Міністерство освіти і науки України
Національний університет водного господарства
та природокористування
Кафедра державного управління,
документознавства та інформаційної діяльності

ISSN 2617-4650
https://doi.org/10.31713/st1-220190

Присвячений першому випуску
магістрів місцевого самоврядування

СТРАТЕГІЯ І ТАКТИКА ДЕРЖАВНОГО УПРАВЛІННЯ

збірник наукових праць
Спецвипуск 1-2, 2019 р.

Рівне – 2019

Зміст випуску

Product Development Game. *The Uneasy Alliance*. *Clark K and Hayes R. (Eds.)*. Boston, 1985.
12. Davymuka S. A., Fedulova L. I. Intelektualnyi resurs – osnovnyi faktor zabezpechennia staloho rozvytku rehioniv Ukrainy v umovakh detsentralizatsii. *Rehionalna ekonomika*. 2017. № 1. S. 5–16.
13. Jacobs G. Towards a New Paradigm in Education. URL: http://cadmusjournal.org/article/volume-2/issue-2-part-2/towards-new-paradigm-education (data zvernennia: 15.07.2019).
14. Khanyn Y. Kakoe nam nuzhno obrazovanye. URL: https://www.sciencehunter.net/Blog/story/Education (data zvernennia: 15.07.2019).
15. Vernadskii V. I. Nauchnaia mysl kak planetnoe yavlenie. M. : Nauka, 1991. 271 s.
16. Bazaluk O. A. Filosofiia obrazovaniia v svete novoi kosmolohicheskoi kontseptsii : uchebnik. K. : Kondor, 2010. 458 s.
17. Bazaluk O. Filosofiia osvity: yii rol ta mistse v systemi filosofskoho znannia. URL: http://dspace.pnpu.edu.ua/bitstream/123456789/977/1/Bazaluk.pdf (data zvernennia: 15.07.2019).

УДК 354:340.133:340.134 https://doi.org/10.31713/st1-2201917
JEL : F 52, H 84, O 18

Сазонець О. М.,
д.е.н., професор,
завідуюча кафедрою міжнародних економічних відносин
Національний університет водного господарства
та природокористування, м. Рівне

Ващишин А. О.,
аспірант кафедри міжнародних економічних відносин
Національний університет водного господарства
та природокористування, м. Рівне

ДЕРЖАВНЕ РЕГУЛЮВАННЯ ФУНКЦІОНУВАННЯМ ТА РОЗВИТКОМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В ДЕРЖАВАХ СВІТУ

Sazonets O. M.,
Doctor of Economics, Professor,
Head of the Department of International Economic Relations,
National University of Water and Environmental Engineering

Vashchyshyn A. O.,
Post-graduate Student of the Department of
International Economic Relations,
National University of Water and Environmental Engineering, Rivne

STATE REGULATION OF FUNCTIONING AND DEVELOPMENT OF CRITICAL INFRASTRUCTURE IN THE COUNTRIES OF THE WORLD

В роботі проаналізовано підходи щодо управління об'єктами критичної інфраструктури в різних країнах світу. Визначено досвід таких країн як США, Китай, Японія, Велика Британія, Франція, Німеччина. Визначено сфери, які відносяться до критичної інфраструктури в окремих країнах, зроблено порівняльний аналіз підходів до розвитку та функціонування об'єктів критичної інфраструктури.

This paper analyzes approaches to managing critical infrastructure in different countries of the world. Experience of such countries as USA, China, Japan, Great Britain, France, Germany is defined. Areas of critical infrastructure identified in individual countries, comparative analysis of approaches to the development and operation of critical infrastructure.

***Ключові слова**:* управління, об'єкти, критична, інфраструктура, країни світу, порівняльний аналіз.

Keywords: management, facilities, critical, infrastructure, countries, benchmarking.

Постановка завдання. Україна налічує на своїй території величезну кількість об'єктів критичної інфраструктури. Ці об'єкти життєво необхідні для розвитку національної економіки, транспортного сполучення, забезпечення функціонування житлово-комунального господарства. Проблеми функціонування, експлуатації таких об'єктів є спільними для України та багатьох інших країн світу. Варто зазначити, що існують відмінності між США, ЄС і Китаєм з точки зору організації державного управління об'єктами критичної інфраструктури. США та ЄС сприяють ідеї участі приватного сектора під час законодавчого процесу, а у відповідь – приватний сектор розглядає підтримку як обов'язок надання внесків та очікування щодо політики розвитку об'єктів критичної інфраструктури. Китайський уряд також розглядає як важливу підвищену прозорість цієї політики. Незважаючи на те, що на протязі офіційного процесу немає законодавчо встановлених дій для приватного сектора, китайський уряд зазвичай використовує 30-денний період, на протязі якого відбувається публічне обговорення для збору відгуків суспільства незадовго до перегляду цієї політики. Крім того, оператори традиційної критичної інфраструктури є приватними особами в США та ЄС, в той час, як більшість операторів у подібних секторах забезпечення діяльності об'єктів критичної інфраструктури в Китаї належить державі, крім сектору послуг Інтернет-мережі.

Аналіз останніх досліджень та публікацій. Обмежене коло фахівців досліджувало стан, розвиток та особливості функціонування об'єктів критичної інфраструктури. У роботах В. Горбуліна та М. Гончара аналізуються передумови формування гібридної агресії Росії проти України та формується основа для її операціоналізації у безпековій політиці країни. Питанням захисту критичної інфраструктури присвячено працю фахівців Національного інституту стратегічних досліджень під назвою «Зелена книга з питань захисту критичної інфраструктури України», автор – Насвіт О.І., Суходоля О.М. Інші роботи цих авторів, які розкривають теоретичні засади, досвід розробки концепції захисту критичної інфраструктури, пріоритетів формування політики захисту критичної інфраструктури та механізмів її реалізації. В подаваному досліджені нами буде проаналізовані аналогічні питання з точки зору практичних заходів розвитку критичної інфраструктури в індустріально розвинутих країнах світу на основі положень, нормативних актів, що діють в цих країнах.

Мета статті. Метою статі є дослідження державного регулювання функціонування та розвитку критичної інфраструктури в державах світу. З метою проведення дослідження буде проаналізовано досвід США, Китаю та країн Європи.

Основні результати дослідження. Проаналізуємо підтримку критичної інфраструктури у США. Національні критичні системи інфраструктури цієї країни, її об'єкти, активи та мережі надають основні послуги, які служать основою американської національної економіки, безпеки та здоров'я і можуть бути атаковані тими, хто прагне заподіяти шкоду Сполученим Штатам та їх інтересам. Посилення і збереження надійної, функціональної і стійкої критичної інфраструктури вимагає активних та скоординованих зусиль. Ці заходи засновані на загальній відповідальності федеральних, державних, місцевих та територіальних одиниць, а також державних та приватних власників та операторів критичної інфраструктури. Головний аспект збереження безпечної критичної

інфраструктури – контроль доступу, обмеження доступу до фізичних засобів та активів тільки тими, хто має законну потребу і був перевірений. Це забезпечить відсутність певного ризику. Хоча Федеральний уряд володіє малою частиною критичної інфраструктури, Федеральна агенція грає різні ролі у захисті критичної інфраструктури країни – у партнерстві з нефедеральними зацікавленими сторонами, щоб забезпечити ефективну підтримку контролю доступу і не створювати перешкоди для потоку операцій законного бізнесу.

Департамент національної безпеки (DHS) є провідним федеральним агентством, відповідальним за внутрішній захист критичної інфраструктури, але інші федеральні відомства несуть відповідальність за контроль за різними відповідними секторами критичної інфраструктури, такими, як оборонно-промисловий сектор та енергетичний сектор. План захисту національної інфраструктури (NIPP) визначає функції та обов'язки Департаменту національної безпеки та агентств специфічних галузей (CCA) – федеральних відомств та відомств по захисту критичної інфраструктури у шістнадцяти її секторах. У 2006 році у відповідь на Президентську Директиву національної безпеки Департамент національної безпеки створив Скринінговий координаційний офіс (SCO), розташований в політичному офісі DHS. Скринінговий координаційний офіс несе відповідальність за нагляд Департаменту національної безпеки та контроль акредитаційних заходів, в тому числі тих, що орієнтовані на доступ до критичної інфраструктури. Акредитація в цьому контексті відноситься до процесу визначення права особи на певну ліцензію, привілеї чи статус від заявки на доступ до використання інформації і до визначення терміну закінчення дії, або потенційного відкликання видання облікового запису.

Керований контроль доступу з боку федерального управління залучає дві групи зацікавлених сторін: користувачі та оператори. Користувачі – це особи, які потребують доступу до критично важливої інфраструктури як основної функції їхньої роботи. Оператори володіють або несуть відповідальність за управління об'єктами критичної інфраструктури, такими, як аеропорти, морські порти та хімічні об'єкти, які в цілому є приватними, але можуть також включати державні об'єкти, такі, як військові установки.

Департамент національної безпеки та інші федеральні відомства допомагають контролювати доступ через найрізноманітніші фізичні засоби та активи секторів інфраструктури, за які вони несуть відповідальність. Ці федеральні адміністратори допомагають операторам захищати важливі інфраструктурні об'єкти від атак, диверсій, крадіжки або неправильного використання під час відкриття законного доступу, що допомагає забезпечити потік бізнесових операцій. При обслуговування потреб оператора адміністратори також повинні забезпечити відповідність федеральним законам та нормам. Федеральні агентства грають різноманітні ролі, які допомагають досягти цього балансу, включаючи, але не обмежуючись:

1) володінням та експлуатацією певних видів інфраструктури;

2) оптовою торгівлею, експлуатацією та управлінням програмами акредитації для конкретних видів інфраструктури;

3) частковою роботою та управлінням активами програм;

4) наданням правил та інструкцій для допомоги власникам та операторам, що реалізують ефективний контроль доступу.

Наприклад, Адміністрація транспортної безпеки (TSA) керує процесом Акредитації кваліфікації транспортних працівників за ідентифікацією (TWIC) процесів, включаючи реєстрацію, фонові перевірки та підтримку облікових даних. Однак, для області безпечної ідентифікації значка дисплея (SIDA), який полегшує доступ в аеропортах і частково керований TSA, оператори аеропорту використовують інформацію перевірки TSA та в кінцевому підсумку приймають остаточні рішення щодо доступу до аеропорту та видачі значків. Аналогічно Атомна регуляторна комісія видає нормативні акти, що стосуються вимог щодо контролю доступу, які повинні бути реалізовані комерційними атомними станціями, та членами Комітету по захисту, також американськими військовими об'єктами та об'єктами з використання Спільної карти доступу

(САС) як одного із способів полегшення доступу до напівзакритої зони в межах установок [1].

Великобританія є другою державою ЄС, яка почала визначати і захищати свою критичну інфраструктуру. У 1999 р. у Великобританії був створений Координаційний центр з безпеки національної інфраструктури (National Infrastructure Security Coordination Centre NISCC), який входив до складу Міністерства внутрішніх справ, пізніше була створена Рада національного центру з безпеки (National Security Advice Centre – NSAC). Ці організації з 2007 р. замінює Центр по захисту національної критичної інфраструктури (Centre for Protection of National Infrastructure – CPNI). У Великобританії національна критична інфраструктура визначається на підставі постійного забезпечення основних послуг. За їх визначення сьогодні несе відповідальність Центр по захисту національної інфраструктури (CPNI – Centre for the Protection of National Infrastructure). Цей Центр надає комплексну інформацію з безпеки національної критичної інфраструктури. Великобританія за зразком США, в захисті критичної інфраструктури, орієнтується, перш за все, на тероризм і порушення кіберпростору. Свою політику держава узагальнює в документах «Антитерористична стратегія» (CONTEST – Counter terrorism strategy), «Програма стійкості критичної інфраструктури» (CIRP – Critical Infrastructure Resilience Programme) і «Стратегія щодо захисту від кібератак» (Cyber Security Strategy) від 2009 р. [2].

Секторами критичної інфраструктуру у Великій Британії є:

1. Служби швидкого реагування (поліція, пожежники, швидка допомога,

берегова поліція);

2. Уряд (державне управління, самоврядування, судочинство, сили національної безпеки, армія);

3. Комунікації, телекомунікації, пошта, мовлення;

4. Охорона здоров'я (медичні послуги);

5. Вода (мережа водопроводів, каналізація);

6. Енергія (нафта, природний газ, електрика);

7. Фінансові послуги, фінанси (менеджмент активів, фінансові установи, інвестиційна, банківська справа, ринки, банківська справа для дрібних споживачів);

8. Продукти харчування (виробництво, імпорт, обробка, дистрибуція, продаж);

9. Транспорт (автомобільний, залізничний, водний, авіаційний) [3].

Критична інфраструктура змінюється з плином подій. Велика Британія намітила зараз свій шлях на вихід з ЄС. Це вчинило вплив на стан її критичної інфраструктури.

Уряд Великобританії оголосив, що підприємства, які надають такі важливі послуги, як енергетика та транспорт, можуть бути оштрафовані на суму 17 мільйонів фунтів або 4 відсотки світового обороту за відсутність ефективних заходів для забезпечення кіберзахисту.

Пропозиції від Департаменту цифрової, культурологічної галузі, медіа та спорту задовольняють вимогам Директиви ЄС щодо мережі та інформаційних систем (HIC), яка набере чинності в травні 2018 року. Компанії з критичною інфраструктурою також повинні будуть показати, що вони мають стратегію для покриття втрат енергії та екологічних катастроф.

Директива стосується втрати послуг, а не втрати даних, що підпадає під Загальні правила захисту даних (GDPR). Пропозиції Великобританії встановлюють максимальний рівень штрафу за найбільш серйозні прогалини в інфраструктурі під час кризи, що стосуються найсуворіших штрафів, що накладаються згідно з Регламентом ЄС щодо захисту загального обсягу даних.

Організації, які надають послуги з водопостачання, енергетики, транспорту та охорони здоров'я – вразливості яких були викриті нещодавніми атаками WannaCry (pt) та NotPetya ransomware, – знаходяться в полі зору. «Штрафи будуть останнім засобом, і вони не застосовуватимуться до операторів, які адекватно оцінили ризики, вжили відповідні заходи безпеки та приймалися компетентними органами влади, але все ще зазнали нападу», – пояснює урядовий висновок [4].

У Великобританії тлумачення Директиви з кібербезпеки висунуло еквівалентні штрафи у розмірі, встановленому Загальним регламентом захисту даних. Сьогоднішнє повідомлення про критичну національну інфраструктуру йде далі,

ніж вимагається ЄС згідно з Директивою з мережевих та інформаційних систем.

У Німеччині у якості реакції на американський PDD-63 в 1997 році виникло Федеральне відомство з інформаційної безпеки (Bundesamt für Sicherheit in der Informationstechnik – BSI). Фізичними аспектами безпеки займалося Федеральне відомство з цивільного захисту та підтримки в разі катастроф (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe – BBK). сьогодні головним координатором захисту критичної інфраструктури є Федеральне Міністерство внутрішніх справ. Важливу роль тут відіграє і Федеральне Міністерство господарства і праці (Bundesministerium für Wirtschaft und Arbeit), так як більше дев'яноста відсотків критичної інфраструктури знаходиться у власності приватних суб'єктів. Нещодавно тут виникла інституція – Захист критичної інфраструктури в Німеччині (Schutz Kritischer Infrastrukturen in Deutschland), яка досліджувала вразливість німецької інфраструктури і запропонувала стратегії її захисту і політику співробітництва і кооперації суспільного управління з приватними суб'єктами. Для цілей координації в 2002 році Федеральним міністерством внутрішніх справ було встановлено міжміністерську робочу групу для критичної інфраструктури AG KRITIS. Стратегічний розвиток та імплементація заходів координуються за допомогою інших федеральних міністерств, перш за все, Федерального міністерства з економіки і технологій, Федерального посольства, Федерального міністерства справедливості, Федерального міністерства закордонних справ, Федерального міністерства оборони при співробітництві з відповідними агентствами [5].

У Франції за координування області критичної інфраструктури відповідає прем'єр-міністр. Міністри окремих міністерств несуть відповідальність за імплементацію рішень. З організаційних складових відповідальність за координування діяльності несе Генеральний секретар з оборони і національної безпеки (Secrétariat Général de la Défense et de la Sécurité Nationale – SGDSN). Він безпосередньо підпорядковується прем'єр-міністру і допомагає Управлінню прем'єр-міністра в координуванні, підготовці, впровадженні та обробці урядових рішень, що стосуються безпеки і оборони, в тому числі і безпеки інформаційних систем. Підхід Франції заснований на управлінні ризиками, превенції, планах реагування і підтримки обміну інформацією. Основи системи критичної інфраструктури були створені в 1997 році, їх визначив французький прем'єр-міністр в Інформаційній і комунікаційної асоціації. Її метою була допомога в досягненні інших членських держав ЄС в галузі використання Інтернету, удосконалення основних громадських служб, стандартизації та навчанні державних працівників, у визначенні більш відповідних процесів щодо безпечного використання інформаційних технологій і мереж. З точки зору правового середовища основним документом є Закон № 6600 / SGDSN / PSE / PSN з 2014 року про захист основних економічних секторів (Secteurs d'Activités d'Importance Vitale) 29. Тут критичними вважаються всі сектори, службовці, що забезпечують основні соціальні і економічні процеси.

До критичних секторів Франції відносяться:

– громадське управління;
– судочинство;
– збройні сили;
– сільське господарство;
– електронні комунікаційні системи, аудіо та відеоінформаційні технології;
– енергетика;
– космос і дослідницька діяльність;
– фінансовий сектор;
– вода;
– промисловість;
– громадське здоров'я;
– транспорт [6].

Збереження критичної інфраструктури та безпеки є особливо актуальним для Японії, тому що цю безпеку треба надати під час Олімпійських і паралімпійських ігор 2020 року та після них.

Один з основних успіхів програми «Збереження критичної інфраструктури та безпеки» є прискорення соціальної реалізації за допомогою співпраці операторів критично важливої інфраструктури. Державна програма створила структуру реалізації, що здатна добре узгоджувати діяльність різних суб`єктів критичної інфраструктури. Громадський Комітет

сприяння розвитку критичної інфраструктури складається з представників від університетів, науково-дослідних інститутів, промисловості та операторів критичної інфраструктури. Робочі групи забезпечують механізм розподілу проблем, визначення потреб та забезпечення координації для інтеграції технологій та систем в кожному дослідженні та темі розробки. Поєднавши ці функції, ця структура працює в бік соціальної реалізації для складових технологій так швидко, як тільки можна [7].

Оператори об'єктів критичної інфраструктури звернулися з проханням урахування в Державні Програмі питань раннього прийняття пріоритетних заходів та оцінок в рамках тестового середовища операторів. Заснована на цих запитах, перевірка для основи розроблених технологій були швидко відстежена. Запровадження Програми відбулося в кінці 2016 року для перевірки правильності управління системою критичної інфраструктури. Це об'єднало як старі, так і нові системи. У той же час, була проведена робота з операторами критичної інфраструктури, що перевіряють виявлення атаки на технології.

Програма є інструментом просуванням розвитку соціальних технологій впровадження, в тому числі вона є загальною соціальною платформою для реалізації та освіти фахівців у галузі безпеки. Платформа розроблена, починаючи з 2017 року, і охоплює операторів критичної інфраструктури. По мірі використання цієї платформи, будуть негайно вирішуватися будь-які проблеми або функції.

У відповідності до рішень прийнятих органами державного управління в процесі реалізації Програми буде налагоджена система, яка продовжуватиме реагувати на нові форми кібер-атак та вразливості до безпеки, ведучи підготовку до подальшого впровадження технологій захисту за допомогою технологій AI та Big Data.

Сильні сторони Японії полягають у стабільних операціях у сфері енергетичного сектору, надійних комунікацій та транспортних мереж. Завдяки цій програмі японці планують забезпечити безпеку, яка фактично виступає як додана вартість безпеки для критичної інфраструктури. Є також сподівання, що країна буде експортувати японські технології безпеки, а також безпечну критичну інфраструктуру до решти світу.

Мережа Європейського Союзу та Директива про інформаційну безпеку (Директива NIS) набула чинності 8 серпня 2016 р. і повинна бути перенесена в національне право усіх держав-членів до 9 травня 2018. Вона являє собою перші зусилля на регіональному рівні щодо гармонізації кібербезпеки та вимог до повідомлень, орієнтованих на «операторів істотної послуги» (OESs) та «постачальників цифрових послуг» (DSPs).

OESs є європейським еквівалентом постачальників критичної інфраструктури в США. Директива NIS дає державам-членам ЄС відповідальність на ідентифікацію OESs на своїй території до 9 листопада 2018 року. Щоб полегшити цей процес, Директива NIS містить наступні вказівки в Статті 5 (2): «Критерії ідентифікації операторів основних послуг [...] є такими:

суб'єкт господарювання надає послугу, яка є необхідною для підтримки критичної суспільної та / або господарської діяльності;

надання цієї послуги залежить від мережі та інформаційної системи;

інцидент буде мати значний руйнівний вплив на надання цієї послуги.

Директива NIS була розроблена протягом трьох років у відповідь на Пропозицію Європейської комісії 2013 року і встановлює заходи щодо досягнення високого загального рівня безпеки та мережевих та інформаційних систем всередині Союзу з тим, щоб поліпшити функціонування внутрішнього ринку. Розробка Директиви була ітераційним процесом, який включав громадські консультації і опитування, семінари з такими організаціями, як Європейське агентство з мереж та інформаційної безпеки (ENISA), активне партнерство між урядом та приватним сектором. Зміст Директиви є широкомасштабним, але орієнтованим насамперед на створення кооперативних механізмів, що допомагають регіональним зусиллям посилення CIP (Critical Infrastructure Protection) разом з параметрами перенесення цієї Директиви до національного законодавства для країн-членів ЄС.

Цими директивами є:

– встановлення зобов'язання всіх

держав-членів щодо ухвалення національної стратегії відносно безпеки мережевих та інформаційних систем;

– створення групи співробітництва для підтримки та сприяння стратегічній співпраці та обміну інформацією між державами-членами, для розвитку довіри серед них;

– створення мережі команд для реагування на інциденти, пов'язані з мережевою небезпекою для участі в роботі, для розвитку довіри між державами-членами та для швидкого та ефективного заохочення до оперативного співробітництва;

– встановлення вимоги щодо безпеки та повідомлень для операторів основних служб та цифрових постачальників послуг;

– встановлення зобов'язання держав-членів щодо призначення національних компетентних органів, єдиних пунктів контактів та пунктів з завданнями, пов'язаними з безпекою мережевих та інформаційних систем.

Хоча ЄС випустив свої загальні дані Положення про захист у 2016 році для посилення безпеки, директива NIS, яка була видана в тому ж році, не включала обмежень щодо транскордонної передачі даних для CIP. Що стосується схеми сертифікації безпеки, то в Директиві зазначено, що «держави-члени ... заохочують використання Європейських чи міжнародних стандартів та специфікацій, що стосуються безпеки мережевих та інформаційних систем». Держави-члени ЄС, як очікується, використовуватимуть Директиву як базову лінію для їх підходу до кібербезпеки (зокрема, що стосується CIP), з адаптації, та реалізації, які відповідають їх унікальним національним потребам. Директива також підкреслює, що основна увага повинна приділятися створенню стимулів для здійснення належного управління ризиками і прийняття стандартів та рішень з безпеки, а також, можливо, встановлення добровільної розширеної схеми сертифікації ЄС на основі існуючих схем в ЄС і на міжнародному рівні. Держави-члени ЄС активно розробляють керівні принципи для приведення у відповідність директиві NIS [8].

Критичній інфраструктурі багато уваги приділяється і в такій потужній країні, як Китай. Протягом минулого року Китай прагнув захисту його критичної інформаційної інфраструктури включенням Програми захисту критичної інформаційної інфраструктури (CIIP) у багато урядових стратегічних документів, законів та правил. До них відносяться:

1) Закон по кібербезпеці (листопад 2016 року);

2) Стратегія розвитку інформаційної кібербезпеки;

3) Документ по регулюванню перетину національнрих кордонів даними.

Перший документ стосується національної кібербезпеки. Другий представляє огляд кібербезпеки у межах країни. Третій вже складає саму кібербезпеку.

У рамках реалізації Китайського Закону про кібербезпеку, який набрав чинності 1 червня 2017 р., Кібернетичне управління Китаю (CAC) випустило проект правил CIIP для публічних коментарів 11 липня 2017 року. Він складається з восьми глав і 55 статей, написаних згідно постанові «Про забезпечення безпеки критичної інформаційної інфраструктури» та відповідно до Закону «Про кібербезпеку Китаю».

Хоча багато урядів визначили сферу застосування Захисту критичної інфраструктури подібним чином, є виразна, але важлива різниця в термінах щодо того, як китайський уряд застосував цей термін як «критична інформаційна інфраструктура захисту» (CIIP), включивши як традиційні сектори, так і великі комерційні Інтернет-послуги, в тому числі електронну комерцію, пошук та соціальні медіа. США та ЄС визначають захист критичної інфраструктури (CIP), включаючи в неї в основному традиційні сектори та промислові системи. Уряд США робить прагнення звузити область визначення критичної інфраструктури, щоб зосередитися на захисті найбільш критичних суспільних послуг.

Сучасне визначення постачальника критичної інформаційної інфраструктури в рамках Положення проекту CIIP CAC, у статті 18, включає в себе наступне:

• державні департаменти та організації у таких галузях, як енергетика, фінанси, транспорт, охорона здоров'я, медичне обслуговування, освіта, соціальне забезпечення, охорона навколишнього середовища та комунальні послуги;

• оператори інформаційних мереж, такі як телекомунікаційні мережі, радіо та телебачення, Інтернет, а також організації забезпечення хмарних обчислень, великих даних та інші широкомасштабні послуги громадської інформаційної мережі;

• дослідницькі установи та виробничі підприємства в таких галузях, як національна оборона, наука і техніка, виробники великого обладнання, хімічне машинобудування, харчова промисловість, ліки;

• прес-агентства, такі як радіостанції, телестанції та інформаційні агентства;

• інші ключові організації.

У статті 19 проекту Регламенту окреслено агентства, що відповідають за CIIP в наступній формі: агентства з управління Інтернетом працюватимуть із Державною агенцією з управління телекомунікаціями та органами громадської безпеки для розробки керівних принципів для ідентифікації ICI, і ці державні сектори будуть очолюватися відповідними урядовими агенціями / міністерствами для ідентифікації ICI в їх відповідних галузях.

Положення статті 29 та 34 Проекту CIIP Кібернетичного управління Китаю вимагають розміщення даних у визначеному місці. Стаття 29 зазначає, що «особиста інформація та важливі дані, зібрані та створені операторами (CII) протягом їхніх операцій в Народній Республіці Китай, зберігатимуться в Китаї». У статті 34 зазначено, що «експлуатація та обслуговування інформаційної критичної інфраструктури буде проводитися в Китаї».

Хоча вимоги зберігання даних і їх розташування в межах територіальних кордонів може гарантувати доступ уряду до даних і операційної інформації, загалом конкретне місцеположення не гарантує покращення безпеки даних або операцій. У глобалізованій економіці певні обмеження навколо даних і операції матимуть вплив на комерційну діяльність та обмін даних, у тому числі пов'язаних з міжнародними банківськими послугами, транспортом, охороною здоров'я, відновлення після аварій та природних катаклізмів, наукових досліджень тощо. В окремому випадку CAC завершила свій третій перегляд політики передачі даних через кордон. Ця процедура ще не завершена повністю. Як керувати потоками даних та обмеженнями операційної роботи в країні з експоненціальним зростанням використання Інтернету і міцною міжнародною торгівлею, залишається ще невирішеною проблемою. Важливо розглянути вплив такої політики на шляху глобальної торгівлі та впровадження передових технологій як у приватних, так і в громадських секторах для керування цифровими перетвореннями по всьому світу.

Орган стандартизації національної безпеки Китаю TC260 вже просуває свою роботу на кількох стандартах, орієнтованих на CIIP з участю державних, академічних та галузевих фахівців. Крім того, Міністерство громадської безпеки Китаю керує багаторівневою схемою захисту (MLPS) протягом останніх десяти років. MLPS – це система ризику, що включає систему класифікації та сертифікації безпеки для IT-систем. Критична інфраструктура, в тому числі державні системи, визначаються як «Рівень 3 та вище» на підставі їх потенційного впливу на національну безпеку.

«Безпечні та керовані» використовуються як основні дві вимоги до забезпечення безпеки в Китаї. Ці політичні цілі було викладено в Китайському Законі «Про кібербезпеку» і вони використовуються як основа для управління закупівлями відповідних технологій CIIP. Статті 30-32 Проекту CIIP цих положень CACI вимагають, щоб всі оператори ICI точно керували безпекою їх постачальників, включаючи віддавання тих товарів чи послуг, які можуть впливати на національну безпеку, на оцінку безпеки за допомогою Наказу з кібербезпеки Департаменту CAC. Передача будь-яких транскордонних даних щодо CIIP також підпадає під дію Наказу з кібербезпеки.

У поєднанні ці стратегії, закони, нормативні акти, і стандарти складають амбітні та складні системи управління CIIP в Китаї.

Прикладом великого прориву, а потім і великої катастрофи в стані критичної інфраструктури Китаю стала гребля «Три Ущелини». Про будівництво цієї греблі мріяв ще сам Мао Цзедун. Роботи почалися в 1994 році і закінчилися в 2006 році. Резервуар довжиною в 660 км, утворений в результаті будівництва греблі, до 2010 року повністю заповнився водою, в результаті чого були затоплені 13 міст, 140 селищ і 1350 сіл.

Уряд Китаю вперше визнав, що будівництво найбільшої в світі греблі «Три Ущелини» привело до цілого ряду проблем, які необхідно терміново вирішувати. Місцева влада давно вже скаржилася на проблеми, викликані

будівництвом греблі. У 2007 році на скликаній китайською владою конференції представники місцевої влади попереджали про можливість катастрофи.

Із зони будівництва греблі «Три Ущелини» було виселено понад мільйон людей. Однією з основних проблем є зміна рівня води в резервуарі, що призводить до частих обвалів. Критики також стверджують, що уряд міг надати велику допомогу вимушеним переселенцям.

У заяві Держради, йдеться, що для евакуйованих необхідно створити додаткові робочі місця, збільшити програми соціального захисту, а також поліпшити систему транспорту. Суперечки навколо греблі почалися ще до початку її будівництва. Третина депутатів Всекитайських зборів народних представників проголосували проти цього проекту, або утрималися від голосування. У заяві Держради кажуть, що про багато проблем, пов'язаних зі зведенням «Трьох ущелин», було відомо ще до початку будівельних робіт[9].

У заяві Державної Ради Китаю, приділяється велика увага досягненням будівельників. У документі говориться, що в результаті будівництва «Трьох ущелин» зменшився ризик повеней, покращилася навігація на річці Янцзи і збільшилося виробництво електроенергії. Однак далі в заяві йдеться про те, що тепер необхідно вирішити ряд серйозних проблем, як, наприклад, поліпшення життєвих умов людей, які були змушені покинути свої будинки через будівництво греблі, захист навколишнього середовища і запобігання геологічних катастроф. Будівництво греблі обійшлося країні в суму близько 40 мільярдів доларів і піддавалося серйозній критиці з боку екологів.

Незалежно від складу та географічного розташування операторів критичної інфраструктури та постачальників технологій, дуже важливо, що державні політики CIP підтримують характеристики гнучкого, масштабованого, галузевого та технологічного. В табл. 1 наведено стислий огляд підходів захисту критичної інфраструктури, що використовуються урядами США, ЄС і Китаю.

Таблиця 1

Порівняльний аналіз підходів до захисту критичної інфраструктури в США, ЄС, Китаї

Підходи до захисту критичної інфраструктури	США	ЄС	Китай
Інституції початкової політики Захисту критичної інфраструктури	Виконавчий порядок та структура Національного інституту стандартів та технологій з кібербезпеки	Директиви (закони) мережі інформаційної безпеки	Китайські закони з кібербезпеки. Проект Регламенту захисту критичної інформаційної інфраструктури. Положення щодо передавання даних через державний кордон. Регламент з регулювання кібербезпеки. Схема багаторівневого захисту.
Участь приватного сектору під час законодавчого процесу	Так	Так	Відсутня
Канали зворотного зв'язку до основного законодавства	Семінари та запити щодо інформації	Громадські консультації; опитування	Період 30-денних громадських коментарів
Визначення критичної інфраструктури на основі ризиків	Так	Так	Так
Дані та операції щодо вимог розміщення	Немає	Немає	Так
Підтвердження глобальних стандартів	Так	Так	Немає

Висновки. США, Європейський Союз та Китай – кожна з цих країн залишається в стадії формування етапів розробки їх підходів до CIP. Важливим документом по структура кібербезпеки є NIST, він удосконалюється, оновлюється. На цей момент Директива NIS є попередницею асоційованих законів, що приймаються державами-членами ЄС. Регламент CIIP Китаю залишається у формі проекту, в той час як проект критичної інформаційної інфраструктури очікується, що буде представлений в найближчому майбутньому.

Варто зазначити, що існують відмінності між США, ЄС і Китаєм з точки зору ролі приватного сектора. США та ЄС сприяють ідеї участі приватного сектора під час законодавчого процесу, а у відповідь – приватний сектор розглядає підтримку як обов'язок надання внесків та очікування щодо політики CIP. Китайський уряд також розглядає як важливу складову підвищену прозорість цієї політики. Незважаючи на те, що на протязі офіційного процесу немає законодавчо встановлених дій для приватного сектора, китайський уряд зазвичай використовує 30-денний період, на протязі якого відбувається публічне обговорення для збору відгуків суспільства незадовго до перегляду цієї політики. Крім того, оператори традиційної критичної інфраструктури є приватними особами в США та ЄС, в той час, як більшість операторів у подібних секторах CIP в Китаї належить державі, крім сектору послуг Інтернет-мережі.

Список використаних джерел

1. Critical Infrastructure Hrotection. Additional Actions by DHS Could Help Identify Opportunities to Harmonize Access Control Efforts. URL: https://www.gao.gov/assets/690/682547.pdf (дата звернення: 15.07.2019).

2. Сметана М. Защита критической инфраструктуры. Подходы государств Европейского Союза к определению элементов критической инфраструктуры. 2014. 60 с.

3. Sector Resilience Plan for Critical Infrastructure. URL: https://www.gov.uk/government/uploads/system/ (дата звернення: 15.07.2019).

4. NotBeingPetya: UK critical infrastructure firms face huge fines for lax security. URL: https://www.theregister.co.uk/2017/08/08/critical_infrastructure_firms_threatened_with_huge_fines_for_lax_security/ (дата звернення: 15.07.2019).

5. Gordon, Kathryn, Dion Maeve. Protection of Critical Iinfrastructure and the Role of Investment Policies relating to National Security. Paris : OECD, 2008. 11 p.

6. Direction protection et sécurité de l'etat, Instruction generale interministerielle relative a la securite des activites d'importance vitale, N°6600/SGDSN/PSE/PSN DU 7 janvier 2014.

7. Goto Atsuhiro. Keeping Critical Infrastructure Safe and Secure During the Olympics/Paralympics and Beyond. URL: http://www8.cao.go.jp/cstp/panhu/sip_english/43-44.pdf (дата звернення: 15.07.2019).

8. Підходи до захисту критичної інфраструктури. URL: https://www.wilsoncenter.org/sites/default/files/approach_to_critical_infrastructure_protection.pdf (дата звернення: 15.07.2019).

9. Плотина «Три Ущелья» создала Китаю серьезные проблемы. URL: http://www.bbc.com/russian/international/2011/05/110519_china_three_gorges$ (дата звернення: 15.07.2019).

10. Ващишин А. О., Сазонець О. М. Європейський досвід управління безпекою критичної інфраструктури. *Актуальні проблеми теорії і практики менеджменту в умовах євроінтеграції* : зб. тез VII Міжнародної науково-практичної конференції. Рівне. 2018. С. 343–346.

References

1. Critical Infrastructure Hrotection. Additional Actions by DHS Could Help Identify Opportunities to Harmonize Access Control Efforts. URL: https://www.gao.gov/assets/690/682547.pdf (data zvernennia: 15.07.2019).

2. Smetana M. Zashchita kriticheskoi infrastruktury. Podkhody hosudarstv Evropeiskoho Soiuza k opredeleniiu elementov kriticheskoi infrastruktury. 2014. 60 s.

3. Sector Resilience Plan for Critical Infrastructure. URL: https://www.gov.uk/government/uploads/system/ (data zvernennia: 15.07.2019).

4. NotBeingPetya: UK critical infrastructure firms

face huge fines for lax security. URL: https://www.theregister.co.uk/2017/08/08/critical_infrastructure_firms_threatened_with_huge_fines_for_lax_security/ (data zvernennia: 15.07.2019).
5. Gordon, Kathryn, Dion Maeve. Protection of Critical Iinfrastructure and the Role of Investment Policies relating to National Security. Paris : OECD, 2008. 11 p.
6. Direction protection et sécurité de letat, Instruction generale interministerielle relative a la securite des activites dimportance vitale, N°6600/SGDSN/PSE/PSN DU 7 janvier 2014.
7. Goto Atsuhiro. Keeping Critical Infrastructure Safe and Secure During the Olympics/Paralympics and Beyond. URL: http://www8.cao.go.jp/cstp/panhu/sip_english/43-44.pdf (data zvernennia: 15.07.2019).
8. Pidkhody do zakhystu krytychnoi infrastruktury. URL: https://www.wilsoncenter.org/sites/default/files/approach_to_critical_infrastructure_protection.pdf (data zvernennia: 15.07.2019).
9. Plotina «Tri Ushchelia» sozdala Kitaiu sereznye problemy. URL: http://www.bbc.com/russian/international/2011/05/110519_china_three_gorges$ (data zvernennia: 15.07.2019).
10. Vashchishin A. O., Sazonets O. M. Yevropeiskyi dosvid upravlinnia bezpekoiu krytychnoi infrastruktury. *Aktualni problemy teorii i praktyky menedzhmentu v umovakh yevrointehratsii* : zb. tez VII Mizhnarodnoi naukovo-praktychnoi konferentsii. Rivne. 2018. S. 343–346.

УДК 330.341.1 (477) https://doi.org/10.31713/st1-2201918
JEL : F 50, L 26, O 33

Саленко А. С.,
головний державний ревізор-інспектор
ДПІ у Печерському районі ГУ ДФС, м. Київ

НАУКОВО-МЕТОДИЧНІ ПІДХОДИ ДО ВИЗНАЧЕННЯ ВИРОБНИЦТВ ЯК ВИСОКОТЕХНОЛОГІЧНИХ КРАЇНАМИ СВІТУ ТА МІЖНАРОДНИМИ ОРГАНІЗАЦІЯМИ

Salenko A. S.,
Chief State Inspector
STI in the Pechersk district of the Main Office
State Fiscal Service, Kyiv

SCIENTIFIC AND METHODICAL APPROACHES TO THE DEFINITION OF PRODUCTIONS AS HIGH-TECH TECHNICAL COUNTRIES OF THE WORLD AND INTERNATIONAL ORGANIZATIONS

Визначено, що високі технології є основою виробництва товарів та послуг. Подано приклади класифікації високих технологій, найбільш детально проаналізовано класифікацію високих технологій ОЕСР, Найбільш популярною для використання в світ та в Україні є класифікація високих технологій є класифікація, що надається ОЕСР. Визначено, що достатньо повною та сучасною є система визначення переліку високих технологій, що запропонована в ЄС. Проаналізовано міжнародні нормативні документи, що визначають особливості розвитку сфери підприємництва враховують інноваційність та технологічність сучасної економіки.

It is determined that high technologies are the basis of production of goods and services. Examples of high technology classification are given, the OECD high technology classification is analyzed in the most detail, the most popular for use in the world and the high technology classification in Ukraine is the OECD classification. It is determined that the system of definition of the