the Military Equipment and Technologies Research Agency of the Romanian MoD, and the EURISC Foundation. The work was supported by a grant of the Romanian National Authority for Science Research, CNDI-UEFISCDI, project number 197/2012. The findings were also presented during the Resilience 2050 Conference organized by the Royal United Services Institute in London, UK, where a related paper won the first edition of the essay competition on resilience issues.

РЕФЕРОВАНІ ВИСТУПИ УЧАСНИКІВ МІЖНАРОДНОЇ ЕКСПЕРТНОЇ НАРАДИ (15-16 ЖОВТНЯ 2015 р.)[1]

[1] *Відбулася* міжнародна експертна нарада з питань захисту критичної інфраструктури в Україні [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/1960/

ЄВРОПЕЙСЬКИЙ ДОСВІД У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ1

Експерт Женевського центру демократичного контролю над збройними силами (*DCAF*) **Валерій РАДЧЕВ** доповів про європейський досвід захисту критичної інфраструктури. На початку свого виступу він нагадав про складне безпекове середовище, в якому опинилися Балканські країни під час воєнних дій в Косово. Пан Радчев підкреслив, що в умовах швидких змін безпекового середовища не повинно виникати затримки у прийнятті політичних рішень із реформування сектору безпеки і оборони. Доповідач зауважив, що кожна країна повинна будувати захист критичної інфраструктури, виходячи із національних особливостей, водночас вивчення досвіду інших країн, здійснення так званого «бенчмаркінгу» є вкрай важливим. Характеризуючи механізми захисту критичної інфраструктури в ЄС, доповідач зауважив, що раніше вони переважно були побудовані на уявленнях про необхідність підготовки економіки, населення та територій до воєнних дій, проте після терористичних атак, скоєних у Мадриді (березень, 2004 рік), ці механізми сфокусовані на забезпеченні безпеки суспільства, повсякденного життя європейців. Пан Радчев зауважив, що ЄС зосереджує увагу на загальноєвропейській інфраструктурі (енергетична, транспортна), водночас поширюючи загальні підходи та стандарти щодо захисту критичної інфраструктури в кожній країні – члені ЄС. Підкреслюючи важливість дослідження каскадних ефектів, пов'язаних з відмовами об'єктів критичної інфраструктури, доповідач навів приклади таких наслідків, що були спричинені терористичними актами в Нью-Йорку (вересень, 2001 рік). Також пан Радчев нагадав відомий принцип: «система надійна настільки, наскільки надійною є її найслабша ланка», а отже, на переконання доповідача, яке він проілюстрував на прикладі банківської системи, у разі слабкості інструментів економічного регулювання марними будуть зусилля з підвищення кібербезпеки, фізичної охорони банків та ін.

Валерій Радчев зазначив, що критична інфраструктура в Європі стає дедалі більш складною та взаємопов'язаною, підвищується вразливість таких об'єктів, і ця тенденція випереджає зусилля європейських держав, спрямованих на покращення механізмів регулювання безпеки, таких як стандарти безпеки.

Розглядаючи принципи побудови захисту критичної інфраструктури в ЄС, доповідач виокремив такі: поступове включення нових

---

[1]*За матеріалами* виступу В. Радчева на Міжнародній експертній нараді щодо розробки Зеленої книги з питань захисту критичної інфраструктури в Україні, НІСД, 9 вересня 2014 р.

складових у систему захисту; пропорційність розміщення ресурсів на основі аналізу ризиків; кооперація між всіма стейкхолдерами (державного та недержавного сектору); забезпечення захисту інформації щодо загроз (рис.).

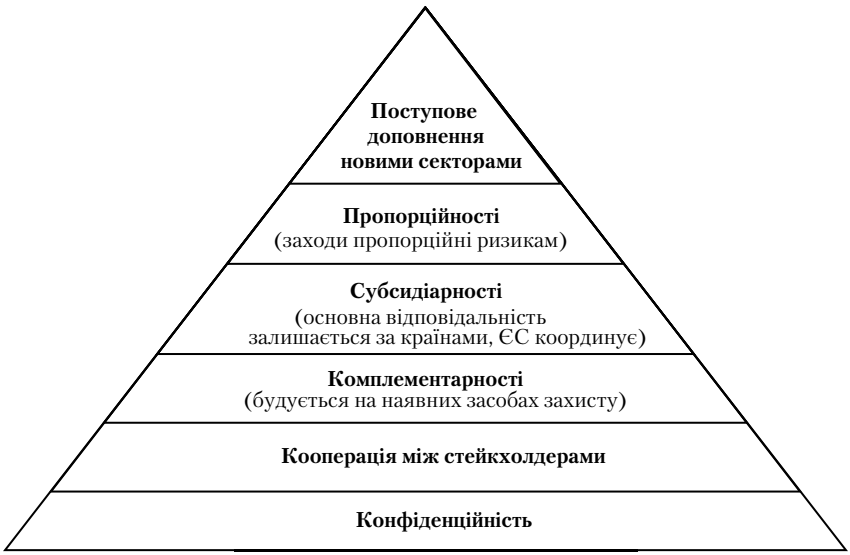

Рис. Основні принципи побудови захисту критичної інфраструктури в ЄС

Підсумовуючи сказане, Валерій Радчев зауважив, що рішення щодо організації захисту критичної інфраструктури є політичними, які значною мірою залежать як від особливостей побудови системи захисту національної безпеки окремої країни, так і від стану безпекового середовища.

ПРО ДОСВІД РЕСПУБЛІКИ ПОЛЬЩА У СТВОРЕННІ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ[2]

Експерт з питань захисту критичної інфраструктури Урядового центру безпеки Республіки Польща **Кшиштоф БЖОЗОВСКІ** доповів

[2] *За матеріалами* виступу К.Бжозовскі на Другій міжнародній експертній нараді щодо розробки Зеленої книги з питань захисту критичної інфраструктури в Україні, НІСД, 25 листопада 2014 р.

про досвід Польщі щодо створення системи захисту критичної інфраструктури. Він повідомив, що в Польщі досі триває дискусія щодо розуміння терміну «критична інфраструктура». У країні, за його словами, є велика кількість зацікавлених сторін, і їхні думки з цього приводу можуть істотно відрізнятися. Тому досягнення розуміння цієї проблеми є доволі складним процесом. А під час дискусії було запропоновано влучну аналогію з тілом людини. Якщо порівняти критичну інфраструктуру з тілом людини, і поставити питання, чи зможе людина прожити без руки, ока, ноги, то відповідь буде ствердною, хоча це й не буде комфортний спосіб життя. Але чи зможе людина прожити без мозку чи серця? Однозначно ні. І це є відповіддю на питання про те, що таке критична інфраструктура. Саме тому потрібно захищати насамперед життєво важливі органи. Аналогічна ситуація і з критичною інфраструктурою (КІ).

Кшиштоф Бжозовскі повідомив, що у Польщі почали з виявлення важливих елементів КІ та кращого розуміння завдання щодо їх захисту. Робота розпочалася під егідою Міністерства внутрішніх справ, але потім Державним секретарем було утворено Центр безпеки, що засвідчило усвідомлення необхідності створення окремої структури.

Польський досвід демонструє, що в цій сфері загалом є три головні проблеми: удосконалення законодавчої бази, визначення якісних критеріїв для віднесення об'єктів до КІ, підтримка якості партнерства шляхом обміну важливою інформацією між зацікавленими сторонами.

У Польщі існує система захисту критичної інфраструктури (ЗКІ), що включає багато структур, до основних з яких належать Урядовий центр з безпеки, оператори об'єктів КІ, міністерства відповідальні за ЗКІ. ЗКІ є обов'язком оператора. При цьому оператори об'єктів КІ зобов'язані готувати плани захисту об'єктів, а також призначати контактних осіб, відповідальних за підтримку відносин з державними органами[3].

З отриманням інформації, що об'єкт включено до списку КІ, оператор повинен упродовж дев'яти місяців підготувати План захисту критичної інфраструктури об'єкта. До цього плану включаються загальні дані про об'єкти, серед яких назва та місце розташування об'єкта, його реєстраційний номер, номери у Комерційному регістрі, Національному судовому реєстрі, відповідальна особа, характеристика об'єкта КІ та основні технічні параметри. Наступним елементом плану є аналіз ризиків для об'єкта КІ з урахуванням виявлених загроз та впливів, визначення рівня ризику для об'єкта та винесення рішення щодо його прийнятності.

[3] *Regulation* of the Council of Ministers of 30 April 2010 № 542 on Critical Infrastructure Protection Plans [Електронний ресурс]. – Режим доступу: http://rcb.gov.pl/eng/wp-content/uploads/2011/03/REGULATION-ON-CIP-PLANS.pdf

Вкрай важливим моментом є співпраця з владою на всіх рівнях (урядовий, місцевий), а також з Агентством внутрішньої безпеки у випадку реагування на терористичну загрозу. У Польщі є Національний план управління в кризових ситуаціях, що включає такі загрози як повінь, епідемії, хімічне забруднення, порушення у подачі електроенергії, порушення у подачі рідкого палива, порушення подачі газу, сильні морози/сильний снігопад, урагани, лісові пожежі, епізоотія тощо.

План ЗКІ повинен мати повний опис захисних заходів за шістьма напрямами, що включають фізичну безпеку, технічну безпеку, безпеку персоналу, інформаційну та кібербезпеку, правовий захист, плани відновлення. Він має передбачати варіанти дій у разі надзвичайної ситуації, для забезпечення безперервного управління, відновлення частини або всього об'єкта КІ. План має включати положення про співробітництво з місцевими органами управління кризовими ситуаціями та національними адміністраціями.

План ЗКІ має бути погоджений упродовж 14 днів та узгоджений у відповідній частині з територіальними органами поліції, пожежної служби, управлінням водопостачання, інспектором будівельного контролю, ветеринарним інспектором, санітарним лікарем, директором Морського бюро, а також упродовж 45 днів – з міністерством, відповідальним за даний об'єкт КІ.

Начальник державного Центру з безпеки має 90 днів для аналізу та затвердження Плану захисту критичної інфраструктури. Якщо плану бракує необхідної інформації або рівень ЗКІ не є достатнім, він повертається до оператора для внесення змін. Плани захисту критичної інфраструктури мають оновлюватися кожних два роки. План захисту КІ містить конфіденційну інформацію, що повинна бути захищена.

ЗАПРОВАДЖЕННЯ МІЖВІДОМЧОЇ ВЗАЄМОДІЇ: ВИКЛИК ДЛЯ УСПІШНОЇ КООРДИНАЦІЇ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ[4]

Експерт Женевського центру демократичного контролю над збройними силами **Тодор ТАГАРЕВ** на початку свого виступу підкреслив, що Україна, підходячи до вирішення такого складного та важливого завдання, як побудова захисту критичної інфраструктури, обрала вдалий формат документа – зелена книга, що дає змогу консолідувати погляди різних зацікавлених сторін. Пан Тодор Тагарев

[4] *За матеріалами* виступу Т. Тагарева на Міжнародній експертній нараді щодо розробки Зеленої книги з питань захисту критичної інфраструктури в Україні, НІСД, 15-16 жовтня 2015 р.

зауважив, що досвід європейських країн свідчить як про досягнення, так і про численні проблеми, пов'язані зі створенням системи захисту критичної інфраструктури, однією з яких є міжвідомча взаємодія.

Численні різноманітні загрози, що впливають на функціонування критичної інфраструктури як у цивільному, так і у військовому вимірах, впливають на здатність забезпечити надання послуг, товарів та функцій, життєво необхідних громадянам та економіці країни. До того ж ці загрози через взаємопов'язаність об'єктів інфраструктури можуть вплинути на всю критичну інфраструктуру. Тому, як зазначив доповідач, захист критичної інфраструктури виходить за межі відповідальності та можливостей окремих відомств, що вимагає ефективного координування їхніх зусиль.

Зазвичай аналіз захисту критичної інфраструктури здійснюється в межах підходів до управління ризиками. Тому, по-перше, потрібно чітко окреслити той набір загроз і сценаріїв (наприклад, до них можуть входити або ні ті, що пов'язані з воєнними діями). По-друге, потрібно оцінити наслідки, не безпосередні для об'єктів, а кумулятивні для економіки та суспільства. По-третє, потрібно розробити рішення для зниження ризику. Доповідач підкреслив, що через різноманітність загроз вирішення останнього завдання потребує координування зусиль як різних відомств, так і приватного сектору, місцевої влади, громадян, а в деяких випадках – і міжнародних інституцій. Щодо запровадження підходу до врахування всіх видів загроз (т.зв. *all-hazzard approach*), то, як зазначив Тодор Тагарев, тут знову потрібне міжвідомче координування.

Пан Тагарев у своїй доповіді представив три форми координування. Перша, з них – це кооперація, яка часто залишається неформальною формою взаємодії за відсутності спільного плану дій, а також при незмінних обов'язках усіх учасників. Друга пов'язана із впровадженням спеціальних координуючих потужностей (огляд сумісності цілей та завдань, взаємодія в межах проектів та програм, встановлення каналів зв'язку, спільні навчання, розподіл функцій та загальний доступ до ресурсів тощо). Остання форма – колаборація, яка означає визначення нових спільних довгострокових цілей та завдань, створення організаційних структур та перерозподіл функцій, вдосконалення планування та обміну інформацією, створення пулу ресурсів тощо. Також завдання координації можна розбити на дві групи: операційна (як діяти разом усім суб'єктам) та розвитку (як розміщувати ресурси, визначати їх характеристики).

Розглядаючи досвід Болгарії з координації зусиль у сфері захисту критичної інфраструктури, Тодор Тагарев повідомив, що у 2005 році в країні прийнято Закон «Про управління кризовими ситуаціями» та утворене Міністерство з надзвичайних ситуацій. Проте робота із

захисту критичної інфраструктури пришвидшилась лише в 2008 році як реакція на прийняття Європейською Комісією Директиви 114[5]. А вже станом на 2010 рік Міністерство з надзвичайних ситуацій було розформоване, сили цивільного захисту передані в управління Міністерству внутрішніх справ, а Закон «Про управління кризовими ситуаціями» скасований. Таким чином, національною «контактною точкою» з питань захисту критичної інфраструктури став Генеральний директорат з питань пожежної безпеки та цивільного захисту Міністерства внутрішніх справ, незважаючи на те, що до загальноєвропейської критичної інфраструктури згідно з Директивою 114 належать об'єкти енергетики та транспорту. Доповідач назвав дві обставини, що спричинили таку ситуацію. По-перше, у Болгарії тривалий час розвивалася Загальнодержавна система цивільного захисту, до завдань якої входило реагування на наслідки природних лих і техногенних катастроф. А по-друге, міністерства, що формують державну політику у сферах енергетики та транспорту, не виявляли інтересу до вирішення завдань захисту критичної інфраструктури, можливо, через відсутність додаткового фінансування на такі цілі. Зокрема, за словами Тодора Тагарева, у Міністерстві транспорту заявили, що в Болгарії немає критичної транспортної інфраструктури європейського рівня, отже, не може виникати додаткових зобов'язань щодо її захисту.

Продовжуючи аналіз досвіду Болгарії, Тодор Тагарев звернув увагу на закон Болгарії «Про систему забезпечення національної безпеки» (прийнятий у 2015 році). У ньому передбачено заходи з покращення координації у сфері безпеки країни через розширення функцій Ради національної безпеки і створення при ній ситуаційного центру. Функції такого центру полягають не тільки в моніторингу ситуації, а й у формуванні варіантів рішень у кризових ситуаціях.

Окремо Тодор Тагарев зупинився на проблемі фінансування превентивних заходів із забезпечення безпеки об'єктів критичної інфраструктури. За його словами, хоча превентивні заходи передбачаються законодавчими нормами, на практиці (це ще раз засвідчили наслідки минулорічних повеней у Болгарії) кошти витрачаються на ліквідацію наслідків.

Відповідаючи на питання, яким чином відбувалося визначення елементів критичної інфраструктури на загальноєвропейському рівні, чи був цей процес керований із Брюсселю, чи, може, країни – члени ЄС самі вирішували, як визначати критичну інфраструктуру, Тодор

[5]*Council* Directive 2008/114/EC of 8 December 200 [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

Тагарев зазначив, що хоча розробка нормативних актів Європейської Комісії здійснюється в Брюсселі, вони мають враховувати різноманітні інтереси країн – членів ЄС, оскільки, по-перше, в процесі підготовки документів задіяні спеціалісти з різних європейських країн, а по-друге, директива має пройти процес ратифікації. При визначенні критичної інфраструктури в першу чергу невеликі європейські країни були зацікавлені віднести до такого переліку якнайменше об'єктів. У результаті в Директиві 114 2008 року для загальноєвропейської критичної інфраструктури розглядаються тільки два сектори (енергетика та транспорт), хоча експерти, які були задіяні в напрацюванні даної Директиви, погоджувалися з тим, що доречно доповнити цей перелік у найближчому майбутньому секторами телекомунікацій та зв'язку.

ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В ЧЕСЬКІЙ РЕСПУБЛІЦІ[6]

Експерт Офісу зв'язку НАТО в Україні **Мартін ЛІНХАРТ** на початку виступу розглянув витоки кризового управління в Чехії, яке отримало розвиток після катастрофічних повеней у 90-х роках минулого століття. Мартін Лінхарт зазначив, що в Чехії існує розмежування понять «кризова ситуація» та «надзвичайна ситуація». Так, кризова ситуація має загальнонаціональний масштаб, може бути спричинена крупною промисловою аварією, природним лихом чи надзвичайною ситуацією іншого характеру, наслідком якої є введення надзвичайного стану, воєнного стану чи стану неминучої загрози національній безпеці.

Доповідач наголосив на необхідності побудови рамкових сценаріїв на національному рівні з метою врахування основних загроз, що можуть призвести до кризової ситуації. Так, за даними Мартіна Лінхарта, у Чеській Республіці таких сценаріїв лише 23, але вони доволі добре визначають основні безпекові виклики для країни.

Розповідаючи про впровадження захисту критичної інфраструктури, доповідач охарактеризував період 2003-2007 рр. як домінування «нечіткого» підходу. На цей період припало створення європейської Зеленої книги із захисту критичної інфраструктури (2005 р.). Проте наступний період був ініційований прийняттям Директиви 114 в 2008 році і тривав майже два роки. За цей час деякі положення даної директиви були виконані. Щодо нововведень в

[6] *За матеріалами* виступу М. Лінхарта на Міжнародній експертній нараді щодо розробки Зеленої книги з питань захисту критичної інфраструктури в Україні, НІСД, 15-16 жовтня 2015 р.

національному законодавстві, пов'язаних із впровадженням захисту критичної інфраструктури, то вони були обмеженими поправками до Закону «Про управління кризовими ситуаціями».

Як зазначив Мартін Лінхарт, основним питанням в організації системи захисту критичної інфраструктури є визначення межі між зобов'язаннями органів влади та операторів даної інфраструктури. Відповідно, ці зобов'язання відображаються на витратах, спрямованих на підвищення безпеки функціонування інфраструктури. Також принциповим моментом є розмежування національної та загальноєвропейської критичної інфраструктури в країні. Як правило, країни-члени ЄС не зацікавлені в тому, щоб значна кількість об'єктів була віднесена до останньої категорії. Наприклад, якщо у Чеській Республіці на національному рівні визначено дев'ять секторів критичної інфраструктури, то загальноєвропейська критична інфраструктура визначається лише в двох із них.

Доповідач звернув увагу учасників наради на необхідність розрізняти поняття «елемент» та «суб'єкт» критичної інфраструктури. Першим є конкретні інфраструктурні об'єкти, як-то трубопроводи, мости, будівлі тощо. Другим – власники таких об'єктів.

Говорячи про завдання щодо ідентифікації елементів критичної інфраструктури, Мартін Лінхарт навів чисельні граничні значення за критеріями віднесення елементів до такої категорії. Наприклад, за кількістю людських жертв встановлено граничне значення в 250 осіб або 2500 госпіталізованих осіб на термін понад 24 години, за економічним впливом – втрата від 0,5 % ВВП країни, за впливом на життєдіяльність населення – порушення важливих функцій для 125 тис. осіб.

Окремо Мартін Лінхарт зупинився на питанні фінансування заходів із попередження кризових ситуацій. Він доповів, що Чеським законодавством передбачено, що за наповнення спеціальних цільових резервних фондів відповідають органи місцевої (регіональної та муніципальної) влади. На національному рівні створено два резервних фонди, але їх наповнення становить лише 100 млн крон для кожного (еквівалент приблизно такої самої суми в гривні).

Наприкінці свого виступу Мартін Лінхарт наголосив на необхідності навчання спеціалістів у сфері захисту критичної інфраструктури та підготовки тих осіб, що ухвалюватимуть рішення під час управління кризами (включаючи представників відомств, місцевої влади, топ-менеджерів великих компаній).

Мартін Лінхард зазначив, які в цій сфері питання мають вирішуватися на основі консенсусу, хоча це і спричиняє повільність руху, оскільки відповідальність за захист об'єктів критичної інфраструктури стає обов'язком країни – члена ЄС, на території якої ці об'єкти розміщені.

ОРГАНІЗАЦІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ, ЩО НАЛЕЖАТЬ ДО СФЕРИ УПРАВЛІННЯ МІНЕНЕРГОВУГІЛЛЯ, В МИРНИЙ ЧАС

Начальник відділу фізичного захисту, антитерористичної діяльності Міненерговугілля **ЛУЧКОВ В'ячеслав Іванович** на початку доповіді нагадав присутнім експертам, що для паливно-енергетичного комплексу питання захисту об'єктів електроенергетики, атомної промисловості та нафтогазового комплексу чітко виписані в законодавстві України. Визначено критерії ідентифікації об'єктів, а в них відображено аспекти економічної безпеки, життєдіяльності населення, екологічної безпеки тощо. Доповідач зазначив, що за необхідності відповідні критерії та граничні показники можуть бути використані для ідентифікації об'єктів критичної інфраструктури, проте вони містяться в документах із закритим доступом. Ситуація, яка склалася в державі, події на Донбасі суттєво вплинули на організацію охорони таких об'єктів енергетики.

Де-юре система має функціонувати в правовому режимі мирного часу. Проте, як зауважив В'ячеслав Лучков, вирішення багатьох питань енергетичної безпеки потребує нових механізмів. Наприклад, проблеми поставки вугілля на об'єкти теплової електрогенерації розв'язувалися в режимі ручного управління спільними зусиллями Міненерговугілля, Служби безпеки та Фіскальної служби. Доповідач додав, що подібні механізми вже передбачені для особливого періоду, але для мирного часу вони не врегульовані, а також нагадав, що нині дві ТЕС (з них Луганська взагалі відключена від об'єднаної енергосистеми України) розміщено на кордоні зони проведення АТО. У такій ситуації ризик руйнування цих ТЕС, зокрема їх відключення, є дуже значним.

Наприкінці виступу В'ячеслав Лучков наголосив на важливості вирішення питання державно-приватного партнерства в секторі енергетики. За його даними, 70 % об'єктів теплової генерації нині перебувають у приватній власності. Таким чином, питання ціноутворення на електроенергію для населення та промисловості, а також пов'язане з ним питання ціни на вугілля є вкрай важливим. Отже, у законодавство потрібно вносити норми, в яких мають бути прописані механізми взаємодії держави та власників об'єктів критичної інфраструктури. Тут логічно запровадити формування дворівневої системи захисту критичної інфраструктури. Перший рівень – аналіз загроз (різного характеру), що має враховуватися в цивільному захисті. Другий – аналіз припинення функцій критичної

енергетичної інфраструктури з механізмом інженерно-технічного та фізичного захисту, сформованого для мирного часу. В'ячеслав Лучков також повідомив про нову редакцію проектної загрози, розроблену нещодавно в Україні, в якій враховано складну безпекову ситуацію на Донбасі.

ЗАХОДИ ЩОДО ФІЗИЧНОГО ЗАХИСТУ, ОХОРОНИ ТА АНТИТЕРОРИСТИЧНОЇ ЗАХИЩЕНОСТІ АТОМНИХ ЕЛЕКТРОСТАНЦІЙ

Начальник відділу Дирекції фізичного захисту та спеціальної безпеки ДП «НАЕК «Енергоатом» **КУНИЦЬКИЙ Ігор Миколайович** наголосив, що дирекцією з фізичного захисту і спеціальної безпеки ДП «НАЕК «Енергоатом» вживається комплекс заходів з організації функціонування системи фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, джерел іонізуючого випромінювання, зокрема при перевезенні радіоактивних матеріалів з метою попередження актів ядерного тероризму, крадіжки або будь-якого іншого незаконного вилучення ядерних і радіоактивних матеріалів.

Крім цього, підрозділами фізичного захисту та антитерористичними штабами ВП АЕС спільно з Дирекцією ФЗСБ протягом 2014–2015 рр. відповідно до державної та відомчої програм впроваджуються практичні заходи з підвищення ефективності та надійності захисту АЕС та об'єктів їх життєзабезпечення, які є уразливими до терористичних загроз.

У 2015 році особлива увага приділялася впровадженню комплексу превентивних заходів, спрямованих на підтримання належного рівня фізичного захисту, антитерористичної та протидиверсійної захищеності Запорізької та Южно-Української АЕС, що наближені до східних областей України, де триває антитерористична операція. Стан, ефективність і достатність впроваджених заходів перевірялися, оцінювалися та аналізувалися спеціалістами з питань фізичного захисту Компанії, у т.ч. інспекторами Держатомрегулювання під час перевірок організації забезпечення фізичного захисту та охорони ВП АЕС і об'єктів їх життєзабезпечення.

Відповідно до вимог Закону України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання», «Правил фізичного захисту ядерних установок і ядерних матеріалів» від 04.08.2006 р. № 1000/15691, «Положення про визначення характеристик можливого нападу на ядерні установки та ядерні матеріали, використання цих відомостей у

фізичному захисті» (НП 306.2.08/1.015-99) вживаються такі заходи з фізичного захисту:

• забезпечується безперервність функціонування систем ФЗ АЕС;

• фахівцями Компанії відповідно до рекомендацій МАГАТЕ і з метою підвищення ефективності забезпечення фізичного захисту розроблені, погоджені з компетентними органами і введені в дію об'єктові проектні загрози, на основі яких визначаються основні критерії побудови працездатних систем фізичного захисту АЕС;

• відпрацьовані й погоджені плани взаємодії, реагування і протидії від нападу на АЕС ззовні.

Відповідно до вимог Постанови Кабінету Міністрів України від 25.12.1997 р. №1471 «Про затвердження Порядку проведення спеціальної перевірки для надання допуску фізичним особам до роботи на ядерних установках з ядерними матеріалами, радіоактивними відходами, іншими джерелами іонізуючого випромінювання» здійснюється спеціальна перевірка і надаються допуски до виконання особливих робіт на ядерних установках та з ядерними матеріалами.

Наразі охорону та оборону ядерних установок та ядерних матеріалів здійснюють відповідні військові частини Національної гвардії України. Відповідно до вимог Статуту бойової служби спеціальних частин МВС України, затвердженого урядовою постановою, міжвідомчими комісіями у складі Міненерговугілля, Держатомрегулювання, НГУ, СБУ, ДФЗСБ та ВП АЕС у визначені терміни переглядаються Акти міжвідомчої комісії з організації охорони та оборони АЕС.

Одним із важливих складників забезпечення надійності функціонування системи протидії можливим диверсійним та терористичним виявам щодо атомних електростанцій, а також персоналу АЕС є проведення різнорівневих навчань з перевірки готовності сил і засобів, які залучаються до забезпечення фізичного захисту, протидії диверсіям та антитерористичної захищеності АЕС і об'єктів їх життєзабезпечення.

За результатами навчань з перевірки готовності сил й засобів, які залучаються до забезпечення фізичного захисту, охорони та оборони АЕС, протидії актам ядерного тероризму та диверсіям, проводиться ретельний аналіз, а також напрацьовуються відповідні пропозиції і висновки.

Так, протягом 2015 р. Компанією спільно з ВП АЕС та силами реагування було проведено чотири планових навчання та окремі тренування (спільно з військовими підрозділами з охорони АЕС Національної гвардії України), до участі в яких залучалися сили та засоби СБУ, НГУ, МВС, ДСНС, місцеві органи самоврядування тощо.

Аналіз стану організації, підготовки та результатів проведених навчань демонструє, що ДП «НАЕК «Енергоатом» та ВП АЕС від-

повідально ставляться до організації, проведення навчань і підготовки персоналу до дій у кризових ситуаціях. Результати навчань також свідчать про достатній рівень підготовки персоналу та сил реагування, необхідних для вирішення завдань з запобігання, виявлення, припинення та мінімізації загроз або вчинення диверсій чи терористичних актів щодо ядерних установок та ядерних матеріалів.

Протягом 2014–2015 рр. у ДП «НАЕК «Енергоатом» вживалися заходи в рамках загальнодержавної та відомчої систем боротьби з тероризмом.

Так, на виконання п. 2 Указу Президента України від 25.04.2013 р. № 230 «Про Концепцію боротьби з тероризмом», Розпорядження Кабінету Міністрів України від 11.07.2013 р. № 547-р «Про затвердження плану заходів з реалізації Концепції боротьби з тероризмом» та Наказу Міненерговугілля України від 16 жовтня 2013 року «Про затвердження плану заходів Міністерства енергетики та вугільної промисловості з реалізації Концепції боротьби з тероризмом на підприємствах паливно-енергетичного комплексу на 2013–2020 роки» розроблений та впроваджений у практичну діяльність відповідним Наказом від 29.01.2014 р. «План заходів ДП «НАЕК «Енергоатом» з реалізації Концепції боротьби з тероризмом на атомних електростанціях на 2014–2020 роки».

Крім цього, з метою оперативного керівництва силами і засобами Компанії в разі виявлення або безпосередньої протидії загрозам екстремістського та терористичного характеру та для забезпечення постійної готовності Антитерористичного штабу Компанії Наказом від 12 вересня 2014 р. затверджено новий склад Антитерористичного штабу ДП «НАЕК «Енергоатом».

З метою недопущення можливих протиправних виявів щодо ядерних установок (ЯУ) та ядерних матеріалів (ЯМ) в умовах дестабілізації громадсько-політичної ситуації та проведення антитерористичної операції на сході держави Дирекція з ФЗСБ спільно зі службами фізичного захисту (СФЗ) та антитерористичними штабами (АТШ) ВП АЕС організувала та вживає таких попереджувальних заходів:

• на всіх ВП АЕС організоване чергування оперативних груп з-поміж керівного складу СФЗ, військових частин НГУ з охорони АЕС (в/ч НГУ), загонів відомчої воєнізованої охорони (ЗВВО);

• здійснюється постійний моніторинг обстановки навколо об'єкта, в межах санітарно-захисної зони та в містах – супутниках АЕС;

• проводиться постійний обмін інформацією між СФЗ та регіональними і місцевими правоохоронними органами в містах – супутниках АЕС;

• забезпечується підвищена готовність підлеглих підрозділів (СФЗ, ЗВВО та військових частин) у режимі охорони і забезпечення

безпечної експлуатації атомних станцій відповідно до планів підрозділів;

• посилено пропускний режим на людських і транспортних КПП, за необхідності здійснюється їх блокування;

• обмежено доступ відвідувачів на територію станцій, заборонено проведення екскурсій;

• силами військових частин Національної гвардії України проводиться постійне патрулювання за периметром об'єктів;

• посилено чергування персоналу ЗВВО на об'єктах життєзабезпечення АЕС, забезпечується візуальний контроль за переміщенням осіб і транспортних засобів у безпосередній близькості до забороненої зони периметрів ВП АЕС;

• додатково проаналізовано та внесено відповідні зміни до порядку дій диспетчерів щодо інформування про НС і КС на об'єктах АЕС тощо.

Ведеться постійна робота зі зміцнення та підвищення ефективності взаємодії з центральними органами влади і правоохоронними органами держави, які є суб'єктами державного плану взаємодії на випадок вчинення диверсії щодо ЯУ, ЯМ, інших ДІВ у процесі використання, зберігання або перевезення, а також щодо радіоактивних відходів у процесі поводження з ними.

Зважаючи на наведене, функціонування системи фізичного захисту АЕС Компанії відповідає вимогам чинного законодавства та відомчим нормативним документам.

Завідувач відділу УкрНДІ цивільного захисту ДСНС України **ГРЕЧАНІНОВ Віктор Федорович** підкреслив, що питання, які порушує Зелена книга, є актуальними. Він висловив сподівання, що робота, яка велася в Інституті з опрацювання Зеленої книги, добігає кінця. Доповідач наголосив на необхідності вирішення низки проблемних питань, що пов'язані з організацією захисту критичної інфраструктури в Україні. Першим з них він назвав взаємодію та обмін інформацією між усіма зацікавленими суб'єктами. Це питання, на превеликий жаль, навіть у межах єдиної державної системи цивільного захисту не вирішується повною мірою між її функціональними та територіальними підсистемами. Він зауважив, що розбудова захисту критичної інфраструктури має виходити з реальних ресурсних можливостей, у першу чергу фінансових, як держави, так і власників інфраструктури.

Віктор Гречанінов зауважив, що, незважаючи на наявність багатьох нормативно-законодавчих актів з регулювання окремих питань захисту критичної інфраструктури, ця нормативна база є застарілою, такою, що не відповідає ані нинішнім безпековим загрозам, ані європейській практиці. До того ж норми часто не виконуються. Він наголосив, що запропонований у Зеленій книзі Проект закону «Про критичну інфра-

структуру» має бути комплементарним вдосконаленню законодавчої бази у сфері цивільного захисту, зокрема Кодексу цивільного захисту. За словами Віктора Гречанінова, якщо «законодавчих норм багато, то незрозуміло, якими керуватися».

Як зазначив доповідач, чинна нині єдина державна система цивільного захисту де-факто не враховує небезпеку об'єктів, що перебувають у приватній власності. Ситуацію погіршує практична відсутність моніторингу техногенної безпеки, а без неї неможливо проводити попередження надзвичайних ситуацій, у тому числі на об'єктах, що відносяться до критичної інфраструктури. Також Віктор Гречанінов звернув увагу на проблему розбудови мережі ситуаційних центрів, яка нині практично відсутня. І хоча фінансові обмеження в короткостроковій перспективі не дозволять розбудувати таку мережу, п'ять-шість центрів для секторів критичної інфраструктури мають функціонувати. Можливо, їх потрібно створювати як міжрегіональні.

Заступник директора Департаменту нагляду і контролю Державної служби України з надзвичайних ситуацій **ПОЛІЩУК Тарас Васильович** нагадав присутнім, що питання розроблення такого документа, як Зелена книга із захисту критичної інфраструктури, було внесено до рекомендацій Спільної робочої групи Україна-НАТО з планування на випадок надзвичайних ситуацій у жовтні 2014 року, і відповідно 21 жовтня 2015 року в штаб-квартирі НАТО про здійснену роботу українська делегація зробить повідомлення. Він зазначив, що на ДСНС покладено завдання імплементації директив Севезо, і функціонування об'єктів підвищеної небезпеки розглядається нині в цьому аспекті. На думку Тараса Поліщука, до критичної інфраструктури можуть бути віднесені об'єкти підвищеної небезпеки, що задовольняють критеріям визначення за Директивою Севезо III, водночас потенційно небезпечні об'єкти не мають бути включені до переліку критичної інфраструктури.

Доповідач привернув увагу присутніх на потребу врегулювання питання щодо відповідності повноважень і відповідальності відомств з питань захисту інфраструктури. Він зазначив, що нинішній статус Державної служби України з надзвичайних ситуацій не дає можливості їй повною мірою здійснювати функції відповідального відомства в запропонованих секторах (хімічна промисловість, мережі життєзабезпечення, служби екстреної допомоги та рятування), оскільки низку функцій із забезпечення безпеки в першому з названих секторів мають інші центральні органи виконавчої влади та органи місцевої влади.

Старший науковий співробітник Інституту проблем математичних машин і систем НАНУ **БІЛОКОНЬ Володимир Михайлович** звернув увагу на те, що відповідно до Стратегії сталого розвитку «Україна-2020» організаційно-технічною основою кризового реагування має стати мережа ситуаційних центрів, і питання її вдосконалення є вкрай

актуальним. Зокрема його поступове вирішення можливе шляхом вдосконалення галузевих ситуаційних центрів, наприклад інформаційно-аналітичного центру Мінприроди.

Він також повідомив, що в межах проекту змін до Закону України «Про основні засади (стратегію) державної екологічної політики на період до 2020 року», запропоновано в перелік завдань внести «захист критичної інфраструктури» (доступний http://www.menr.gov.ua/ecopolit). До цього Закону має бути сформований національний план дій, відповідно до якого завдання будуть деталізовані переліком відповідних заходів.

Доповідач підкреслив, що створення організаційної структури з координації захисту критичної інфраструктури в Україні є можливим в ідповідно до виконання євроінтеграційних зобов'язань, і саме такий досвід є в країні. Левова частина першої секції була надана іноземним експертам з країн-членів ЄС та НАТО, а основним стало питання щодо висновків із досвіду впровадження захисту критичної інфраструктури в цих країнах.

Радник з питань кібербезпеки Офісу зв'язку НАТО в Україні **Мустафа АЙДИНЛІ** доповів про досвід організації мережі центрів (команд) реагування на кіберзагрози (*CERT*) у Туреччині. Він нагадав присутнім, що в широкому розумінні кібербезпека є комплексом інструментів управлінського, політичного, технологічного, концептуального та методологічного характеру, стандартів та гарантій безпеки, а також професійної підготовки кадрів, обміну кращою практикою, засобів забезпечення технічного захисту в кіберсередовищі, особливо для критичної інфраструктури. Основними ж завданнями кібербезпеки можуть бути названі: забезпечення цілісності та автентичності даних, можливості доступу до інформації, функціонування інформаційно-телекомунікаційних мереж, забезпечення конфіденційності даних та захист від несанкціонованого доступу, а також забезпечення тривалості та безперервності діяльності компаній, які є операторами критичної інфраструктури.

Доповідач розповів про етапи створення мережі центрів (команд) реагування на кіберзагрози в Туреччині. Створенню загальнодержавного центру реагування на кіберзагрози (травень 2013 р.) передувало рішення уряду (жовтень 2012 р.) про забезпечення та координацію на національному рівні вивчення проблеми кібербезпеки, утворення Ради з кібербезпеки (січень 2013 р.) та ухвалення Національної стратегії кібербезпеки та Плану дій на 2013-2014 роки. До Ради з кібербезпеки входять керівники ключових міністерств і відомств Туреччини.

Мустафа Айдинлі зупинився й на Стратегії кібербезпеки Туреччини. Він визначив основні напрями цього документа: регуляторні заходи; діяльність з проходження нормотворчих процесів; започаткування

на національному рівні структур з реагування на кіберінциденти; підсилення національних можливостей у сфері забезпечення кібербезпеки; освіта, підготовка кадрів, підвищення свідомості щодо кібербезпеки. Ці напрями зв'язані із 29 пунктами (до них входять 95 підпунктів) Плану дій, для яких своєю чергою визначено відповідальні інституції.

Доповідач навів завдання команд реагування на кіберзагрози, розповів про структуру мережі цих команд, що активно розвивається в Туреччині останніми роками. «Національний центр реагування на кібер-інциденти» (*USOM-TR-CERT*), який буде функціонувати в цілодобовому режимі (24/7) та задіяний для реагування на ті загрози, що мають загальнонаціональний масштаб. Під координацією національного центру будуть функціонувати секторальні центри реагування на кібер-інциденти. Останні мають не тільки реагувати на інциденти, а й тісно співпрацювати з організаціями та підприємствами відповідних секторів (критичної інфраструктури). Також інші центри реагування на кіберінциденти організовуються в рамках структур організацій і агентств, що функціонують під координацією секторального центру. Важливою частиною роботи таких центрів є взаємодія з правоохоронними органами та органами правосуддя з питань надання даних (доказів при розслідуванні).

Як зазначив Мустафа Айдинлі, центр реагування на кібер-інциденти в структурі Міністерства оборони Туреччини (*TAF-CERT*) має найбільші потужності та окрему нормативну базу. Цей центр у військовій сфері відповідальний за визначення основних вимог із кібербезпеки, стандартів та правил користування інформаційними системами, проведення сертифікації та аудиту, проведення навчань та тренінгів з кібербезпеки. Поряд з *TAF-CERT* власні команди реагування на кіберзагрози мають Генеральний штаб та штаб-квартири збройних сил, проте вони використовуються задля моніторингу внутрішніх мереж. При виникненні серйозної ситуації (кібератаки) вони звертаються до *TAF-CERT*.

Експерт Центру передового досвіду НАТО з енергетичної безпеки **Ларі Х'ЮЗ** доповів про проблеми забезпечення кібербезпеки критичної енергетичної інфраструктури. Він розпочав свій виступ з прикладів кібератак, що здійснювалися на різні інженерні системи, та наголосив, що подібні атаки можуть бути спрямовані й на об'єкти критичної інфраструктури.

Ларі Х'юз нагадав присутнім про Президентську директиву № 63 (травень 1998 р.), в якій критична інфраструктура визначалася не тільки як фізичні об'єкти, а ще й ті, що мають кіберскладик (віртуальні). Ця принципова особливість підкреслює значущість забезпечення кібербезпеки критичної інфраструктури.

Щодо енергетичного сектору, то доповідач навів порівняння переліків секторів критичної інфраструктури в різних країнах і підкреслив,

що даний сектор присутній у всіх цих переліках. Як правило, до критичної енергетичної інфраструктури відносять нафтопереробні заводи, сховища енергосировини, трубопроводи, об'єкти електрогенерації, передачі та дистрибуції електроенергії.

Розглядаючи критичну інформаційну інфраструктуру, Ларі Х'юз розділив її на інформаційні і телекомунікаційні технології та системи автоматизації й управління промисловими об'єктами. Для першої групи дедалі більшої важливості набувають «розумні мережі» (англ. *Smart Grid* – застосовується для позначення мереж постачання електроенергії, в яких використовуються цифрові комунікаційні технології для виявлення та реагування на локальні зміни у користуванні мережею), а через їх поширеність зростають і ризики кібератак на такі мережі. Для другої групи ключовою проблемою є безпека систем диспетчерського управління та збору даних (англ. *SCADA – Supervisory Control and Data Acquisition*). Доповідач навів декілька схем здійснення кібератак на такі об'єкти, підкреслюючи необхідність забезпечення захисту як програмного та апаратного забезпечення, так і персоналу об'єктів.

Частину своєї доповіді Ларі Х'юз присвятив механізмам забезпечення кіберзахисту на об'єктах критичної інфраструктури. Він звернув увагу на важливість стандартів з кібербезпеки та необхідність їх дотримання під час розроблення, виготовлення та користування обладнанням (таким як автоматизовані системи диспетчерського управління та збору даних).

Заступник начальника відділу перспективного розвитку ПАТ «Укргідроенерго» **ШАПОВАЛОВ Олександр Едуардович** звернув увагу на важливість загальносистемних проблем функціонування Об'єднаної енергетичної системи України. Він зокрема наголосив, що для енергетичних мереж вкрай важливим нині є питання забезпечення безпеки поставок сировини для ТЕС, оскільки брак енергетичної потужності покривається за рахунок теплової електрогенерації. Такий тип взаємозв'язку має бути врахований при аналізі та формуванні механізмів попередження кризових ситуацій, пов'язаних з функціонуванням критичної енергетичної інфраструктури.

Докторант Національної академії державного управління при Президентові України **АНДРЕЄВ Сергій Олександрович** нагадав присутнім, що в новій Стратегії національної безпеки України загрози безпеці критичної інфраструктури вказані як окрема група. Він звернув увагу на саму концепцію захисту критичної інфраструктури, закладену в Зеленій книзі, яка, на його думку, свідчить про технократичний підхід, абсолютизацію матеріальних цінностей на противагу людиноцентричному підходу, який має домінувати в концепції національної безпеки. Він підкреслив, що нині постає питання, чи має захист критичної інфраструктури виокремлюватися як самостійний напрям державної по-

літики в безпековій сфері, чи комплекс заходів із захисту критичної інфраструктури має стати складовою частиною забезпечення енергетичної, техногенної, інформаційної безпеки тощо.

На думку Сергія Андреєва, комплекс заходів із захисту критичної інфраструктури міг би здійснюватися в межах цивільної оборони в Україні, у тісному зв'язку із заходами щодо територіальної оборони та мобілізаційної підготовки. Але зважаючи на той факт, що систему цивільної оборони ліквідовано, а державну систему цивільного захисту фактично ще не створено, завдання захисту критичної інфраструктури вирішити неможливо. Також Сергій Андреєв наголосив на тому, що досягнення завдань захисту критичної інфраструктури вимагає підготовки, навчання кваліфікованих кадрів у сфері національної безпеки.

Зміст

Content

Наукове видання

ЗЕЛЕНА КНИГА З ПИТАНЬ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

Збірник матеріалів міжнародних експертних нарад

Літературний редактор: *О. В. Москаленко*
Комп'ютерне верстання: *О. І. Сабадаш, І. О. Коваль*
Відповідальна за випуск: *О. М. Романова*

Оригіналмакет підготовлено
в Національному інституті стратегічних досліджень:
вул. Пирогова, 7а, Київ-30, 01030
Тел/факс: (044) 234-50-07
email: infoniss@niss.gov.ua

Формат 60х84/16. Ум. друк. арк. 10,23.
Наклад 200 пр. Зам. № ДФ421

ПП «Фенікс»
03680, м. Київ, вул. Шутова, 13-Б
Тел./факс: (044) 501-93-01