УДК 004.056 (045)

С. О. ГНАТЮК, М. О. РЯБИЙ, В. М. ЛЯДОВСЬКА

ВИЗНАЧЕННЯ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ТА ЇЇ ЗАХИСТУ: АНАЛІЗ ПІДХОДІВ

Запропоновано аналітичне дослідження нормативно-правової бази розвинених держав світу щодо варіацій ключових понять у галузі захисту критичної інформаційної інфраструктури. У результаті аналізу виявлено як спільні, так і відмінні особливості підходів до визначення критичної інфраструктури (та інших суміжних понять) низки держав, а також окреслено вітчизняні проблеми в цій галузі. Здобуті результати будуть корисні при проведенні багатокритеріального аналізу зазначених дефініцій і допоможуть у розробці методик віднесення тих чи інших об'єктів до критичної інформаційної інфраструктури.

Ключові слова: інформаційна безпека держави; дефініція; концепція; критична інфраструктура; захист критичної інформаційної інфраструктури.

Вступ

Сучасне суспільство повністю залежить від інформаційно-комунікаційних систем і мереж, відмова яких може призвести до хаосу, величезних фінансових збитків і навіть до масової загибелі людей. Щоправда, більша частина людства схильна сприймати найважливіші послуги (зокрема, їхню якість) як належне. І так триває доти, доки щось або хтось не порушить роботу згаданих систем. Для визначення й узагальнення найважливіших та найуразливіших активів держави до міжнародного законодавства було впроваджено термін ***критична інфраструктура***. Транспортні та енергетичні мережі, нафто- та газопроводи, урядові та військові об'єкти — усе це надважливі компоненти діяльності сучасного суспільства. Проте останнім часом особливо актуалізувалося питання забезпечення безпеки зазначених об'єктів і захисту критичної інфраструктури в цілому.

Аналіз відомих досліджень і постановка завдання

Поняття ***критична інфраструктура*** почали активно вживати у другій половині 1990-х років переважно стосовно розподілених великомасштабних інформаційних систем (центрів обробки даних, об'єднаних комунікаційних мереж тощо) [1]. Більшість розвинених держав самостійно робили спроби дати визначення критичної інфраструктури та розробити стратегію її захисту. Згідно з [2] перелік життєво важливих (критичних) інфраструктур різний для окремих держав і визначається відповідно до їхніх традицій, суспільних та політичних переконань, а також географічних та історичних особливостей кожної держави. Важливим компонентом критичної інфраструктури є її інформаційна складова — ***критична інформаційна інфраструктура***, концепцію захисту якої, уперше розроблену в США, згодом було розвинено й адаптовано в більшості розвинених держав світу [1–4].

Аналіз вітчизняної нормативної бази показує, що галузь захисту критичної інформаційної інфраструктури в нашій державі перебуває на початковому етапі формування. І хоча чинним законодавством України й визначено окремі об'єкти вітчизняної соціально-економічної сфери, на яких надзвичайні події можуть призвести до суспільно небезпечних наслідків, усе ж вони не становлять єдиної системи [3]. Окрім того, немає чітко визначеної понятійно-термінологічної основи в цій галузі, а це, у свою чергу, гальмує інтеграцію нашої держави у світовий інформаційний простір.

З огляду на сказане ***мета статті*** — дослідження нормативно-правової бази розвинених держав світу щодо відмінностей ключових понять у галузі захисту критичної інформаційної інфраструктури.

Основна частина дослідження

Як показує світова практика, становлення нормативно-правової бази в галузі захисту критичної інфраструктури — процес тривалий. На підтвердження пріоритетної уваги політичного керівництва різних держав до зазначеної проблематики достатньо навести стислий перелік основних документів [4; 5]:

- ♦ адміністративні накази Президента США № 13010 «Про роботу з дослідження вразливості захисту критичної інфраструктури від кібернетичних і фізичних загроз» (липень 1996 р.); № 13228 «Організація захисту США від терористичних загроз» (жовтень 2001 р.) та № 13231 «Про захист національних критичних інформаційних систем» (жовтень 2001 р.);
- ♦ стратегії національної безпеки США (липень 2002 р. та березень 2010 р.);
- ♦ Національна стратегія захисту критичної інфраструктури та основних фондів США (лютий 2003 р.);
- ♦ Директива Президента США з національної безпеки № 7 (грудень 2003 р.);

♦ плани захисту національної інфраструктури США (жовтень 2006 р. та жовтень 2009 р.);

♦ Політика у сфері кіберпростору США (2009 р.);

♦ Концепція критичної інфраструктури у Словацькій Республіці, її захисту та оборони (2007 р.);

♦ Національна програма захисту та оборони критичної інфраструктури Словацької Республіки (2008 р.);

♦ Програма захисту національної критичної інфраструктури Угорщини (2008 р.);

♦ Постанова Ради Міністрів Республіки Болгарія «Про порядок, спосіб та компетентні органи для визначення критичної інфраструктури та об'єктів і оцінки ризиків» (жовтень 2012 р.);

♦ Основи державної політики у сфері забезпечення безпеки населення Російської Федерації та захищеності критично важливих і потенційно небезпечних об'єктів від загроз техногенного, природного характеру й терористичних актів (вересень 2006 р.);

♦ Концепція федеральної системи моніторингу критично важливих, потенційно небезпечних об'єктів і вантажів Російської Федерації (серпень 2005 р.);

♦ Методика віднесення об'єктів державної та недержавної власності до критично важливих об'єктів для національної безпеки Російської Федерації (жовтень 2012 р.).

Аналізуючи зазначені документи, доходимо висновку про пильну увагу світової спільноти до захисту як критичної інфраструктури загалом, так і критичної інформаційної інфраструктури зокрема. При цьому помічаємо неузгодженість тих чи інших положень законодавства різних держав із питань захисту критичних інфраструктур, недосконалість механізмів віднесення об'єктів (оцінювання їхньої критичності) до критичної інфраструктури та інші проблеми. Таким чином, кожна держава визначає власну критичну інфраструктуру з погляду критичності окремих секторів або важливості певних послуг для економіки держави та безпеки її суспільства.

На основі аналізу джерел [2–7] складено табл. 1, де наведено різні визначення критичної інфраструктури.

Отже, як випливає з табл. 1, термін «критична інфраструктура» не має сталого тлумачення і кожна держава вкладає у нього свій зміст

Таблиця 1

Варіації дефініцій поняття *критична інфраструктура*

№ з/п	Держава	Визначення
1	Австралія	Фізичні об'єкти, інформаційні технології, комунікаційні мережі, ланцюжки постачань, які в разі знищення, модифікації або недоступності протягом тривалого часу матимуть істотний вплив на соціальне чи економічне благополуччя нації або негативно позначаться на здатності забезпечувати національну оборону Австралії та гарантувати її національну безпеку
2	Австрія	Природні ресурси, послуги, інформаційні технології, мережі, а також інші активи, які в разі порушення або руйнування можуть серйозно вплинути на здоров'я, безпеку, економічний добробут громадян або ефективне функціонування уряду
3	Великобританія	Активи, послуги та системи, що підтримують економічне, політичне й соціальне життя Великобританії, втрата яких може: 1) викликати масштабну загибель людей; 2) відчутно вплинути на національну економіку; 3) призвести до інших серйозних соціальних наслідків; 4) перетворитись на одне з невідкладних завдань національного уряду
4	Ізраїль	Інфраструктура, порушення функціонування якої може призвести до значних соціально-економічних потрясінь, здатних підірвати стабільність у суспільстві і тим самим призвести до реалізації загроз національній безпеці країни
5	Канада	Фізичні та інформаційно-технічні засоби, мережі, послуги й активи, які в разі порушення або руйнування матимуть серйозний вплив на здоров'я, безпеку економічного добробуту канадійців або ефективне функціонування уряду Канади
6	Нідерланди	Продукти, послуги та супровідні процеси, які в разі порушення або відмови, можуть викликати серйозні соціальні негаразди — величезні жертви або серйозні економічні збитки
7	Німеччина	Організації та об'єкти, які мають настільки важливе суспільне значення, що їх відмова або знецінення може викликати стійкий дефіцит постачання, істотні порушення громадського порядку або інші драматичні наслідки
8	Норвегія	Конструкції та системи, необхідні для підтримання найважливіших функцій суспільства, постійна доступність яких гарантує кожному члену суспільства почуття власної та громадської безпеки
9	Росія	Об'єкти, порушення (або припинення) функціонування яких призводить до втрати управління, руйнування інфраструктури, незворотних негативних змін або руйнування економіки країни (деякого суб'єкта, адміністративно-територіальної одиниці) чи до суттєвого погіршення безпеки життєдіяльності населення, що мешкає на цих територіях, на тривалий час

Закінчення табл. 1

№ з/п	Держава	Визначення
10	США	Системи та об'єкти, фізичні чи віртуальні, які настільки важливі для держави, що їх недієздатність або знищення підриває національну безпеку, економіку, здоров'я чи безпеку населення або призводить до наслідків, що поєднують у собі всі зазначені негативи
11	Хорватія	Діяльність, мережі, послуги, матеріальні блага та інформаційні технології, вихід із ладу або знищення яких значно вплинули б на здоров'я та безпеку громадян або на діяльність державної влади
12	Швейцарія	Інфраструктура, порушення, відмова або руйнування якої може істотно вплинути на здоров'я населення, громадські справи, навколишнє середовище, безпеку та соціально-економічне благополуччя
13	Японія	Об'єкти інфраструктури, формування яких покладається на суб'єктів господарювання і які надають настільки незамінні послуги, що зниження їхньої ефективності або недоступність може мати важливе значення для соціального життя та економічної діяльності людей

і власну специфіку. Це пояснюється тим, що національні потреби й проблеми істотно різняться залежно від регіону, рівня розвитку держави та інших специфічних чинників. Саме ці чинники і є основною перешкодою на шляху стандартизації (на міжнародному рівні) у галузі захисту критичної інфраструктури. І все ж у розмаїтті дефініцій простежується спільна риса критичної інфраструктури різних держав світу, а саме: її ключове значення для безпеки громадян, суспільства й держави. Згідно з табл. 1 критична інформаційна інфраструктура розглядається як центральний компонент у критичній інфраструктурі різних держав (Австралії, Австрії, Канади, США та Хорватії), що знаходить відображення у відповідних визначеннях цього поняття. Головні причини критичності інформаційної складової інфраструктури випливають зі стрімкого поширення інформаційних технологій у всіх сферах людської діяльності, що призводить до залежності від них громадян, суспільства й держави, а також до посилення уразливостей і потенційних загроз різного характеру. Визначення критичної інформаційної інфраструктури, що спираються на концепції та політику різних держав світу [2–5], наведено в табл. 2.

Відсутність поняття «критична інформаційна інфраструктура» у законодавстві деяких держав можна пояснити тим, що інформаційна складова входить до обсягу поняття інфраструктури взагалі (тобто критичної інфраструктури) і не виокремлюється як певна ланка. Слід, проте, зазначити, що в тлумаченні цього терміна в різних державах простежується чітка аналогія. Наприклад, Австралія,

Таблиця 2

Варіації дефініцій поняття *критична інформаційна інфраструктура*

№ з/п	Держава	Визначення
1	Великобританія	Активи, послуги та системи, які підтримують економічне, політичне й соціальне життя Великобританії і мають настільки велике значення, що будь-яка часткова або повна їх втрата може призвести до великомасштабної загибелі людей; мати серйозний вплив на національну економіку; інші серйозні соціальні наслідки для суспільства чи значної частини спільноти або призвести до появи невідкладних завдань у національному уряді
2	Естонія	Інформаційні та комунікаційні системи, підтримка, надійність і безпека яких має важливе значення для нормального функціонування країни
3	Індія	Комп'ютерні ресурси, виведення з ладу або руйнування яких може завдати шкоди національній безпеці, економіці та охороні здоров'я
4	Корея	Системи управління інформацією або інформаційно-комунікаційні мережі в державних і приватних установах, які в разі скоєння у них кіберзлочинів можуть серйозно вплинути на національну безпеку, повсякденне життя громадян, національну економічну стабільність
5	Малайзія	Сукупність активів (реальних і віртуальних), систем і функцій, які мають життєво важливе значення для нації і недієздатність чи знищення яких може мати серйозний вплив на національну економіку, імідж, оборону та безпеку, можливість виконання урядом своїх функцій, а також на суспільну охорону здоров'я й безпеку
6	Нідерланди	Інформаційні системи (програмне забезпечення, апаратні засоби й дані), які підтримують один або кілька найважливіших об'єктів інфраструктури, порушення роботи або відімкнення яких може завдати серйозної шкоди функціонуванню залежної критичної інфраструктури
7	Росія	Сукупність автоматизованих систем управління критично важливими об'єктами, що забезпечують взаємодію інформаційно-телекомунікаційних мереж, призначених для розв'язання завдань державного управління, гарантування обороноздатності, безпеки та правопорядку, порушення (або припинення) функціонування яких може призвести до тяжких наслідків

Канада, Нідерланди, Великобританія і США виробили спільний погляд на критичну інформаційну інфраструктуру як «інформаційні системи (програмне забезпечення, апаратні засоби й дані) та послуги, які підтримують один чи кілька найважливіших об'єктів інфраструктури, порушення роботи або відімкнення яких завдає серйозної шкоди функціонуванню залежної критичної інфраструктури» [2]. Окрім того, у деяких державах (наприклад, Малайзії) особливо акцентується значення критичної інфраструктури для нації, навіть і саме поняття «критична інформаційна інфраструктура» вживається в розумінні «критична національна інформаційна інфраструктура».

З огляду на те, що в кожному з наведених визначень особлива увага приділяється питанню національної безпеки, ідеться про впровадження нового важливого напрямку політики — захист критичної інфраструктури держави.

Узявши до відома досвід деяких розвинених держав, можна розкрити зміст терміна ***захист критичної інфраструктури*** докладніше за допомогою таких визначень:

♦ усі зусилля, спрямовані на забезпечення функціональності, безперервності та цілісності критично важливих об'єктів інфраструктури з метою запобігання загрозам, ризикам і уразливості, а також для нейтралізації їх наслідків і швидкого оновлення інфраструктури в разі відмов, атак та інших випадків, що порушують її належне функціонування (законодавство Польщі) [4];

♦ концепція, яка стосується готовності та реагування на серйозні інциденти, пов'язані з критичною інфраструктурою регіону або нації (словник Wikipedia) [8];

♦ захист комунікаційних чи інформаційних послуг, доступність, надійність і стійкість яких мають важливе значення для функціонування сучасної (національної) економіки, безпеки та інших важливих соціальних цінностей (законодавство США) [9];

♦ можливість підготовки до захисту, пом'якшення впливу, реагування і відновлення критичної інфраструктури в разі виникнення перебоїв або знищення (законодавство ЄС) [10].

Отже, усі зазначені держави сформулювали політику (концепцію) і розробили практичні рекомендації для захисту об'єктів критичної інфраструктури, приділивши особливу увагу інформаційним системам і мережам. З огляду на це варто виокремити поняття ***захист критичної інформаційної інфраструктури***. Це згідно з [10] «програми та заходи інфраструктур, власники, оператори, виробники, користувачі і регулюючі органи яких спрямовані на збереження виконання функцій найважливіших інформаційних інфраструктур у випадку аварій, нападів або нещасних випадків, що перевищують установлений мінімальний рівень послуг і спрямовані на мінімізацію часу відновлення і пошкодження».

У законодавстві України немає поняття «захисту критичної інфраструктури» та «захисту критичної інформаційної інфраструктури», а вказано лиш об'єкти окремих галузей [3], що потребують захисту з боку держави — об'єкти нафтогазової галузі (розпорядження КМУ від 27.05.2009 р. № 578-р), об'єкти, які мають стратегічне значення для економіки та безпеки держави (постанова КМУ від 10.08.1993 № 615) та об'єкти, що становлять підвищену екологічну небезпеку (постанова КМУ від 27.07.1995 № 554).

Висновки

Здійснено аналітичне дослідження нормативно-правової бази розвинених держав світу щодо різних варіацій ключових понять у галузі захисту критичної інформаційної інфраструктури, таких як ***критична інфраструктура***, ***критична інформаційна інфраструктура***, ***захист критичної інфраструктури***, ***захист критичної інформаційної інфраструктури***.

У результаті аналізу нормативних документів і наукових джерел було виявлено спільні та відмінні риси в підходах до визначення критичної інфраструктури різних держав, а також наголошено на вітчизняних проблемах у цій галузі. Здобуті результати будуть корисні при проведенні багатокритеріального аналізу зазначених дефініцій, а також у процесі розробки методик віднесення певних об'єктів до критичної інформаційної інфраструктури.

Література

1. Гнатюк, С. О. *Критерії визначення елементів критичної інфраструктури держави / С. О. Гнатюк, В. М. Лядовська // «Інноваційний потенціал світової науки — XXI сторіччя»: матеріали XXIII всеукраїнської наук.-практ. конф., 10–15 грудня 2013 р.— Запоріжжя: Вид-во ПГА, 2013.— С. 55–57.*

2. International *critical information infrastructure protection handbook 2008–2009 / Edited by A. Wenger, V. Mauer & M. Cavelty // Center for Security Studies, ETH Zurich, 2009.*

3. Довгань, О. Д. *Критична інфраструктура як об'єкт захисту від кібернетичних атак / О. Д. Довгань // Інформаційна безпека: виклики і загрози сучасності: матеріали наук.-практ. конф., 5 квітня 2013 р.— К.: НА СБ України, 2013.— С. 17–20.*

4. Бірюков, Д. С. *Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні / Д. С. Бірюков, С. І. Кондратов. — К. : НІСД, 2012.— 96 с.*

*5. **Методика** віднесення об'єктів державної та недержавної власності до критично важливих об'єктів для національної безпеки Російської Федерації: № 2–4–87–23–14.— Офіц. вид.— М.: МНС Росії, від 17.10.2012 р.— 29 с.*

*6. **Безпека** критичних інфраструктур [Електронний ресурс].— Режим доступу: http://www.slideshare.net/lukatsky/pir-center-critical-infrastructire-protection.*

*7. **Про погляд** на проблему безпеки критичної інфраструктури в державі Ізраїль [Електронний ресурс].— Режим доступу: http://www.noravank.am/rus/articles/detailphp?ELEMENT_ID=6516.*

*8. **Critical** infrastructure protection [Електронний ресурс].— Режим доступу: http://en.wikipedia.org/wiki/Critical_infrastructure_protection.*

*9. **A Critical** Information Infrastructure Protection Approach to Multinational Cyber Security Events [Електронний ресурс].— Режим доступу: http://www.enisa.europa.eu/activities/cert/ events/files/ENISA_best_practices_for_ciip_Willke.pdf.*

*10. **Green paper** on a European programme for critical infrastructure protection (COM/2005/576 final) [Електронний ресурс].— Режим доступу: http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf.*

С. А. Гнатюк, М. А. Рябый, В. Н. Лядовская

ОПРЕДЕЛЕНИЕ КРИТИЧНОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ И ЕЕ ЗАЩИТЫ: АНАЛИЗ ПОДХОДОВ

Предложено аналитическое исследование нормативно-правовой базы развитых государств мира, касающееся вариаций ключевых понятий в области защиты критичной информационной инфраструктуры. В результате анализа выявлены как общие, так и отличительные особенности подходов к определению критичной инфраструктуры (и других смежных понятий) ряда государств, а также очерчены отечественные проблемы в этой области. Полученные результаты будут полезны при проведении многокритериального анализа указанных дефиниций и при разработке методик отнесения определенных объектов к критичной информационной инфраструктуре.

Ключевые слова: информационная безопасность государства; дефиниция; концепция; критичная инфраструктура; защита критичной информационной инфраструктуры.

S. O. Gnatyuk, M. O. Ryabyi, V. M. Lyadovska

APPROACHES TO THE DEFINITION OF CRITICAL INFORMATION INFRASTRUCTURE AND ITS PROTECTION

In this article was considered an analytical research of the legal framework of developed states in the world which concerned different variations of the key concepts in critical information infrastructure protection. The analysis was revealed differences and similarities in the approaches to the determination of the critical infrastructure in different countries (and related concepts), and stressed the domestic problems in this area. The obtained results will be useful in carrying out the multi-criteria analysis of these definitions, as well as in the development of the classifying methods of certain facilities to the critical information infrastructure.

Keywords: information security; definition; concept; critical infrastructure; critical information infrastructure protection.