УДК 349, 323, 355/359

ЄРМЕНЧУК Олександр Петрович

ПОНЯТТЯ «КРИТИЧНА ІНФРАСТРУКТУРА»

Постановка проблеми. Історичний ретроспективний аналіз розвитку світових держав та цивілізацій свідчить, що перед кожним суспільством періодично постають небезпеки як зовнішнього, так і внутрішнього характеру. З часом, залежно від економічного, соціального та технологічного рівня розвитку, змінюються лише форми таких загроз та об'єкти спрямувань, ураження чи виведення з ладу яких може призвести до людських жертв і значних матеріальних збитків з найсерйознішими негативними наслідками для життєдіяльності суспільства, соціально-економічного розвитку держави, забезпечення її суверенітету, територіальної цілісності та національної безпеки.

Аналіз останніх досліджень і публікацій. Про існування певних об'єктів, що мають принципово-важливе значення для забезпечення сталого функціонування суспільства було відомо ще древнім китайцям та грекам.

На етапі зародження цивілізацій однією з основних загроз для соціального устрою вважалось вторгнення іноземних військ, тобто безпосередня військова загроза. Так, древньокитайський філософ Сунь-Цзи ще в 7 ст. до н. е. у своїй праці про мистецтво війни виділяв 5 найуразливіших об'єктів, які прагне знищити будь-який ворог, а саме: люди, запаси, обози, склади, загони [1, с. 70].

У ті часи до важливих (критичних) об'єктів обов'язково включали транспортну мережу та водопроводи, які були надзвичайно необхідними для населення держав. Їх стабільна робота вважалася запорукою забезпечення потреб громадян та необхідною умовою для управління народом. У зв'язку з цим під час нападу ворогів основною задачею оборонців було захистити саме ці об'єкти від зруйнування. Загалом у подальшому здобуття чи знищення таких об'єктів стало основою військового мистецтва та діяльності спецслужб.

Вважається, що першим, хто почав використовувати слово інфраструктура, був Сократ (5 ст. до н. е.). Так, він зазначав: «Для того щоб людина існувала, їй потрібні тили, які надає суспільство: безпека, соціальний порядок та господарські товари. Однак це вона може отримати в тому випадку, якщо буде поважати концепт суспільства та свої обов'язки. Основними з цих обов'язків є забезпечення інфраструктури та послуг, наданих суспільством» [2]. Згодом термін «інфраструктура» («infrastructure») використовується спочатку у військовій, а потім і в інших сферах. Наприклад, у Франції у значенні «те, що знаходиться під забудовами». На

думку деяких вчених, у тому числі Стефена Левіса, саме використання зазначеного слова французькими працівниками при будівництві залізничних доріг, тунелів та мостів в США сприяло його поширенню в Америці, але потім його значення дещо змінюється [3].

Сьогодні, з розвитком людства, значного прогресу досягли і форми ведення війни. Результатом еволюційних змін у системі міжнародних відносин та відмінною рисою XXI століття можна назвати неоголошені війни, так звані гібридні війни [4, с. 21]. На думку Ф. Хофмана, військового консультанта та аналітика, в гібридних війнах агресор часто використовує унікальну комбінацію загроз, скерованих на найбільш вразливі місця жертви агресії. Ф. Хофман визначає її у застосуванні щодо тактично важливих об'єктів у вигляді найрізноманітніших комбінацій дозволеної зброї, партизанської війни, тероризму тощо для досягнення політичних цілей. За його прогнозами, з цим видом війн доведеться мати справу все частіше [5]. Український політолог та історик Є. Магда серед засобів впливу, під якими розуміються загрози у таких війнах, виділяє наступні їх комбінації: політичні, воєнні, економічні, соціальні, інформаційні, терористичні, підривні тощо [4, с. 30–31].

При зміні засобів мета зазначених дій залишається тією ж – отримання різного роду вигоди: матеріальної, фінансово-економічної чи політичної. Їх ціллю стають ті ж найважливіші (критичні) об'єкти держави, котра є жертвою агресії.

Еволюція форм та засобів ведення війни є прямо залежною від об'єктів спрямувань, що теж еволюціонують. Останніми десятиліттями бурхливий розвиток технологій, особливо в IT-сфері, призвів до значних, а іноді й до революційних змін у підвищенні ступеню взаємозв'язку, взаємопроникнення і взаємозалежності різноманітних мереж і систем, виробничих, фінансових, торговельних та інших процесів в усіх сферах життя більшості країн світу. Лише в XX столітті, під час так званої «Карибської кризи», вперше почали інтенсивно вирішувати питання, пов'язані із критичною інфраструктурою «не військового» характеру – безпеки телекомунікаційних мереж. Серед найбільш резонансних фактів кібератак на об'єкти критичної інфраструктури варто згадати кібератаки на об'єкти ядерної галузі Ірану в 2010 році за допомогою комп'ютерного вірусу Stuxnet. Українські оператори теж ставали об'єктами деструктивного впливу. Зокрема, в 2015 році троянською програмою BlackEnergy було виведено з ладу енергосистему «Прикарпаттяобленерго». Тоді було вимкнено близько 30 підстанцій, понад 230 тисяч мешканців залишились без світла. Загалом, згідно даних з відкритих джерел, в грудні 2016 року на засіданні РНБО України було зазначено, що лише за останні 2 місяці в Україні було зафіксовано 2,5 тис. кібератак [6].

Тому провідні світові держави поряд з фізичною інфраструктурою останнім часом почали виділяти та здійснювати захист кібер-критичної інфраструктури. У Плані захисту критичної інфраструктури США від

2015 року закріплено, що забезпечення безпеки та стійкості фізичної та кіберкритичної інфраструктури сприяє мінімізації наслідків від дії загроз та її швидкому відновленню [7]. У Німеччині, окрім загроз від терактів, злочинних дій та від стихійних явищ, виділяють третій вид – загрози від технічних збоїв та людських прорахунків, під якими розуміються, в тому числі і кіберзагрози [8].

Доцільно також зазначити про існування небезпеки іншого, не соціального, а природного характеру. До неї слід віднести паводки, засухи, епідемії, епізоотії та епіфітотії, землетруси, бурі тощо. Майже усі країни виділяють окремою групою загрози природного характеру.

Отже, критична інфраструктура завжди була і залишається першочерговим об'єктом захисту та джерелом інтересу агресора чи важливим об'єктом, що може бути уражений різного роду факторами, в тому числі не лише соціальними, а і природними. Залежно від розвитку суспільства зміст поняття «критичної інфраструктури» постійно змінюється. Водночас спроби виділити її в окрему категорію та організовувати належний захист на рівні загальнодержавного підходу в світі розпочато досить нещодавно.

Враховуючи зазначене, на етапі формування в Україні законодавства у сфері критичної інфраструктури та побудови системи її захисту, пошуку ролі й місця в цій системі захисту установ, організацій (серед яких зараз активно вирішується статус та повноваження Кабінету Міністрів України, РНБО України, СБ України, Держспецзв'язку тощо) нашій державі важливо простежити еволюцію зазначеного поняття, зрозуміти його зміст та сформулювати повне, завершене і при цьому характерне для нас визначення критичної інфраструктури. Це і зумовлює актуальність наукової розробки питання.

Метою дослідження є обґрунтування поняття «критичної інфраструктури», а також участі в процесі її функціонування органів СБ України.

Аналіз світового досвіду свідчить, що над проблематикою критичної інфраструктури з 80-х років XX століття активно почали працювати США, зокрема Національний дослідний інститут (U.S. National Research Council) [9]. Досить популяризувала проблематику у 80-х роках XX століття книга «Америка в руїнах» [10]. Значно активізувалось дослідження проблеми після терористичних актів 11 вересня 2001 року в США, 11 березня 2004 року в Мадриді та 7 липня 2005 року – Лондоні.

Виклад основного матеріалу. Як уже зазначалось, зміст поняття «критична інфраструктура» постійно коригується та удосконалюється. Так, у 2002 році в рамках роботи Євроатлантичної ради НАТО закріплено, що «критична інфраструктура включає в себе фізичні та кібернетичні системи забезпечення важливих та необхідних видів діяльності економіки та державного управління». Серед галузей, в першу чергу, включено телекомунікаційні, енергетичні, банківські, фінансові, водно-господарські системи та аварійні служби державної і недержавної власності.

Досить активно дослідження з безпеки почали проводитись з 2003 року в рамках програми ЄС «European industrial potential in the field of security research» та «European Security Research Programme (ESRP)». З 2007 року в цілях підготовки заходів на випадок війни чи надзвичайних подій розпочалась робота над ініціативою «Research for Secure Europe» (дослідження для безпеки Європи). Поряд із зазначеним, починаючи з 2004 року на рівні ЄС та Європейської комісії почалось створення проекту захисту критичної інфраструктури «European Programme for Critical Infrastrukture Protection» (далі – EPCIP). У ньому важливу увагу було приділено захисту від терористичних загроз. В цей час під критичною інфраструктурою розуміється «обладнання, служби і інформаційні системи життєво важливі для держави, знищення чи відмова від яких призведе до послаблення суспільства, національного господарства, системи охорони здоров'я, безпеки ефективного функціонування державного устрою».

17 листопада 2005 року Комісія прийняла «Зелену книгу» по захисту критичної інфраструктури (EPCIP). Її основним завданням було сформувати як на політичному, так і безпосередньо на рівні виконавців загальну позицію та заходи із захисту критичної інфраструктури в країнах – членах ЄС. Червоною ниткою проведено те, що захист критичної інфраструктури кожної країни потребує посилення взаємодії та обміну інформацією щодо загроз на загальноєвропейському рівні та між окремими країнами учасниками.

Дослідження підходів держав ЄС до розуміння критичної інфраструктури сьогодні засвідчує її сприйняття як комплексної системи, що має побудову мережі, яка включає окремі елементи цієї мережі та ланцюжок з'єднань (окремих пов'язаних елементів). Місця з'єднань елементів ланцюжків утворюють вузол. Пошкодження чи руйнування одного з вузлів впливає на діяльність інших та може призвести до повалення всієї критичної інфраструктури. Тому в інтересах захисту критичної інфраструктури потрібно захищати такі вузли. Захист критичної інфраструктури будується на зменшенні вразливості системи чи збільшенні її стійкості до наслідків надзвичайних подій [11, с. 32]. В США розрізняють 2 елементи, що стосуються критичної інфраструктури, це сама критична інфраструктура та основні елементи (активи чи джерела) в сукупності їх нараховують 16 секторів. В Європі застосовують «рівні областей» (секторів) та «рівні продуктів та послуг» (елементів), їх кількість складає від 8 до 10. Якщо раніше захист критичної інфраструктури в Європі, в першу чергу, був націлений на забезпечення стабільного функціонування національних критичних інфраструктур, то зараз основною метою Європейської програми по захисту критичної інфраструктури є забезпечення рівномірного захисту критичної інфраструктури всього європейського простору. Згідно з положеннями програми основними її завданнями є протидія тероризму та кіберзагрозам.

Вочевидь, враховуючи викладене, при формулюванні визначення

вітчизняної критичної інфраструктури доцільно зважати на те, що світова практика визнала доцільність включення до складу інфраструктури матеріальних та нематеріальних об'єктів. Характеристику значення цих об'єктів для функціонування держави пропонується описати словосполученням «надзвичайно важливі». Вони подібним чином визначаються у законодавстві США та Німеччини, де звучать, як «системи та засоби, фізичні чи віртуальні, настільки життєво важливі для Сполучених Штатів...» (Patriot Act, 2001) та «організаційні та фізичні структури і об'єкти настільки життєво важливі для суспільства та економіки Німеччини...» [12].

Саме тому, на нашу думку, вітчизняне визначення критичної інфраструктури має включати «сукупність надзвичайно важливих матеріальних та нематеріальних об'єктів національної інфраструктури». На законодавчому рівні це забезпечить можливість здійснення заходів із протидії тероризму та кіберзагрозам критичній інфраструктурі на загальнодержавному рівні таким чином, як це здійснюється і в країнах ЄС.

Важливо зауважити, що останнім часом при визначенні терміна «критична інфраструктура» акцент зміщується з фізичного виміру об'єктів все більше до їх функцій та послуг. Саме вони забезпечують потреби суспільства, держави та її економіки, тому і лежать в основі визначення критичності. Це надає ефективні методологічні можливості для визначення критеріїв відбору елементів критичної інфраструктури та черговості при організації їх захисту [12, с. 6–9].

Іншою характеристикою об'єктів критичної інфраструктури є їх належність до національної інфраструктури. Як зазначалось у попередніх роботах автора, «національна інфраструктура» – це взаємопов'язана система державного управління та об'єктів інфраструктури, що забезпечує діяльність у різних сферах функціонування держави її економіки та суспільства. «Об'єкт інфраструктури» може об'єднувати в собі – державні та приватні підприємства, організації та установи, а також їх власність та результати діяльності, що забезпечують функціонування держави її економіки та суспільства» [13]. Лише надзвичайно важливі об'єкти національної інфраструктури можуть визначатися критичною інфраструктурою.

У директиві Ради ЄС критична інфраструктура поділяється на національну критичну інфраструктуру та європейську. Національна критична інфраструктура включає «засоби, системи та їх частини, держави – члена ЄС, що є принциповими для збереження найбільш важливих суспільних функцій, здоров'я, безпеки, забезпечення належних господарських чи соціальних умов для населення, порушення чи руйнування яких спричинило б державі – члену ЄС серйозні наслідки в результаті відмови таких функцій» [14]. Оскільки деякі елементи критичної інфраструктури мають вагоме значення не лише на національному, а й на міждержавному рівні, в ЄС визначили європейську критичну інфраструктуру, до якої віднесли «критичну інфраструктуру, що знаходиться в державах-членах ЄС, порушення чи руйнація

якої могли б спричинити серйозні наслідки не менше як у двох державах» [14]. Цікаву думку з приводу того, що відноситься до критичної інфраструктури можна знайти в статті професора Йозефа Ржиги в журналі «Урбанізм і територіальний розвиток». Позиція автора характеризується тим, що критерії вибору мають ґрунтуватися на професійних знаннях з урахуванням обсягу, важливості та часового фактора [15].

Загалом, аналізуючи поняття «критична інфраструктура», логічним висновком є те, що воно повинно включати ті найважливіші об'єкти, без яких, чи з порушенням діяльності яких, у державі можуть настати навіть невідворотні негативні процеси, може бути завдано великих збитків громадянам, їх здоров'ю та життю, соціально-економічному стану країни. Саме від стабільної діяльності критичної інфраструктури залежить функціонування національної інфраструктури та економіки в цілому.

Як зазначалося вище, критична інфраструктура перебуває під постійним впливом загроз безпосередніх чи потенційних або відомих та невідомих (так званий Х-фактор). Європейці серед загроз критичній інфраструктурі виокремлюють глобальні, тобто ті, що можуть спричинити загальні наслідки географічної, міжгалузевої, економічної та соціальної небезпеки [12, с. 19–20]. Водночас у національних законодавствах провідних країн світу загрози критичній інфраструктурі в основному розділяють на три основні категорії, виходячи з характеру їх походження. Перша – ризики, які неможливо попередити (пожежі тощо). Друга – ризики, які виникають через помилки управління та діяльності. Третя – зовнішні ризики, над якими держава та оператори не мають контролю. Українські науковці Національного інституту стратегічних досліджень, враховуючи особливості безпекової ситуації, в якій перебуває наша країна, пропонують виокремлювати три категорії загроз, на які має бути налаштований захист критичної інфраструктури: аварії та технічні збої, зокрема, авіаційні катастрофи, ядерні аварії, пожежі, аварії у системах енергозабезпечення, викиди небезпечних речовин, відмови систем, аварії та надзвичайні події зумовлені недбалістю, організаційними помилками тощо; небезпечні природні явища, зокрема, надзвичайні погодні умови, лісові, степові та торф'яні пожежі, сейсмічні явища, епідемії та пандемії, космічні явища, урагани, торнадо, землетруси, цунамі, повені і т. ін.; зловмисні дії, зокрема, зловмисні дії груп або окремих осіб таких, як терористи, злочинці і диверсанти, а також військові дії в умовах війни. Особливо небезпечними є комбіновані загрози та загрози, реалізація яких може призвести до катастрофічних і різноманітних каскадних ефектів внаслідок взаємозалежності елементів критичної інфраструктури.

Незважаючи на те, що з часом змінюються форми загроз, об'єкти спрямування, методи впливу, але характерною особливістю критичної інфраструктури, яку обов'язково доцільно відобразити у вітчизняному визначенні, є наслідки їх руйнації або пошкодження. Їх, як правило, більшість країн світу визначають як

«спричинення людських жертв і значних матеріальних збитків з найсерйознішим негативним впливом на життєдіяльність суспільства, соціально-економічний розвиток держави, забезпечення її суверенітету, територіальної цілісності та національної безпеки».

На переконання автора, до ознак критичної інфраструктури також необхідно включити можливість значно впливати на забезпечення національної безпеки. Саме це є однією з її основних відмінних рис від національної інфраструктури. Це, в свою чергу, спонукає до необхідності якісного та всебічного дослідження розглянутої проблеми та надання пропозицій щодо підвищення ефективності діяльності у зазначеній сфері органів СБ України.

Висновки. Доцільно наголосити, що якісне тлумачення змісту поняття «критична інфраструктура» є запорукою створення ефективної системи її функціонування та захисту. Тому вкрай важливо достатньо чітко окреслити складові критичної інфраструктури, адже вона забезпечує умови для існування не лише певного суспільства та держави, а в глобальному розумінні – всього населення Землі.

Таким чином, з урахуванням зазначеного вище можна сформулювати наступне визначення **критичної інфраструктури** – це система надзвичайно важливих матеріальних та нематеріальних об'єктів національної інфраструктури (а також їх власність та результати діяльності), що забезпечують її стале функціонування, руйнація або пошкодження яких (наявними загрозами) може призвести до людських жертв і значних матеріальних збитків із найсерйознішими негативними наслідками для життєдіяльності суспільства, соціально-економічного розвитку країни та національної безпеки.

З огляду на поняття в подальшому доцільно формувати перелік вітчизняних секторів критичної інфраструктури, приймаючи до уваги наявні ресурси та потреби у підтримці та захисті основних об'єктів економіки держави та їх функцій. Після формування секторів критичної інфраструктури необхідно розпочати складання переліку конкретних об'єктів та елементів критичної інфраструктури. Він може налічувати від десятків пунктів до кількох тисяч. Захист критичної інфраструктури має відбуватись на основі розробки Програми захисту критичної інфраструктури та відповідних Програм захисту секторів економіки України. Програми повинні бути зв'язані з механізмами державної підтримки та стимулювання розвитку економіки, а тому розроблятися у рамках відповідних державних цільових програм. Це сприятиме їх фінансовому забезпеченню. Важливе місце має приділятись державній системі захисту критичної інфраструктури, де відповідне місце має зайняти СБ України. Роль спецслужби має полягати в участі у визначенні загроз, формуванні об'єктів критичної інфраструктури та в організації заходів по її захисту від загроз, в тому числі розробленні відповідних планів. Окрему увагу доцільно приділяти підготовці основного закону у

сфері та якісній системі нормативно-правових актів, що регулюють відносини в процесі функціонування критичної інфраструктури. Без цього неможливе безпечне існування суспільства, функціонування економіки держави і належний захист національних інтересів.

Список використаних джерел

1. Трактаты о военном искусстве / Сунь-Цзы, У-цзы / [пер. с китайского ; предисловие и коммент. Н. И. Конрада]. – М. : АСТ: Астрель; СПб. : Terra Fantastica, 2010. – 606 с.

2. Evolutions of Infrastructure: 15,000 Years of History by Demeter G. Fertis, Anna Fertis, Published by Vantage Press, 1998.

3. [Електронний ресурс]. – Режим доступу: http://hakpaksak.wordpress.com/2008/09/22/the-etymology-of-infrastructure-and-the-infrastructure-of-the-internet.

4. Магда Е. Гибридная агрессия России: уроки для Европы / Евгений Магда. – К. : Каламар, 2017. – 284 с.

5. Hoffman F. Onnot-so-newwarfare: political war fare vs hybrid threats [Електронний ресурс]. – Режим доступу : http://warontherocks.com.

6. [Електронний ресурс]. – Режим доступу : https://uk.m.wikipedia.org/wiki/Кібервійна.

7. National Critical Infrastructure Security and Resilience Research and Development Plan, 2015 [Електронний ресурс]. – Режим доступу : https://www.dhs.gov/publication.

8. Защита критической инфраструктуры. Концепция основных мер защиты. Рекомендация для предприятий. – Bundesministerium des Innern, 2006 [Електронний ресурс]. – Режим доступу : https://www.bmi.bund.de.

9. Infrastructure for the 21st Century Framework for a Research Age. Washington: National Academies Press, 1987.

10. Choate, Pat a Susan Walter. America in ruins: the decaying infrastructure. Durham, N.C. : Duke Press Paperbacks, 1981.

11. Марек Сметана. Защита критической инфраструктуры. Подходы государств Европейского Союза к определению элементов критической инфраструктуры / Марек Сметана. – Острава : ВШБ – Технический университет Острава, 2014/2015. – 60 с.

12. Зелена книга з питань захисту критичної інфраструктури / Д. Бірюков [та ін.] ; Нац. ін-т стратегічних досліджень. Експерти. Офіс зв'язку НАТО в Україні. – Київ, 2015. – 35 с.

13. Єрменчук О. П. Складові національної інфраструктури. / О. П. Єрменчук // Науковий вісник ДДУВС. – 2017. – № 4.

14. Směrnice Rady 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.

15. Říha, Josef., Urbanismus a územní rozvoj – ročník X – číslo 4/2007 [Електронний ресурс]. – Режим доступу : http://www.uur.cz/images/5-publikacni-cinnost-a-knihovna/casopis/2007/2007-04/08_kriticka.pdf.

Рецензенти:
доктор юридичних наук, доцент
О. Кириченко,
кандидат юридичних наук
В. Дараган

Аннотация. Путем анализа иностранных источников прослежена эволюция понятия «критическая инфраструктура» и определены ее особенности. Дана характеристика элементов критической инфраструктуры. Установлено, что она формирует условия для жизнедеятельности не только конкретного общества и государства, а имеет межгосударственный характер. Предлагается авторское определение понятия: «критическая инфраструктура».

Ключевые слова: критическая инфраструктура, защита критической инфраструктуры, национальная безопасность, определение, угрозы, понятие.

Abstract. On the basis of the foreign sources analysis the evolution of the «critical infrastructure» concept has been deduced and its peculiarities have been determined. The characteristic of the critical infrastructure components was given. It was established that critical infrastructure provided conditions for a certain society and state life, and also had interstate nature. The author's definition of the term «critical infrastructure» was proposed.

Key words: critical infrastructure, critical infrastructure protection, national security, definition, threats, concept.

УДК 159.9.019:377.35

ПЕЛЕПЕЙЧЕНКО Людмила Миколаївна
РЕВУЦЬКА Світлана Михайлівна

НАЦІОНАЛЬНА ГВАРДІЯ УКРАЇНИ ЯК ОБ'ЄКТ НАПАДІВ В ІНФОРМАЦІЙНІЙ ВІЙНІ

Постановка проблеми. Терміни *інформаційна війна, гібридна війна* не тільки ввійшли до наукового обігу в конфліктології, політології, соціології, психології, теорії мовної комунікації – вони поширились у друкованих виданнях мас-медіа, на телебаченні і радіо, в повсякденній мові українців. Причина цього явища зрозуміла і не потребує коментарів – в суспільстві обговорюють ті проблеми, що найбільше хвилюють громадськість, що є болісними, злободенними. У численних наукових працях, присвячених проблемам інформаційної війни, намагаються виявити її причини, визначити форми, методи і засоби її ведення, відшукати способи протидії інформаційній агресії. Вирішення наведених завдань можливе за умови ретельного аналізу конкретних нападів на владу,