Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.

Державне управління: удосконалення та розвиток. 2024. № 5.

DOI: http://doi.org/10.32702/2307-2156.2024.5.1
УДК 351.861

А. Л. Помаза-Пономаренко,
д. держ. упр., старший дослідник, начальник наукового відділу проблем державної безпеки, Навчально-науково-виробничий центр Національного університету цивільного захисту України
ORCID ID: https://orcid.org/0000-0001-5666-9350
Д. В. Тарадуда,
к. техн. н., доцент, заступник начальника кафедри організації та технічного забезпечення аварійно-рятувальних робіт, Національний університет цивільного захисту України
ORCID ID: https://orcid.org/0000-0001-9167-0058

ВЕКТОРИ ЗАБЕЗПЕЧЕННЯ СТІЙКОГО ФУНКЦІОНУВАННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ Й ОБ'ЄКТІВ ПІДВИЩЕНОЇ НЕБЕЗПЕКИ В УКРАЇНІ ТА ЗА КОРДОНОМ

A. Pomaza-Ponomarenko,
Doctor of Sciences in Public Administration, Senior Researcher, Head of the Scientific Department for State Security Problems, Training Research and Production Centre of National University of Civil Protection of Ukraine
D. Taraduda,
PhD in Technical Science, Associate professor, Deputy Head of Department of Organization and Technical Support of Emergency Rescue Works, National University of Civil Protection of Ukraine

VECTORS OF ENSURING SUSTAINABLE FUNCTIONING OF CRITICAL INFRASTRUCTURE FACILITIES AND FACILITIES OF INCREASED DANGER

Виявлено, що повномасштабна агресія рф проти України зумовлює значне збільшення надзвичайних ситуацій на об'єктах критичної інфраструктури й об'єктів підвищеної небезпеки. Ця агресія спрямована на дестабілізацію публічної (громадської та цивільної) безпеки, що актуалізувало низку існуючих публічно-управлінських проблем у сфері такої безпеки України. Зокрема, тих, що стосуються попередження надзвичайних ситуацій на об'єктах критичної інфраструктури й об'єктах підвищеної небезпеки. Ці об'єкти в різній мірі становлять загрозу для життя та здоров'я населення, а також окремо взятих територій України. Визначено, що у світі застосовуються різні наукові підходи до визначення об'єктів критичної інфраструктури, серед яких найбільш часто використовують саме секторальний підхід. Він передбачає визначення пріоритетних питань інформаційного обміну, тому що для підвищення обізнаності про захист об'єктів критичної інфраструктури обидві сторони (уряди та оператори цих об'єктів) повинні результативно взаємодіяти під час забезпечення публічної безпеки. З'ясовано, що для забезпечення конфіденційності обміну інформацією найбільш широко використовується Протокол світлофора (TLP), який вважається однією з найкращих практик. Установлено, що з метою розвитку передової практики інформаційного обміну деякі країни створили невеликі довірені спільноти, в яких можна обмінюватися інформацією безпечним та надійним способом. Один із таких прикладів є платформи обміну, розроблені в ЄС – Інформаційна мережа попередження на об'єктах критичної інфраструктури. Ця мережа є ініціативою Європейської комісії, яка координується її Генеральним директоратом із внутрішніх справ. З огляду на це рекомендується Україні доєднатися до цієї мережі з метою впровадження її алгоритмів. Уважаємо, що це має підвищити рівень соціальної безпеки України.

It was found that the Russian Federation's full-scale aggression against Ukraine causes a significant increase in emergency situations at critical infrastructure facilities and high-risk facilities. This aggression is aimed at destabilizing public (public and civil) security, which actualized a number of existing

public-management problems in the sphere of such security in Ukraine. In particular, those related to the prevention of emergency situations at critical infrastructure facilities and high-risk facilities. To varying degrees, these objects pose a threat to the life and health of the population, as well as individual territories of Ukraine. It was determined that various scientific approaches to the definition of critical infrastructure objects are used in the world, among which the sectoral approach is most often used. It provides for the identification of priority issues of information exchange, because in order to raise awareness about the protection of critical infrastructure facilities, both parties (governments and operators of these facilities) must effectively interact while ensuring public safety. It was found that the Traffic Light Protocol (TLP), which is considered one of the best practices, is the most widely used to ensure the confidentiality of information exchange. It has been established that in order to develop best practices in information sharing, some countries have created small trusted communities where information can be shared in a safe and secure way. One such example is the exchange platforms developed in the EU - the Information Network of Warning on Critical Infrastructure Objects. This network is an initiative of the European Commission, coordinated by its Directorate-General for Home Affairs. In view of this, it is recommended that Ukraine join this network in order to implement its algorithms. We believe that this should increase the level of social security of Ukraine.

***Ключові слова**: публічне управління, національна безпека, публічна безпека, цивільний захист, соціальна безпека, соціальний захист, надзвичайні ситуації, об'єкти підвищеної небезпеки, об'єкти критичної інфраструктури, забезпечення стійкого функціонування об'єктів інфраструктури, ЄС, США.*

***Keywords:** public administration, national security, public safety, civil protection, social security, social protection, emergency situations, high-risk facilities, critical infrastructure facilities, ensuring sustainable functioning of infrastructure facilities, EU, USA.*

Постановка проблеми. Одним із ключових факторів соціального розвитку, забезпечення обороноздатності й економічної безпеки держав є

інфраструктура. Уперше термін «інфраструктура» (лат. infra – «нижче», «під» та лат. structura – «будова», «розташування») з'явився 1920–1928 р.р. серед військових. Цю категорію визначали, як «комплекс взаємопов'язаних обслуговуючих структур або об'єктів, що складають та забезпечують основу функціонування системи, що забезпечують дію збройних сил» [6; 8]. На сьогодні поняття інфраструктури дещо змінилось, але найголовніша сутнісна ознака залишилася тією ж - інфраструктура повинна забезпечувати задоволення найважливіших інтересів населення, що може відбуватися в різних піднапрямках.

Умови сьогоднішньої ситуації в Україні вимагають приділення особливої уваги розвитку теорії ризиків виникнення надзвичайних і кризових ситуацій, кількість яких збільшується через повномасштабну агресію рф на об'єктах критичної інфраструктури й об'єктах підвищеної небезпеки. Відтак, набувають актуальності питання, пов'язані з вчасним попередженням надзвичайних ситуацій, що можливо за допомогою впровадження комплексного моніторингу й управління такими ситуаціями. Система такого управління у своїй основі повинна мати міцний науково-методичний фундамент, а зміст її має бути спрямований на набуття глибоких знань та вироблення практичних навичок та умінь діяти у різних ситуаціях [2; 3; 10; 11]. Усе це визначає актуальність обраної проблематики дослідження.

Аналіз останніх досліджень і публікацій. Проблематика публічного управління щодо формування публічної (громадської, цивільної) безпеки є предметом як вітчизняних, так і зарубіжних учених В. Андронова, К. Бєлікова, Л. Берга, О. Бойко, А. Воденичарова, С. Калояннідіса, Е.Дж. Кіршнера, Н. Клименко, Ю. Ключки, О. Крюкова, О. Лещенко, П. Махортова, О. Подскальної, С. Потерійка, В. Терент'євєвої, О. Твердохліба, В. Чжу, М. Хойтинк та ін. [1; 2; 3; 8; 9].

Постановка завдання. Метою статті є визначення векторів забезпечення стійкого функціонування об'єктів критичної інфраструктури й об'єктів підвищеної небезпеки в Україні та за кордоном.

Виклад основного матеріалу. Поняття «інфраструктура» є одним із ключових у розвитку різних сфер життя. При цьому «критична інфраструктура» це та категорія, довкола якої вибудовуються питання життєздатності всіх країн. Актуальними сьогодні на міжнародному рівні є питання ведення інформаційного протистояння, у межах якого задіяними виявляються багато галузей, що є елементами критичної інфраструктури [там само]. В основі визначення «критична інфраструктура» закладено поняття «критичність». У низці визначень це поняття застосовне до тієї складової категорії «інфраструктура», яка співвідноситься з питаннями безпеки та реалізації ключових функцій. В інженерії критичність може розглядатися як векторна властивість систем різного функціонального призначення відповідно до [9] «критичний – найважливіший, вирішальний, визначальний». Критичність визначається з урахуванням властивостей та функцій досліджуваного об'єкта. Як складові критичності виділяють: безпеку (надійність), результативність наслідків, можливість мінімізації ймовірності виникнення наслідків [там само]. Одним із показників критичності є структурна критичність (важливість, надійність).

Отже, для формування загального уявлення про категорію «критична інфраструктура» (далі – КІ), під час дослідження проаналізовано визначення критичної інфраструктури з таких класів визначень:

1) європейські визначення (згідно з Директивою Ради 2008/114/ Європейського Союзу (ЄС);

2) інші міжнародні визначення: НАТО (CCD – CoE (Талліннське) керівництво), MCE-T, CEP/EAPC), UNISDR;

3) національні визначення (визначення, введені у наступних країнах – Австралія, Австрія, Барбадос, Бельгія, Бразилія, Болгарія, Канада, Колумбія, Хорватія, Куба, Кіпр, Чехія, Данія, Ефіопія, Фінляндія, Франція, Німеччина, Греція, Ірландія, Ізраїль, Ямайка, Японія, Кенія, Королівство Саудівська Аравія, Косово, Латвія, Литва, Люксембург, Мальта, Мексика, Молдова, Чорногорія, Нідерланди, Безпеки та розвідки (AIVD)), Нова Зеландія, Норвегія, Пакистан,

Філіппіни, Польща, Португалія, Катар, Румунія, Російська Федерація, Іспанія, Швеція, Швейцарія, Туреччина, Україна, Великобританія, США (Патріотичний закон, DoD, NIST) та ін.;

4) стандартне визначення (визначення стандартів ІСО/МЕК ТР 27019:2013, IETF);

5) інші ухвали (ухвали Міжнародної ради з управління ризиками (IRCG), CCD-CoE НАТО, Онтаріо (Канада)) [8; 9].

У всіх терміноконструкціях КІ визнається як життєво важлива функція послуг, наданих активом суспільству. Більшість країн визначають інфраструктуру як критично важливу, якщо її руйнація матиме загальнонаціональні наслідки. Однак предмет впливу незначно варіюється від країни до країні. Наприклад, у США наслідки руйнування критично важливої інфраструктури безпосередньо пов'язані з національною безпекою та безпекою громадян й економіки. В ЄС загальнорегіональне визначення включає економічне та соціальне благополуччя. Визначення НАТО також включає будь-який вплив на навколишнє середовище. Отже, наявні різні підходи до визначення поняття КІ. Результати аналізу даних визначень дозволили охарактеризувати КІ як базове на міжнародному рівні європейське визначення, якого дотримуються найбільша кількість країн. Крім того, наразі активно розвивається категорія «критична інформаційна система» [9].

Варто відзначити, що, незважаючи на різноманітність підходів у визначенні КІ, виявлено – значимість КІ на всіх рівнях держави, що послаблює соціально-економічний ефект розвитку суспільства у разі порушення роботи КІ. Це насамперед актуалізує проблему забезпечення безпеки КІ у тому числі, з урахуванням інфраструктурних залежностей та зв'язків, на рівні світової спільноти. Ідея концептуалізації питань забезпечення безпеки критичної інфраструктури (далі – БКІ) не нова. Захист стратегічних національних ресурсів та активів була частиною планування національної оборони ще за часів Другої світової війни. Однак сьогодні значний вплив на сприйняття Урядами БКІ та способів його вирішення обумовлюється пріоритетами безпеки,

довгостроковості цілей розвитку та фінансовими міркуваннями. Виходячи з цього, країни намагаються ідентифікувати та захистити свої критично важливі активи від різнохарактерних загроз. Вихідною точкою тут є узгоджена державна політика та правове середовище.

Довгострокова політика у сфері розвитку суспільства та держави залежить від цілісності КІ. Так, ще у 2014 році у Доповіді про світовий розвиток за 2014 рік зроблено акцент на стійкості та надійності інфраструктур як важливому факторі національного прогресу, позначено підходи до планування політики, що ґрунтуються на оцінці ризиків, як потужному інструменті для розвитку. Розвиток КІ, систем БКІ історично склався неоднозначно: залежно від специфіки та рівня розвитку країн. Так, загрози економічному та соціального благополуччя громадян стали основними рушійними силами для створення системи захисту КІ ЄС, що є економічним та політичним партнерство між 27 європейськими країнами. В ЄС КІ була визначена як актив або система, яка необхідна для підтримки життєво важливих громадських функцій (ЄС, 2008). У результаті сформовано загальний підхід країн – членів ЄС до БКІ (див. табл. 1).

Цей підхід ґрунтується на трьох стратегіях:

1) Спеціальна стратегія БКІ, широко відома як Європейська програма захисту критичної інфраструктури (EPCIP), яка була прийнята в 2004;

2) Стратегія європейської безпеки (з 2003 року);

3) Європейська стратегія внутрішньої безпеки (з 2010 року).

З погляду управління та практичної реалізації на рівні ЄС процес захисту КІ розділений на три етапи: ідентифікація, призначення та захист КІ.

Таблиця 1. Ключові політичні та правові документи, що формують структуру БКІ в ЄС

Рік	Назва	Короткий опис документа
2003	Європейська стратегія безпеки, 12 грудня 2003 року (ЄС, 2003)	Визначає середовище безпеки ЄС, ключові проблеми безпеки та подальші політичні наслідки для ЄС. Забезпечує концептуальну основу для спільної безпеки й оборонної політики
2004	Європейська програма захисту критично важливих об'єктів інфраструктури (EPCIP) (ЄС, 2004)	Документ високого рівня, який визначає основні засади БКІ для ЄС. Визнано та описано загрози, які можуть призвести до втрати життєво важливих послуг
2006	Повідомлення Комісії з EPCIP від 12.12.2006 COM (2006) 786 фінал (ЄС, 2006)	Пояснювальний документ щодо сприяння впровадженню EPCIP на національному рівні.
2008	Директива 2008/114 про визначення європейських найважливіших інфраструктур та оцінку необхідності їх захисту (ЄС, 2006)	Визначає принципи та процедури для визначення КВ на рівні ЄС чи національній КІ, яка визнана КІ на рівні ЄС
2010	Стокгольмська програма – Відкрита та безпечна Європа, що служить та захищає громадян, 2010/C 115/01 (ЄС, 2010)	Формулює дорожню карту для роботи ЄС заради справедливості, свободи та безпеки
2010	Повідомлення Комісії Європейському парламенту та Раді про Стратегію внутрішньої безпеки ЄС у дії: п'ять кроків на шляху до більш безпечної Європи, 22.11.2010 COM(2010) 673 фінал (ЄС, 2010a)	Виявляє й усуває загальні загрози безпеці ЄС, такі як національні катастрофи, злочинні мережі та радикалізація
Підтверджуючі документи		
2012	Робочий документ працівників Комісії з огляду EPCIP SWD(2012) 190 (ЄС, 2012a)	Узагальнює результати огляду Директиви EPCIP та CIP
2013	Робочий документ співробітників Комісії з нового підходу до EPCIP, 28.8.2013 SWD (2013) 318 остаточний (ЄС, 2013)	Установлює новий підхід до EPCIP, заснований на трьох основних принципах: запобігання, готовність та реагування

Джерело: складено на підставі [8; 9; 12]

З 2013 року ЄС реалізовував новий підхід до Європейської програми БКІ. Пілотний проект спрямований на оптимізацію захисту та стійкості

чотирьох вибраних європейських критичних інфраструктур: Європейська організація з безпеки аеронавігації (Євроконтроль), Galileo – глобальна навігаційна інфраструктура під цивільним контролем. Генеральний директорат з міграції та внутрішніх справ є структурним підрозділом Єврокомісії та провідною організацією щодо формування плану БКІ межах Єврокомісії [3].

Об`єднаний дослідницький центр (JRC), власний дослідницький центр Європейської комісії – підтримує діяльність з оцінки й аналізу. ЄС використовує секторальні критерії визначення КІ. Критерії наведено у документі Європейської сертифікації фахівців у галузі інформатики на основі тяжкості наслідків порушення чи руйнування, яка оцінюється на основі суспільного ефекту, економічного ефекту, впливу на довкілля, політичного ефекту. Як тільки КІ ідентифіковано, її власники/оператори роблять певний набір дій розробки Плану безпеки Оператора. Директива БКІ уповноважує органи влади у державах-членах відповідати за забезпечення відповідності КІ її вимогам. Уряд кожної країни обирає, який конкретний орган чи органи несуть відповідальність за впровадження системи БКІ, за належне включення положень на рівні ЄС до свого національного законодавство [5].

Більшість найважливіших секторів інфраструктури у Фінляндії перебуває у приватній власності. Компанії державного сектора у більшій частині надають кібернетичні ноу-хау й експертні знання, а також послуги у сфері безпеки та захисту. З цієї причини національний підхід до політики та законодавства БКІ спрямований на підвищення компетенцій безпеки КІ у рамках підприємницької діяльності, на підвищення обізнаності та зміцнення співпраці між приватним сектором та відповідними органами БКІ. Згідно з політикою Фінляндії у сфері безпеки й оборони у 2004 роки ІКТ були визначені як один із найважливіших секторів інфраструктури. Фінляндія більше орієнтована на стійкість КІ, ніж на захист. Маючи економіку, яка значною мірою залежить від індустрії ІКТ, стратегія БКІ Фінляндії приділяє значну увагу загроз кібербезпеці [8; 9].

В Англії КІ визначається як інфраструктурні активи (фізичні або

електронні), які життєво важливі для подальшого надання основних послуг, втрата яких призведе до суттєвих економічних чи соціальних наслідків (табл. 2). Імпульсом до зміцнення системи БКІ в Англії послужили руйнівні повені 2007 р. За результатами аналізу того, що сталося, було збудовано міжсекторальну компанію за участю власників/операторів, що регулюють діяльність органів й уряду для підвищення стійкості КІ та основних послуг.

Стратегія національної безпеки визначає загальний підхід до БКІ Великобританії та спрямована на забезпечення безпечного та стійкого середовища в контексті вибраних ризиків. З 2008 року уряд Великобританії проводиться щорічна національна оцінка ризиків (NRA). Хоча NRA є конфіденційною оцінкою, уряд публікує документ, відомий як Національний реєстр ризиків (NRR) [9]. Відповідно до останньої Стратегії національної безпеки Великобританії (Уряд Її Величності, 2010 р.) проводиться новий захід - Оцінка ризиків національної безпеки (NSRA) [8]. На відміну від NRA, NSRA виходить за рамки внутрішніх ризиків і повторюється кожні два року. У 2010 році уряд прийняв «Стратегічні рамки та політичну заяву про підвищення стійкості КІ до руйнувань внаслідок стихійних лих».

У 2011 році стратегічні рамки були доповнено «Керівництвом щодо підвищення стійкості критичної інфраструктури та основних послуг». Керівництво включає принципи стійкості інфраструктури, основи будівельних процесів та рекомендації з різних практик. Активи в рамках КІ визначаються як критичні з використанням Шкали критичності, яка надає категорії для різних ступенів серйозності впливу. Ці активи називаються ключовими точками. На галузевому рівні уряд Англії використовує секторальний підхід. Плани стійкості сектора складаються відповідно до NRAS. БКІ при секторальному підході здійснюється за допомогою незалежних оглядів, запрошених урядом для конкретного сектору. Вивчаючи секторальну політику для БКІ, Англія прийняла дві основні стратегічні рамки: Національну стратегію забезпечення інформаційної безпеки та Стратегію кібербезпеки (Кабінет міністрів Великобританії, 2015) [5; 6; 10].

Таблиця 2. Сектори критичної інфраструктури за кордоном і в Україні

Сектори КІ	ЄС	США	Фін-ляндія	Англія	Іспанія	Південна Корея	Україна	ФРН	Японія	Синга-пур
Енергетика	+	+	+	+	+	+	+	+	+	+
Транспорт	+	+	+	+	+	+	+	+	+	+
ІКТ та телезв'язок	+	+	+	+	+	+	+	+	+	+
Фінансовий сектор	+	+	+	+	+	+	+	+	+	+
Водопостачання	+	+	+	+	+	+		+	+	+
Сектор охорони здоров'я	+	+	+	+	+	+	+	+	+	+
Харчовий сектор	+	+	+	+	+					
Державний сектор		+		+		+	+			
Хімічна промисловість	+	+			+		+	+		
Сектор ядерної безпеки	+	+			+	+	+			
Служба порятунку		+		+						+
Сфера досліджень	+				+		+			
Космос, авіація	+				+		+			+
Критичні виробничі та енергетичні центри		+			+		+			
Греблі		+								
Комерційні об'єкти		+								
Оборона промисловість		+					+			
Засоби масової інформації			+							+
Обслуговування інфраструктури			+				+			
Навколишнє середовище						+				
Уряд										+
Усього	11	16	9	9	12	9	12	7	6	10

Джерело: складено на підставі [5; 6; 8; 9]

Іспанія є підходящим прикладом щодо швидкого розвитку структури БКІ. Основні зусилля в цій країні були зроблені у період із 2007 р. по 2013 р.

Країна прийняла стратегію БКІ, розробила плани, приділила особливу увагу загрозам кібербезпеки та створила каталог із вичерпним переліком національних критично важливих інфраструктурних активів. Наразі Іспанія концентрується на впровадженні та подальшому вдосконаленні своєї критичної інфраструктури у найважливіших сферах. Сектори КІ Іспанії не були чітко визначені до 2007 року, коли Секретаріат державної безпеки Іспанії затвердив Національний план захисту КІ. У 2007 році уряд Іспанії опублікував каталог із переліком національних найважливіших інфраструктур. Інфраструктури класифікуються відповідно до її вартістю чи «критичністю», та наслідками її втрати. Ця класифікація виконується з використанням шкали критичності.

У межах секторів існують певні критичні елементи інфраструктури, які називаються Ключовими точками. Найважливіші активи складають найважливішу національну інфраструктуру країни та окремо називаються інфраструктурними активами. Інфраструктурні активи можуть бути фізичними чи логічними. Шкала критичності включає три вимірювання: вплив на надання основних послуг у країні, економічні наслідки, впливом геть життя. Центр захисту національної інфраструктури Іспанії (CPNI) розробив заснований на загрозах підхід, який оцінює кожен Шкалі критичності у разі втрати. Значимість сектора та вплив на населення є ключовими чинниками щодо рейтингу події. Після оцінки кожного ключового пункту CPNI надає рекомендації щодо безпеки, які потім реалізуються державним департаментом-спонсором. БКІ Іспанії підпадає під стратегічні рамки національної безпеки в рамках першої Стратегії національної безпеки, яка була прийнята у червні 2011 р. [12]. У 2013 році була прийнята поточна Стратегія національної безпеки. Іспанія є однією з країн, де національний уряд наділяє повноваженнями провінційні та регіональні органи влади, які беруть участь у процесах БКІІ при координації уряду через державного секретаря з питань безпеки. Іспанія приділяє особливу увагу безпеці свого кіберпростору. Структуру БКІІ визначає Національний план КІ, узгоджений з Стратегією

кібербезпеки ЄС. Поточна Національна стратегія кібербезпеки була прийнята у 2013 р. Отже, можна говорити про застосування насамперед секторального підходу до визначення КІ практично у всіх країнах. При цьому практично у всіх країнах пріоритетними визнаються питання інформаційного обміну, тому що для підвищення обізнаності про захист об’єктів критичної інфраструктури обидві сторони (уряди й оператори цих об’єктів) повинні комплексно розуміти роль один одного у забезпеченні соціальної безпеки, а також деякі основні концепції.

Республіка Південная Корея (далі – РПК) розпочала свою кампанію з цифровізації у 1980-х роках та в результаті визнана була необхідність захисту цифрових записів, конфіденційності в Інтернеті та критичності інформаційної інфраструктури раніше, ніж інші країни. Це призвело до вчасних дій для стійкої експлуатації БКІ. Перший Закон РК про БКІІ було прийнято у січні 2001 року. Цей закон визначає КІ, а також заходи захисту та протидії кібер-інцидентам, визначає роботу консалтингових агенцій з ІБ, розглядає питання захисту, запобігання, контрзаходів, технічної підтримки, міжнародного співробітництва та покарання за кіберзлочини. У ньому також визначена структура управління БКІ та визначаються ролі та функції Комітету із захисту інформаційної інфраструктури (БКІ). Закон РПК про БКІ визначає національну КВ як «визначені об'єкти, які вважаються необхідними для постійного управління для захисту національних магістральних систем». У березні 2013 р. розпочалася підготовка до ухвалення урядом всеосяжної національної стратегії кібербезпеки – Національного комплексного плану кібербезпеки. Цей план був побудований на чотирьох основних принципах: оперативність, співпраця, надійність, креативність. Згідно з планом, критичні системи мають бути зашифровані, системи аварійного відновлення розширено, а важливі дані захищені. У національній інфраструктурі ІКТ відіграють вирішальну роль [8; 9].

У 2015 р. у РПК налічувалося 354 інфраструктури ІКТ, які були позначені як КІ. Ними керують 17 відповідних центральних адміністративних

установ та 209 керуючих організацій. Об'єкт, важливість якого визнана Міністерством науки РПК, ІКТ та планування майбутнього (MSIP) або Національною службою розвідки (NIS), Керівна організація оцінює з погляду можливості позначення його як КІІ. Комітет із захисту інформаційної інфраструктури (БКІ) підтверджує результати оцінки керуючої організації. Після цього, для цієї інфраструктури призначається керуюча організація. Функції її – це щорічне вжиття захисних заходів для пошуку й усунення нових уразливостей у короткостроковій перспективі, впровадження ефективної системи управління шляхом аналіз побічних ефектів від довгострокових інцидентів [там само].

Національні спроби захисту КІ США розпочалися 1998 року. Перший указ Президента з питань БКІ було видано 1998 року. У 2002 році Сполучені Штати також ухвалили Закон про реорганізацію та централізацію функцій безпеки на федеральному рівні, спрямований на протидію існуючим загрозам та викликам, Закон про національну безпеку (HSA). Цей закон забезпечує координацію та захист критично важливого інфраструктури. HSA також сприяло ухваленню Закону 2002 року про інформації про КІ (Закон КІ), який регулює обмін інформацією між операторами КІ та установами державного сектора. У Директиві, оновленій у 2003 році, докладно викладено положення щодо визначення та захисту КІ. Першою Стратегією національної безпеки передбачено підготовку Національного плану захисту інфраструктури (NIPP), який був опублікований у 2006 році. Поточний NIPP 2013 забезпечує керівництво зусиллями зацікавлених сторін підвищення безпеки та стійкості найважливіших інфраструктур по всій країні. З 2013 року Виконавчий указ 13636 «Підвищення кібербезпеки критичної інфраструктури» та Директива Президента про безпеку та стійкості КІ (PPD-21) регулюють рамки БКІ США. Політична місія уряду полягає у зміцненні безпеки та стійкості критично важливої інфраструктури країни шляхом управління фізичними та кібер-ризиками за допомогою спільних та комплексних зусиль спільноти КІ.

У США, як і в багатьох країнах, національний план складається із

секторальних підходів відповідно до вимог PPD-21. Він безпосередньо доручає галузевим агентствам (SSAS), керувати процесом співробітництва у сфері забезпечення БКІ. Поточний список із 16 найважливіших секторів інфраструктури було складено в 2013 році. Визначення критичних інфраструктур починається з оцінки ризиків на національному рівні. Зусилля уряду щодо виявлення КІ засновані на поетапний підхід. Протягом усього процесу враховуються три фактори ризику: фізичний, кібернетичний та людський. Це схоже на підхід Великобританії, яка враховує фактори фізичної, інформаційної та кадрової безпеки, а також РПК, що розглядає пов'язані з управлінням фізичні та технологічні фактори.

Висновки. Підсумовуючи акцентуємо, що важливо, щоб обмін управлінським досвідом у сфері визначення критичної інфраструктури був надійним і безпечним. З'ясовано, що для забезпечення конфіденційності обміну інформацією найбільш широко використовується Протокол світлофора (TLP), який вважається однією з найкращих практик. Установлено, що з метою розвитку передової практики інформаційного обміну деякі країни створили невеликі довірені спільноти, в яких можна обмінюватися інформацією безпечним та надійним способом. Один із таких прикладів є платформи обміну, розроблені в ЄС – Інформаційна мережа попередження на об'єктах критичної інфраструктури. Ця мережа є ініціативою Європейської комісії, яка координується її Генеральним директоратом із внутрішніх справ. З огляду на це рекомендується Україні доєднатися до цієї мережі з метою впровадження її алгоритмів. Уважаємо, що це має підвищити рівень соціальної безпеки України.

Література

1. Андрейцев В.В. Суб'єктний склад діяльності, пов'язаної з об'єктами підвищеної небезпеки: господарсько-правові аспекти // Економіка та право. 2019. № 3. С. 39–48.

2. Бойко О.А. Об'єкти підвищеної небезпеки: упровадження вдосконалених підходів до їх ідентифікації // Цивільний захист та пожежна

безпека. 2023. № 1 (15). С. 83–91.

3. Домбровська С.М., Шведун В.О., Крюков О.І., Ігнатьєв О.М. Державна політика у сфері моніторингу стану потенційно небезпечних об’єктів: монографія. Харків: «Діса плюс», 2023. 240 с.

4. Помаза-Пономаренко А.Л., Мороз С.А. Цивільний захист як сфера забезпечення національної безпеки України // Національна безпека в умовах війни, післявоєнної відбудови та глобальних викликів XXI століття : Матеріали Всеукр. науково-прак. конф. (07-08.12.2023 р., м. Житомир). С. 305–308.

5. Помаза-Пономаренко А.Л., Тарадуда Д.В. Забезпечення стійкості системи державного регулювання об’єктів підвищеної небезпеки // Державне управління: удосконалення та розвиток. 2024. № 4. URL: https://www.nayka.com.ua/index.php/dy/article/view/3461. (дата звернення 26.04.2024).

6. Помаза-Пономаренко А.Л., Тарадуда Д.В. Механізми забезпечення цивільної безпеки України: аспекти попередження НС на об’єктах військово-промислового комплексу // Публічне адміністрування та національна безпека. 2024. № 3 (44). URL: https://www.inter-nauka.com/issues/administration2024/3/9732 (дата звернення 26.04.2024).

7. Помаза-Пономаренко А.Л., Тарадуда Д.В., Порока С.Г. Організаційно-правові засади імплементації Механізму цивільного захисту ЄС в Україні в контексті гарантування національної безпеки // Державне будівництво: електронний журнал. 2023. № 2 (34). С. 67-79.

8. Klaver M.H.A., Luiijf H.A.M., Nieuwenhuijs A.H., Cavenne F., Ulisse A., Bridegeman G. European risk assessment methodology for critical infrastructures // 2008 First International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future, IEEE, Piscataway, New Jersey, USA, 10-12 November 2008, pp. 1–5.

9. Nakamura E.T., Silva J.A., Rios J.M.M. Mobile Telecommunications Networks for the 2014 World Cup. URL: https://www.gsma.com/latinamerica/wp-content/uploads/2012/06/WorldCup2014-CPqD.pdf (Accessed 26 April 2024).

10. Pomaza-Ponomarenko A., Taraduda D., Leonenko N., Poroka S., Sukhachov M. Ensuring the safety of citizens in times of war: aspects of the organization of civil defense // AD ALTA: Journal of Interdisciplinary Research. 2024. Vol. 14. Issue 1. Pp. 216–220.

11. Popov O., Taraduda D., Sobyna V., Dement M., Pomaza-

Ponomarenko A. (2020). Emergencies at Potentially Dangerous Objects Causing Atmosphere Pollution: Peculiarities of Chemically Hazardous Substances Migration. Systems, Decisions and Control in Energy I. Studies in Systems, Decision and Control. Switzerland: Springer International Publishing AG. Vol. 298. P. 151–163.

12. The Spanish Security Strategy 2011. Everyone's Responsibility. Gobierno de Espana. URL: https://publications.hse.ru/en/chapters/78410684 (Accessed 26 April 2024).

References

1. Andreytsev, V.V. (2019), "Subject composition of activities related to objects of increased danger: economic and legal aspects", *Ekonomika ta pravo*, vol. 3, pp. 39–48.

2. Boyko, O.A. (2023), "Objects of increased danger: introduction of improved approaches to their identification", *Tsyvil'nyy zakhyst ta pozhezhna bezpeka*, vol. 1 (15), pp. 83–91.

3. Dombrovska, S.M., Shvedun, V.O., Kryukov, O.I. and Ignatiev, O.M. (2023), *Derzhavna polityka u sferi monitorynhu stanu potentsiyno nebezpechnykh ob"yektiv* [State policy in the field of monitoring the state of potentially dangerous objects], Disa Plus, Kharkiv, Ukraine.

4. Pomaza-Ponomarenko, A.L. and Moroz, S.A. (2023), "Civil defense as a sphere of ensuring the national security of Ukraine", *Zbirka dopovidej na Vseukayins'koyi naukovo-praktychnij konferentsii* [Conference Proceedings of the All-Ukrainian Scientific and Practical Conference], National University, Zhytomyr, Ukraine, pp. 305–308.

5. Pomaza-Ponomarenko, A.L. and Taraduda, D.V. (2024), "Ensuring the stability of the system of state regulation of increased danger facilities and critical infrastructure facilities", *Derzhavne upravlinnya: udoskonalennya ta rozvytok*, vol. 4, available at: https://www.nayka.com.ua/index.php/dy/article/view/3461 (Accessed 26 April 2024).

6. Pomaza-Ponomarenko, A.L. and Taraduda, D.V. (2024), "Mechanisms for ensuring civil security of Ukraine: aspects of emergency prevention at the facilities of the military-industrial complex", *Publichne administruvannya ta natsional'na bezpeka,* vol. 3 (44), available at: https://www.inter-nauka.com/issues/administration2024/3/9732 (Accessed 26 April 2024).

7. Pomaza-Ponomarenko, A.L., Taraduda, D.V. and Poroka, S.G. (2023),

"Organizational and legal principles of the implementation of the EU Civil Protection Mechanism in Ukraine in the context of guaranteeing national security", *Derzhavne budivnytstvo: elektronnyy zhurnal*, vol. 2 (34), pp. 67–79.

8. Klaver, M.H.A., Luiijf, H.A.M., Nieuwenhuijs, A.H., Cavenne, F., Ulisse, A. and Bridegeman, G. (2008), "European risk assessment methodology for critical infrastructures", *2008 First International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future*, IEEE, Piscataway, New Jersey, USA, 10-12 November, pp. 1–5.

9. Nakamura, E.T., Silva, J.A. and Rios, J.M.M. "Mobile Telecommunications Networks for the 2014 World Cup", available at: https://www.gsma.com/latinamerica/wp-content/uploads/2012/06/WorldCup2014-CPqD.pdf (Accessed 26 April 2024).

10. Pomaza-Ponomarenko, A., Taraduda, D., Leonenko, N., Poroka, S. and Sukhachov, M. (2024), "Ensuring the safety of citizens in times of war: aspects of the organization of civil defense", *AD ALTA: Journal of Interdisciplinary Research*, vol. 14, issue 1, pp. 216–220.

11. Popov, O., Taraduda, D., Sobyna, V., Dement, M. and Pomaza-Ponomarenko, A. (2020), "Emergencies at Potentially Dangerous Objects Causing Atmosphere Pollution: Peculiarities of Chemically Hazardous Substances Migration", *Systems, Decisions and Control in Energy I. Studies in Systems, Decision and Control,* Switzerland: Springer International Publishing AG, vol. 298, pp. 151–163.

12. The Spanish Security Strategy (2011), "Everyone's Responsibility. Gobierno de Espana", available at: https://publications.hse.ru/en/chapters/78410684 (Accessed 26 April 2024).

Стаття надійшла до редакції 26.04.2024 р.