Дмитро Бірюков

КОНЦЕПЦІЯ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЯК ЕЛЕМЕНТ ЗАГАЛЬНОЄВРОПЕЙСЬКОЇ БЕЗПЕКОВОЇ ПОЛІТИКИ

У роботі досліджується роль концепції захисту критичної інфраструктури в системі забезпечення національної безпеки країн ЄС. Представлено короткий огляд етапів імплементації даної концепції в нормативно-правових документах ЄС та

охарактеризовані основні чинники та тенденції, що спричиняють загрози для об'єктів критичної інфраструктури в країнах ЄС.

Ключові слова: *Європейський Союз (ЄС) регіональна безпека, критична інфраструктура (КІ).*

Dmytro Biriukov. Concept of Critical Infrastructure Protection as a component of common European security policy. *In this paper we investigate the role of the concept of critical infrastructure protection in European security policy. A brief overview of implementation stages of this concept in the EU legislation is presented. Also we describe major factors and trends that cause threats to critical infrastructure in the EU.*

Keywords: *European Union, regional security, critical infrastructure.*

На сьогодні високий ступінь впровадження новітніх технологій є ознакою рівня розвиненості країни, визначальним чинником її економічної конкурентоспроможності, а отже, і необхідною умовою для досягнення цілей, які визначаються національними інтересами. В той же час, поряд з багатьма перевагами технологічний прогрес утворив умови безпрецедентної залежності як окремої людини, так і суспільства від систем, що надають інформаційні, комунікаційні, транспортні, енергетичні, фінансові та інші послуги. З руйнуванням таких систем на сьогодні пов'язують найбільш небезпечні безпекові сценарії для провідних держав світу, зокрема для країн ЄС. Тому, зважаючи на обмеженість ресурсів, об'єктивну неможливість забезпечити абсолютний захист і безпеку всіх інфраструктурних систем, в багатьох країнах світу імплементується концепція критичної інфраструктури (КІ), що дозволяє сконцентрувати увагу на системах, мережах та окремих об'єктах, знищення або порушення роботи яких матиме найсерйозніші негативні наслідки для національної безпеки цих країн [1;2].

На початку двотисячних років у наукових роботах почали наголошувати на необхідності подальшого розвитку механізмів захисту європейської КІ на основі трансатлантичних взаємовідносин в економічній та безпековій сферах [3]. На той час у Сполучених Штатах уже були скоєні безпрецедентні терористичні акти, і у відповідь на них прийняті законодавчі акти, в яких захист КІ від терористичних загроз визначався як одне з основних завдань системи захисту національної безпеки.

В ЄС створення правових та організаційних механізмів захисту КІ було ініційовано в 2004р. у зверненні Європейської ради до Європейської комісії (ЄК), в якому ЄК доручалося підготувати загальну стратегію захисту КІ. В жовтні 2004 р. ЄК оприлюднила офіційне повідомлення [4], яке містило як огляд дій ЄК у цій сфері, так і пропозиції щодо додаткових заходів заради вдосконалення європейської системи запобігання, готовності та реагування на терористичні атаки спрямовані проти елементів КІ. У згаданому повідомленні зазначається, що через значну кількість об'єктів, які потенційно можуть бути віднесені до КІ, забезпечити їх захист на загальноєвропейському рівні неможливо, тому дотримуючись принципу субсидіарності, загальноєвропейським інституціям потрібно сконцентрувати зусилля на захисті тих об'єктів, припинення функціонування яких буде мати транскордонний вплив, залишивши за країнами ЄС відповідальність за решту об'єктів. В той же час, як наголошується в даному повідомленні, підхід до захисту КІ у всіх країнах ЄС повинен бути методологічно близьким. В офіційному повідомленні №786 за 2006р [5]. ЄК рекомендувала всім країнам ЄС вжити таких заходів:

- розробити національну програму захисту КІ;
- забезпечувати такий рівень охорони здоров'я, технологічної безпеки, соціально-економічного благополуччя, який би гарантував «стійкість» нації до загроз;
- уніфікувати зусилля, спрямовані на захист КІ, надавши єдиному державному органу, що звітує з цього питання, функції координації дій державних органів влади, що відповідають за окремі галузі промисловості, до яких належать об'єкти КІ;
- визначити органи державної влади, відповідальні за сектори КІ, та відповідні приватні компанії;
- створити умови для ефективної взаємодії та обміну інформацією, даними і досвідом між країнами-членами ЄС, урядовими структурами та приватним сектором;
- зробити внесок у створення гармонізованої методології аналізу ризиків.

Встановлення критеріїв та визначення показників, за якими певні інфраструктури або їх елементи можна віднести до КІ, є окремим питанням для вивчення. Пропозиції щодо процедури та

критеріїв визначення об'єктів КІ на загальноєвропейському рівні були представлені в Зеленій книзі (2005р.) [6]. В ній розглядалося 11 секторів КІ, в які було включено 37 підсекторів. Надалі, під час підготовки проекту директиви, були внесені цих 11 секторів із 29 підсекторами [7], а вже в ухваленій директиві ЄК [8] згадується тільки два сектори енергетика та транспорт.

Елементи всередині КІ, у свою чергу, також можуть бути впорядковані за значимістю. Наприклад, у Швейцарії найвище значення надано двом підсекторам енергетики (постачання газу та електроенергії), банківським установам, інформаційним технологіям і телекомунікаціям, залізничному транспорту та автомобільним шляхам, а також мережі постачання питної води [9].

Визначення категорій об'єктів КІ дозволяє встановити диференційовані вимоги до гарантування безпеки цих об'єктів з урахуванням, зокрема, ступеня потенційної небезпеки здійснення акту незаконного втручання або теракту і його можливих наслідків.

Функціонування КІ пов'язується із підтримуванням життєво важливих функцій у суспільстві, захистом базових потреб і гарантуванням відчуття безпеки і захищеності у населення. Наприклад, у Норвегії це питання було порушено в звіті урядової комісії, яку очолював екс-прем'єр-міністр Коре Віллок. Серед нових викликів, пов'язаних з безпекою суспільства, були, зокрема, названі технологічні зміни, підвищення економічної ефективності та тиску, зниження повноти державних послуг і аутсорсинг державних послуг для комерційних підприємств [10; 11]. Ці проблеми, поряд з появою «нових» загроз, таких як тероризм, організована злочинність і кліматичні зміни принципово змінили контекст для відомств та спеціалізованих служб, відповідальних за підтримку та захист КІ.

Терористичні акти, скоєні в європейських країнах у 2000-х рр., показали, що навіть за наявності розгалуженої системи протидії тероризму, на їх території існує значний терористичний ризик. Аналіз офіційного звіту, складеного після теракту в Лондоні (липень 2005р.), свідчить, що інфраструктурні об'єкти та місця масового скупчення людей є дуже вразливими до терористичних загроз [12].

Інша група загроз – природного характеру, як свідчить статистика міжнародної бази даних з надзвичайних ситуацій [13], характеризується тенденцією до зростання чисельності стихійних

метеорологічних явищ та розміру їх наслідків для країн ЄС. Тому все більше уваги приділяється дослідженням стійкості електроенергетичних мереж, які вважаються найбільш вразливими до кліматичних чинників. Небезпечність стихійних лих та кліматичних чинників викликана одночасним впливом на різні об'єкти і, навіть, сектори КІ, виникненні аварій через так звані відмови із загальної причини, або каскадний вплив таких відмов [14].

Масштабні аварії в електроенергетичних мережах демонструють щільний взаємозв'язок між різними секторами КІ, різноманітні прояви ефекту каскадних відмов. Наприклад, «затемнення» в Італії, що відбулося у вересні 2003 р., призвело до перебоїв у функціонуванні залізничного транспорту, служб та установ надання медичної допомоги населенню, фінансових електронних сервісів, і, взагалі, усіх телекомунікаційних мереж [15].

Не викликає сумніву те, що *серед техногенних загроз для КІ особливу небезпеку становлять кіберзагрози*. Кібератак через мережу Інтернет зазнають сервери державних установ, великих компаній, фінансових установ. Новітньою тенденцією стали кібератаки на промислові системи автоматизованого управління технологічними процесами [16].

Слід відзначити, що *в ЄС виділяються значні кошти на проведення науково-дослідних проектів з тематики захисту КІ.* У вище згаданому робочому документі апарату ЄК наводяться дані про виконання понад сотні науково-дослідних проектів на загальну суму в 45 млн. євро [17]. Загрози для об'єктів КІ оцінюються із застосуванням різноманітних методик та прикладного програмного забезпечення, в основі яких лежить загальна методологія оцінки ризиків, причому ключовою особливістю оцінки ризиків для КІ є врахування численних взаємозв'язків та залежностей. Про це свідчить звіт Інституту захисту та безпеки громадян (входить до складу Об'єднаного дослідницького центру ЄК) [18].

Захист КІ потребує партнерської взаємодії між власниками та операторами КІ, з одного боку, та урядовими структурами країн ЄС з іншого. В офіційному повідомленні ЄК зазначається, що «посилення відповідних заходів безпеки органами державної влади, пов'язаних з хвилею атак, які спрямовані проти суспільства в цілому, а не проти окремих діючих гравців промисловості, мають

бути здійснені за рахунок держави» [19]. Тобто, на державу покладається фундаментальна роль щодо захисту КІ. В той же час відповідальність за управління ризиком пов'язаним із промисловими об'єктами, системою поставок, інформаційними технологіями та комунікаційними мережами лягає на власників та операторів об'єктів КІ. Тому інформаційні попередження, консультативні та дорадчі матеріали повинні бути доступні та допомагати громадськості й приватному сектору в захисті ключових систем інфраструктури.

Водночас забезпечення безпеки та надійності функціонування вимагає значних фінансових витрат, а прийняття рішень щодо таких інвестицій здійснюється на основі ретельного економічного аналізу в розрізі «витрати-вигоди». Як показують дослідження, компанії, що працюють в телекомунікаційному секторі КІ, приділяють значно більше уваги здатності технічних систем впорюватися з відмовами (аваріями), що характеризуються високою ймовірністю настання але низьким рівнем втрат, в той же час як аваріям, що характеризуються низькою ймовірністю настання та вкрай високим рівнем наслідків приділяється менше уваги і ресурсів [20]. Використання такого підходу пояснюється намаганнями компаній створити для себе ринкові переваги (за показником якості послуг) хоча б в середньо терміновій перспективі, залишаючись привабливими для інвесторів.

Необхідно також відмітити, що розбудова КІ неминуче пов'язана з економічною конкуренцією, лобіюванням та політичним тиском. Показовим є приклад протидії впровадженню європейської супутникової системи позиціонування Галілео з боку урядових кіл Сполучених Штатів (заступник міністра оборони США Пол Вольфовіц у грудні 2001 р. надіслав лист 15 міністрам оборони країн ЄС, у якому наводив аргументи проти створення Галілео), які усвідомлювали, що Галілео створюється як альтернатива, що може витіснути американську Глобальну систему позиціонування [21].

Для України може бути корисним *досвід імплементації концепції захисту КІ в законодавствах деяких східноєвропейських країн*. Наприклад, в нормативно-правовій базі Республіки Польща введено термін «захист критичної інфраструктури», під яким розу-

міються всі «зусилля, спрямовані на забезпечення функціональності, неперервності та цілісності критично важливих об'єктів інфраструктури в цілях запобігання загрозам, ризикам і вразливості та обмеження, а також нейтралізації їх наслідків і швидкого оновлення інфраструктури у випадку відмов, атак та інших випадків, що порушують її належне функціонування»[22] .

Подібна ж ситуація спостерігається у нормативно-правовій базі Словацької Республіки, де в 2007 р. уряд ухвалив «Концепцію критичної інфраструктури в Словацькій Республіці, її захисту та оборони» [23], а на її основі в 2008 р. була розроблена «Національна програма захисту та оборони критичної інфраструктури»[24]. Ці документи визначають загальні (концептуальні) характеристики стратегії захисту КІ, але не надають детального опису заходів з її здійснення.

У законодавстві Республіки Болгарії термін «критична інфраструктура» подано в Законі «Про захист від стихійних лих» (жовтень 2011р.): «критична інфраструктура» є системою або їх частиною, яка необхідна для підтримки життєво важливих соціальних функцій, здоров'я, безпеки, економічного чи соціального добробуту населення, її руйнування або знищення матиме серйозний негативний вплив та спричинить для Болгарії нездатність підтримувати такі функції. Прийнята постанова Ради Міністрів «Про порядок, спосіб та компетентні органи для визначення критичної інфраструктури та об'єктів і оцінки ризиків» (жовтень 2012р.) [25]. Також діють нормативні документи, що регламентують порядок взаємодії між окремими відомствами щодо питань захисту критичної інфраструктури (див., наприклад, інструкцію) [26]. Відповідно до положень директиви ЄК №114 2008р. Рада Міністрів Республіки Болгарія прийняла постанову, в якій визначається порядок визначення об'єктів критичної інфраструктури в двох секторах (енергетика та транспорт) та заходів з їх захисту.

Таким чином, на сьогодні концепція захисту критичної інфраструктури імплементована як в загальноєвропейському законодавстві, так і в національних законодавствах окремих країн-членів ЄС. Загальноєвропейською критичною інфраструктурою вважається та, що має транскордонне, в межах ЄС, значення. Нині лише два сектори (енергетика та транспорт) визначені як пріоритетні на загальноєвропейському рівні.

Україна за своїм географічним положенням є частиною енергетичного та транспортного панєвропейського простору, а, отже, де-факто пов'язана з європейською критичною інфраструктурою, що відкриває можливості для діалогу з питань безпеки критичної інфраструктури між вповноваженими органами влади України та країн європейських сусідок України.

---

1. *CEPS* task force report: Protecting critical infrastructure in the EU / B.Hammerly, A.Renda. – Brussels: Centre for European policy studies, 2010. – 100 p.

2. *Critical infrastructure* protection at the European level [Електронний ресурс]// Studia diplomatica. – 2011. – LXIV-1. – Режим доступу: http://www.nonproliferation.eu/

3. *Lembke J.,* EU critical infrastructure and security policy / European economic and political issues. – Vol.6. – Nova Science Publishers Inc., 2002. – P. 49 – 79.

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

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

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

7. *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/

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

9. *Brem S.,* Developing a national CIP strategy: Swiss experiences and results // European CIIP Newsletter. – 2009. – Vol.5, No.2. – P. 13 – 15.

10. *Protection* of critical infrastructures and critical societal functions in Norway [Електронний ресурс] // Report NOU 2006:6 submitted to the Ministry of Justice and the Police by the government appointed commission for

the protection of critical infrastructure on 5th of April 2006. – Режим доступу: http://www.regjeringen.no/

11. *Report* into the London terrorist attacks on 7 July 2005. Presented to Parliament by the Prime Minister / Intelligence and Security Committee, 2006.

12. *EM-DAT :* The OFDA/CRED International Disaster Database / Université Catholique de Louvain, Брюссель, Бельгія. – [Електронний ресурс]. – Режим доступу: www.emdat.be

13. *Rubbelke D., Vogele S.,* Impacts of climate change on European critical infrastructures: The case of the power sector // Environmental science and policy. – 14. – 2011. – P. 53 – 63.

14. *Modelling* interdependent infrastructures using interacting dynamical models / Rosato V., Issacharoff, L., Tiriticco, F., Meloni, S., Porcellinis, S.D., Setola, R. // Int. J. of Critical Infrastructures. – 2008. – 4. – P. 63 – 79.

15. *International* CIIP Handbook / Edt. Wenger A., Metzger J., Dunn M. – Zurich: Swiss Federal Institute of Technology, 2012. – 218 p.

16. *SWD(2013) 318 final:* On a new approach to the European Programme for Critical Infrastructure Protection. Making European Critical Infrastructures more secure [Електронний ресурс]. – EC staff working document. – Режим доступу. – http://ec.europa.eu

17. *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.

18. *Communication* from the Commission to the European Parliament and the Council – The repercussions of the terrorist attacks in the United States on the air transport industry (COM/2001/574 final). – [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/

19. *Protection* of critical infrastructures and critical societal functions in Norway [Електронний ресурс] // Report NOU 2006:6 submitted to the Ministry of Justice and the Police by the government appointed commission for the protection of critical infrastructure on 5th of April 2006. – Режим доступу: http://www.regjeringen.no/

20. *Tanner J.C.,* Galileo is go, despite Pentagon pressure – First Mile – Brief Article // Telecom Asia, 31 May, 2012 [Електронний ресурс]. – Режим доступу: http://findarticles.com/p/articles/mi_m0FGI/is_5_13/ai_86827056/

21. *Act* of 26 April 2007 on Crisis Management. – Пер. англ. мовою [Електронний ресурс]. – Веб-сайт Урядового центру з питань безпеки, Республіки Польщі. – Режим доступу: http://rcb.gov.pl/eng/wp-content/uploads/2011/03/ACT-on-Crisis-Management-final-version-31-12-2010.pdf

22. *Koncepcia* kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany [Електронний ресурс]. – Веб-сайт Міністерства внутрішніх справ Республіки Словаччина. – Режим доступу: http://www.minv.sk/?ochrana-kritickej-infrastruktury&subor=10691

23. *Národný* program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike [Електронний ресурс]. – Веб-сайт Міністерства внутрішніх справ Республіки Словаччина. – Режим доступу: http://www.minv.sk/?ochrana-kritickej-infrastruktury&subor=10692

24. *Наредба* за реда, начина и компетентните органи за установяване на критичните инфраструктури и обектите им и оценка на риска за тях [Електронний ресурс]. – Българският правен портал. – Режим доступу: http://www.lex.bg/bg/mobile/ldoc/2135816878

25. *Инструкция* № М-3 от 18.06.2011 г. «За взаимодействие между министерството на отбраната и министерството на вътрешните работи» // Издадена от Министерството на отбраната и Министерството на вътрешните работи (Обн. ДВ. бр.60 от 5 Август 2011г.) [Електронний ресурс]. – Българският правен портал. – Режим доступу: http://www.lex.bg/bg/laws/ldoc/2135744408

26. *Постановление* №18 от 01.02.2011 г. «За установяването и означаването на европейски критични инфраструктури в република България и мерки за тяхната защита» [Електронний ресурс]. – Българският правен портал. – Режим доступу: http://www.lex.bg/-bg/laws/ldoc/2135716127