Ирина Манжул, к. ю. н.
Національна академія Служби безпеки України

ПОНЯТТЯ ТА ЗАХИСТ КРИТИЧНОЇ НФРАСТРУКТУРИ В США, ЄС, УКРАЇНІ

Irina Manzhul, PhD in Law
National Academy of Security Service of Ukraine

CONCEPT AND PROTECTION OF CRITICAL INFRASTRUCTURE IN THE US, EU, UKRAINE

The article studied critical infrastructure protection and national security. This study is about experience in this field. The rules and practices of special state bodies responsible for state protection of critical infrastructure were analyzed. It was found that in Ukraine there is no coordination of public and private sector in protection for national security; ongoing sectoral legislation exists separately and independently by different agencies. The paper proposes approval of the national program for protection of critical infrastructure, national action plan relevant programs in the energy sector, development of ministries, competent for certain infrastructures, their physical protection; as well as police and special units with experience in response to the criminal actions of prevention and liquidation.

Key words: critical infrastructure, energy infrastructure, national plan, national program, directives, orders, public and private sector, coordination.

Починаючи з середини 90-х рр. XX ст., спочатку в США, пізніше в європейських країнах політики, науковці, практичні працівники починають розробляти поняття критична інфраструктура, визначати її складові, обґрунтовувати необхідність захисту. Безпека національних критичних інфраструктур сьогодні вважається першочерговим завданням всіх сучасних країн світу. Пріоритетна увага при цьому приділяється захисту енергетичних, транспортних, інформаційних, комунікаційних інфраструктур. Вже накопичений досвід щодо розробки відповідних національних планів і програм, координації дій державних і приватних органів, реалізації завдань та функцій державної і місцевої влади. Дослідження зазначеної практики зумовлюється потребою застосування в Україні кращого інструментарію захисту критичної інфраструктури від тих зловмисних дії, які можуть вивести із ладу системи та об'єкти, що забезпечують національну безпеку.

Поняття критичної, у тому числі енергетичної інфраструктури, в Україні досліджують Д.С.Бірюков, О.Л.Глушкевич, О.В.Іванченко, С.І.Кондратов, О.М.Суходоля, В.І.Пеньковський, О.В.Устименко, С.Є Хлонь та інші. Ними розглядається зарубіжний досвід, аналізується стан із визначенням об'єктів критичної інфраструктури в українському законодавстві та їх захист.

Ставимо за мету коротко розглянути та зіставити досвід щодо визначення та захисту критичної інфраструктури в США, ЄС та Україні, запропонувати напрями удосконалення відповідної вітчизняної практики.

Вперше питання про необхідність захисту критичної інфраструктури було підняте в США. Зауважимо, що захист критичної інфраструктури насамперед передбачався від кібер-уразливості, кібер-загроз. Дефініція критична інфраструктура не є однозначною, що зумовлюється необхідністю постійних змін у визначенні в певний період життєдіяльності країни тих об'єктів, які особливо потребують державного захисту. Якщо у 1996 р. в США адміністрація Б.Клінтона до критичної інфраструктури в США відносила: телекомунікації, електроенергетичні системи, нафту і газ та їх зберігання і транспортування, банківську справу та фінанси, транспорт, системи водопостачання, аварійні служби, безперервність керування, то у 2003 р., було сформовано чотирнадцять критичних секторів, у тому числі продукти харчування, охорона здоров'я, хімічна промисловість і небезпечні матеріали[1], а у 2013 р. – 16[2]. Зауважимо, що різне поняття критичної інфраструктури було

[1] Eckert, S. *Protecting Critical Infrastructure: The Role of the Private Sector*, 18 <https://www.ridgway.pitt.edu/Portals/1/pdfs/Publications/Eckert.pdf>.

[2] *Presidential Policy Directive – Critical Infrastructure Security and Resilience* (2013). <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

сформовано в США до подій 11.09.2011 р. та після того. З 2001 р. офіційним визначенням критичної інфраструктури було наступне: критична інфраструктура, це "сукупність фізичних або віртуальних систем і засобів, важливих для США такою мірою, що їх вихід з ладу або знищення можуть призвести до згубних наслідків в області оборони, економіки, охорони здоров'я та безпеки нації"[1]. Сьогодні до одного з найбільш цитованих визначень віднесемо таке: критична інфраструктура, це «системи та об'єкти, фізичні та віртуальні, настільки життєво важливі для держави, що недієздатність або знищення таких систем або об'єктів підриває національну безпеку, здоров'я або безпеку населення, або має своїм результатом будь-яку комбінацію з перевищеного вище»[2].

Енергетична інфраструктура визначається як основна в критичній інфраструктурі. На 2015 р. вона характеризується наступним чином: понад 80 відсотків енергетичної інфраструктури країни належить приватному сектору, поставляючи паливо для транспортної галузі, електроенергії домашніх господарств і підприємств, та інших джерел енергії, які є невід'ємною частиною росту і виробництва по всій країні. Енергетична інфраструктура ділиться на три взаємопов'язаних сегменти: електроенергії, нафти і природного газу. Приблизно 48 відсотків електроенергії виробляється шляхом спалювання вугілля (в першу чергу, що перевозяться залізничним транспортом), 20 відсотків на атомних електростанціях, і 22 відсотків шляхом спалювання природного газу, 3 відсотки йде на відновлювані джерела енергії, решта це ГЕС. Практично всі галузі залежать від електроенергії та транспортного сектору[3]. Тривале порушення енергосистем може серйозно вплинути на всі інші інфраструктури[4].

Ще у 1996 р. президент Клінтон видав розпорядження №13010, яким створив комісію президента з захисту життєво важливої інфраструктури (PCCIP). На комісію покладалося завдання вивчити зростаючу залежність американської економіки і способу життя від стану критичних інфраструктур. Із врахуванням рекомендації комісії у 1998 р. президентом була затверджена директива /NSC-№63 «Стратегія спільних зусиль адміністрації США і приватного сектору в галузі захисту критичної інфраструктури», в якій як національна мета визначалося завдання захисту критично важливих об'єктів інфраструктури нації від навмисних дій, які б значно зменшили їх можливості [5]. Нею встановлювалися завдання федерального уряду, державних і місцевих органів влади, приватного сектору; необхідність координації та тісних взаємозв'язків між ними; керівні принципи захисту критичної інфраструктури, серед яких – відповідальність та партнерство; структура та організація захисту об'єктів критичної інфраструктури від кібер- та фізичних нападів; необхідність створення Координаційної групи, розроблення Національного координаційного плану, посади Національного координатора, їх завдання та функції [6].

Відповідно до указів президента № 13130 та №13231 були створені Національна Рада з критичної інфраструктури (National Infrastructure Advisory Council – NIAC), Центр інформаційного обміну і аналізу (Information Sharing and Analysis Centers), Національний центр аналізу та імітаційного моделювання інфраструктури (The National Infrastructure Simulation and Analysis Center – NISAC), в листопаді 2002-го утворено Міністерство внутрішньої безпеки, на яке було покладено загальне керівництво заходами забезпечення захисту національної інфраструктури від різних загроз[7].

До останніх документів в цій сфері віднесемо: президентську директиву №7 (HSPD-7) грудня 2007 р., яка замінила директиву №63 і визначила напрями національної політики для федеральних департаментів і агентств з метою захисту критичної інфраструктури від терористичних атак,

---

[1] *Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism* (USA PATRIOT ACT) ACT OF 2001 (2001). <https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf>.

[2] Montanari, L., Querzoni, L. (2014). *Critical Infrastructure Protection: Threats, Attacks and Countermeasures,* 7 <http://www.dis.uniroma1.it/~tenace/download/deliverable/Report_tenace.pdf>.

[3] *Energy Sector* (2016). <http://www.dhs.gov/energy-sector>.

[4] Marsh, Robert T. Chairman (1997). Critical Foundations Protecting America's Infrastructures. *The Report of the President's Commission*, 12. <https://www.fas.org/sgp/library/pccip.pdf>.

[5] Ryan, J. (1998). *The Infrastructure of the Protection of the Critical Infrastructure.* <http://www.iwar.org.uk/cip/resources/pdd63/pdd63-article.htm>.

[6] *Presidential Decision Directive/NSC-63* (1998). <http://fas.org/irp/offdocs/pdd/pdd-63.htm>.

[7] Moteff, J.D. (2015). *Critical Infrastructures: Background, Policy, and Implementation.* <http://www.iwar.org.uk/news-archive/crs/8087.pdf>.

розмежування ролі і відповідальності міністерств та інших структур, а також коректування їх взаємодії із захисту критичної інфраструктури; План захисту національної інфраструктури (травень 2007 р.), який передбачає забезпечення безпеки критичної інфраструктури держави в різних секторах економіки США. Він постійно вдосконалюється і передбачає створення інструментів для забезпечення партнерства в зазначеній сфері; до його основних елементів відноситься: усесторонній підхід до захисту критичної інфраструктури; комплексна і достовірна оцінка стану інфраструктури держави; організація і координація партнерства на всіх рівнях від державного до приватного сектору; інтеграція в посилені захисту фізичних об'єктів, кіберпростору, населення та інше[1]. Зауважимо, що оскільки велика частина енергетичної інфраструктури в сучасній індустріальній економіці, як правило, знаходиться у приватній власності і управляється власниками, у тому числі ними є оператори, в США постійно піднімається питання про необхідність впровадження державно-приватного партнерства в сфері захисту критичної, у тому числі, критичної енергетичної інфраструктури. Президентська директива №21 (лютий 2013 р.) «Безпека та стійкість критичної інфраструктури»[2] має за мету єдності всіх національних зусиль для зміцнення і підтримки безпечного функціонування стійкості критичної інфраструктури; встановлює засади національної політики; спільну відповідальність всіх державних та приватних структур за стан критичної інфраструктури; направлена на підвищення їх загальної координації; встановлює три стратегічні імперативи для зміцнення безпеки критичної інфраструктури (пошук і уточнення функціональних взаємозв'язків, ефективний обмін інформацією, здійснення інтеграції та аналізу планування та операцій захисту критичної інфраструктури) вказує на ролі та обов'язки міністра внутрішньої безпеки; секретаря національної безпеки; кожного сектора критичної інфраструктури; міністерств та відомств; уточнення до Національного плану захисту інфраструктури, містить інші положення.

Під керівництвом Департаменту внутрішньої безпеки (DHS), (створений у 2005 р.), промисловість, федеральні, державні та регіональні організації створили мережу взаємопов'язаних координаційних рад в рамках загальної системи координації захисту критичних інфраструктур, забезпечуючи міцну основу для стійкого партнерство. Система включає в себе 18 державних координаційних рад (GCC). Для кожного сектора розроблений конкретний план із врахуванням адаптованих цілей і стратегій для реалізації плану захист інфраструктури (NIPP). Кожен сектор використовує загальну систему управління ризиками, визначає цілі та уразливі активи, оцінює і визначає пріоритети ризиків, здійснює захисні заходи, а також оцінює їх ефективність. Галузеві річні звіти використовуються для відслідковування результатів у досягненні цілей. Проте, як зазначається в публікаціях, партнерство секторів ще не досягло повного потенціалу: федеральний уряд повинен поліпшити координацію агентств, задіяти всі сектори, і активізувати свої зусилля з державними та місцевими органами влади і регіональними коаліціями[3].

Важливу роль в захисті критичної енергетичної інфраструктури відіграють розвідувальні органи, під їх керівництвом та за їх допомогою здійснюється вирішення всіх виникаючих питань, у тому числі таких як: усвідомлення ситуації, оцінка загроз, підтримка прийняття рішення, координація та співпраця між оперативними установами та інші. Активна розвідка, на думку доктора Мартіна Раднера (професор університету Карлтон, Оттава, Канада)[4] сприяє визначенню стратегічної мети (яка полягає у виявленні, запобіганні та ліквідації загроз критичної енергетики та громадської безпеки); національних заходів безпеки (систематичний збір, аналіз, звітність щодо загроз в зазначеній сфері); забезпеченню безпеки персоналу насамперед на об'єктах приватного сектору енергетики із врахуванням оцінок уразливості і загроз безпеці на погляд операторів приватного сектору. Підкреслюється значення та необхідність взаємної інформації про загрози та

[1] Баранник, А. (2016). *Организация обеспечения безопасности критической инфраструктуры в США.* <http://pentagonus.ru/publ/organizacija_ obespechenija_bezopasnosti_kriticheskoj_infrastruktury_v_ssha/19-1-0-1277>.

[2] *Presidential Policy Directive (2013) – Critical Infrastructure Security and Resilience.* <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

[3] Berkeley, Alfred R., Grayson, Margaret E., Gallegos, Gilbert G. (2008). *Critical Infrastructure Partnership Stratigic Assessment Final Report and Recommendations,* 27. <http://www. dhs.gov/ sites/default/files/publications/niac-ci-partnership-assessment-final-report-10-14-08-508.pdf>.

[4] Rudner, M. (2008) *Protecting Critical Energy Infrastructure Through Intelligence*, 654-656. <https://wikileaks.org/gifiles/attach/131/131113_ProtectEnergyInfrastructureThruIntel-Rudner.pdf>.

небезпеку критичній енергетичній інфраструктурі між розвідувальними органами і приватним сектором в цій сфері, навчання та підготовку персоналу, підвищення його кваліфікації в сфері безпеки, та координаційна роль загалом розвідувальних органів.

Вперше питаннями критичної інфраструктури європейські країни почали займатися з 1998 р. на національному рівні з метою захисту інформаційних і комунікаційних технологій. Перше визначення критичної національної інфраструктури було зроблено у Великобританії у 1999 р., пізніше в інших європейських країнах. Універсального визначення цього поняття критичної інфраструктури не має, кожна країна до неї відносить ті об'єкти, системи, процеси, сфери діяльності, що потребують обов'язкового захисту та від яких залежить національна безпека. Європейська комісія визначає критичну інфраструктуру як сукупність активів, систему або її частину, яка знаходиться в державах-членах та має важливе значення для підтримки життєво важливих функцій суспільства, здоров'я, безпеки, економічного або соціального благополуччя людей, і порушення або руйнування яких матиме істотний вплив на ці держави, в результаті відмови підтримувати ці функції[1]. У 2008 р. ЄС було визначено 11 секторів, які відносяться до критичної інфраструктури, це: хімічна промисловість; енергія; фінансовий; харчова промисловість; здоров'я; ІКТ; атомна промисловість; дослідні установи, космос, транспорт; і вода [2].

До важливих документів Європейської комісії віднесемо такі документи як: Європейська програма захисту критичної інфраструктури та Захист критичної енергетичної та транспортної інфраструктури Європи. В Європейській програмі захисту критичної інфраструктури визначена мета прийняття документу (поліпшення захисту критично важливих інфраструктур у ЄС); види загроз (пріоритетну від тероризму); принципи (субсидіарність, взаємодоповнюваність, конфіденційність інформації, співпраця із зацікавленими сторонами, відповідність заходів загрозам, секторальний підхід); межі захисту (національна критична інфраструктура держав-членів ЄС); підходи до планування плану дії та інші аспекти[3]. Зазначена програма була розроблена у 2005 р., впроваджена в 2006 р.

В повідомленні Комісії Ради Європи та Європейського парламенту 2007 р. «Захист критичної енергетичної та транспортної інфраструктури Європи» визначаються транспорт і енергетика, як два найбільш важливих секторів економіки, що відіграють основну роль у зусиллях ЄС щодо сприяння інтеграції та єдиного ринку; зняття бар'єрів на шляху вільного транскордонного пересування людей, товарів, капіталу і послуг. До енергетичної інфраструктури включено забезпечення нафтою і газом, їх видобуток та зберігання, трубопроводи, диспетчерські пункти, виробництво і передача, розподіл електроенергії, ядерно-паливний цикл, гідро-електроенергія. До транспортної – аеропорти, управління повітряним рухом, морські порти і морська навігація, автомобільний, залізничний (мости, тунелі, трек, вокзали, центри управління) та внутрішні водні шляхи.

В документі розроблені критерії щодо захисту зазначених підрозділів транспорту та енергетики, які сумісні з пакетом захисту критичної інфраструктури; наведені потенціальні наслідки їх руйнування, чи зруйнування; викладені перспективні плани Комісії: моніторинг за розвитком нових видів інфраструктури; дотримання принципів субсидіарності та пропорційності; надання грантів для проектів, пов'язаних з захистом критичної інфраструктури в галузі транспорту та енергетики; сприяння захисту критичної інфраструктури тих країн, що не входять в ЄС[4].

У 2013 році Європейська Комісія оцінила досягнутий прогрес в реалізації Європейської програми захисту життєво важливої інфраструктури і запропонувала, аналізуючи можливі загрози, ввести новий пілотний проект. Він включає в себе посилений захист передачі електромереж, газотранспортної системи, управління повітряним рухом, новий підхід до захисту критичної інфраструктури. Нині Комісія ЄС з європейського захисту життєво важливої інфраструктури для енергетики, транспорту, фінансів фокусується на: 1) процедурі для виявлення, оцінки, захисту

---

[1] Hammerli, B., Renda, A. (2010). *Protecting Critical Infrastructure in the EU*, 21 <http://aei.pitt.edu/15445/1/Critical_Infrastructure_Protection_Final_A4.pdf>.

[2] *Proposal for a Council Decision on a Critical Infrastructure Warning Information Network* (2008). <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52008PC0676>.

[3] *Communication from the Commission on a European Programme for Critical Infrastructure Protection* (2006), 1-10. <http://ccpic.mai.gov.ro/docs/COM2006%20786final.pdf>.

[4] *Communication from the Commission to the Council and the European Parliament Protecting Europe's Critical energy and Transport Infrastructure (modified)* (2009), 6-7. <http://www.eumonitor.nl/9353000/1/j9vvik7 m1c3gyxp/ vi7jgt6cbqy0>.

критичних інфраструктур енергетики і транспорту; 2) заходах для захисту критичної інфраструктури інформаційної мережі (CIWIN) – системи зв'язку на основі Інтернету для обміну інформацією, досліджень і передової практики; 3) фінансуванні більше 100 проектів в галузі охорони критичної інфраструктури, які спрямовані на розв'язання різних питань, включаючи національний та європейський обмін інформацією та систем оповіщення, електричних мереж та інше; 4) міжнародному співробітництву з Європейською економічною зоною (ЄЕЗ) та Європейською асоціацією вільної торгівлі (ЄАВТ), а також нарадами між ЄС, США та Канади [1].

Розглянемо стан захисту критичної інфраструктури, у тому числі, критичної енергетичної в Україні. У вітчизняному законодавстві визначення терміну критична інфраструктура ми не зустрічаємо, хоча сам термін вже використовується[2]. До критичної інфраструктури, спираючись на законодавчі акти, науковці відносять численні об'єкти, які потребують особливих умов їх захисту та функціонування. Зокрема, такий перелік наведений в Аналітичній записці Національного інституту стратегічних досліджень «Про проблеми вдосконалення системи захисту критичної інфраструктури в Україні». До них, із посиланням на вітчизняне законодавство, Д.С.Бірюков відносить: підприємства, що мають стратегічне значення для економіки і безпеки держави; об'єкти підвищеної безпеки; важливі державні об'єкти; об'єкти, що підлягають особливій охороні підрозділами Державної служи охорони за договорами; об'єкти, що підлягають особливої охороні та обороні в умовах надзвичайних ситуацій та особливий період; особливо важливі об'єкти електроенергетики; особливо важливі об'єкти нафтогазової галузі; Національна система конфіденційного зв'язку; платіжні системи; система екстреної допомоги населенню; аварійно-рятувальні служби; нерухомі об'єкти культурної спадщини[3].

Під критичною інфраструктурою частіше всього розуміють: "системи та об'єкти, фізичні чи віртуальні, настільки життєво важливі для держави, що недієздатність або знищення таких систем або об'єктів підриває національну безпеку, економіку, здоров'я або безпеку населення, або має своїм результатом будь-яку комбінацію з переліченого вище"[4]. В Зеленій книзі з питань захисту критичної інфраструктури України пропонується наступне визначення: «Критична інфраструктура України – це системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки» [5]. Критичну енергетичну інфраструктуру розуміють як «сукупність елементів – об'єктів (будинків та споруд), технічних засобів і технологій, обслуговуючого персоналу, які функціонують синергічно під час вирішення завдань видобутку (виробництва) і первинної переробки, зберігання, транспортування і збуту – нафтогазових (паливно-енергетичних) ресурсів; – ресурсів електроенергетики; – ресурсів атомної енергетики» [6].

Важливість захисту енергетичної інфраструктури останнім часом значно зросла в силу багатьох об'єктивних та суб'єктивних чинників і обставин внутрішнього і зовнішнього характеру. Саме тому на науково-теоретичному рівні проблематика критичної інфраструктури та її складових розробляється досить активно. Вище наводились розроблені науковцями приклади понять критична інфраструктура, критична енергетична інфраструктура, об'єктів критичної інфраструктури. Також розроблені загальні підходи до організації охорони критичних об'єктів енергетики; пріоритетні завдання формування системи захисту критичної енергетичної інфраструктури; засади державної

[1] *Protection of critical infrastructure* (2013). <http://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure>.

[2] Суходоля, О.М. Захист енергетичної інфраструктури: аналіз української законодавчої бази. *Аналітична записка.* <http://www.niss.gov.ua/articles/1568/>.

[3] Бюрюков, Д.С. Про проблеми вдосконалення системи захисту критичної інфраструктури в Україні. *Аналітична записка*. <http://www.niss.gov.ua/articles/1477/>.

[4] Суходоля, О.М. Захист енергетичної інфраструктури: аналіз української законодавчої бази. *Аналітична записка.* <http://www.niss.gov.ua/articles/1568/>.

[5] Бірюков, Д.С., Кондратов, С.І, Насвіт, О.І., Суходоля, О.М. (2015). *Зелена книга з питань захисту критичної інфраструктури в Україні: аналітична доповідь.* Київ: НІСД.

[6] Иванченко, О.В. *CASE-анализ критических энергетических инфраструктур с использованием аппарата моделирования полумарковых процессов*. <http://crictecs.csn.khai.edu/documents/17721/198701/CriCTecS_2013.09.24_Presentation_%E2%84%961.pdf/85b83c56-3edd-47e3-b067-af15d121970d>.

політики захисту енергетичної інфраструктури[1], пропозиції до удосконалення державної системи захисту державної інфраструктури (визначити на законодавчому рівні функції та завдання органів державної влади та суб'єктів господарювання різних форм власності; встановити солідарну відповідальність як органів державної влади, так і приватного сектору за захист критичної інфраструктури; розробити єдиний законодавчий акт щодо захисту критичної інфраструктури від зловмисних дій; модернизувати систему захисту національної безпеки)[2].

В Зеленій книзі з питань захисту критичної інфраструктури в Україні визначені поняття захист критичної інфраструктури, категорії загроз критичній інфраструктурі, принципи формування захисту критичної інфраструктури (координованості, єдності методологічних засад, державно-приватне партнерство, принцип забезпечення конфіденційності), розроблені складові загальної координації захисту критичної інфраструктури (створення національного центру, вдосконалення нормативно-правової бази, оцінка загроз критичній інфраструктурі, підготовка національного плану захисту, державної цільової програми, координації зусиль всіх зацікавлених сторін та інш.), а також структура проекту ЗУ «Про критичну інфраструктуру».

Отже, в Україні на науково-теоретичному рівні здійснені грунтовні напрацювання щодо захисту критичної, у тому числі, енергетичної, інфраструктури. Проте вони не мають належного практичного впровадження. Зазначене зовсім не означає, що в Україні не має захисту тих об'єктів, що забезпечують національну безпеку, він здійснюється галузевим законодавством, розрізнено та самостійно різними відомствами.

В Україні необхідно, як це має місце, наприклад в США, розробити Національну програму захисту критичної інфраструктури, відповідний національний план. Їх прийняття забезпечить координацію комплексного захисту критичної інфраструктури на загальному та галузевому рівні, обмін оперативною взаємною інформацією між державним і приватним сектором. Окремо має реалізуватися програма захисту критичної інфраструктури в особливо важливих секторах. Наведемо приклад ЄС, де реалізується програма щодо захисту критичної інфраструктури в енергетиці та транспорті з чіткою фіксацією повноважень та функцій кожної структури підгалузі.

Бажано залучити до розробки майбутніх, необхідних для захисту критичної інфраструктури в Україні, Національної програми та Національного плану представників галузевих міністерств, відомств, компетентних щодо специфіки об'єктів інфраструктури, їх фізичного захисту; а також правоохоронних органів та спеціальних підрозділів, що мають досвід реагування на злочинні дії. Варто перейняти досвід США та деяких європейських країн, в яких створені спеціальні державні структури (наприклад, департаменти), відповідальні за стан критичної інфраструктури в країні, реалізацію та координацію відповідних заходів.

References

1. Eckert, S. *Protecting Critical Infrastructure: The Role of the Private Sector*, 18. <https://www.ridgway.pitt.edu/Portals/1/pdfs/Publications/Eckert.pdf>.
2. *Presidential Policy Directive – Critical Infrastructure Security and Resilience* (2013). <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.
3. *Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism* (USA PATRIOT ACT) ACT OF 2001 (2001). <https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf>.
4. Montanari, L., Querzoni, L. (2014). *Critical Infrastructure Protection: Threats, Attacks and Countermeasures,* 7. <http://www.dis.uniroma1.it/~tenace/download/deliverable/Report_tenace.pdf>.
5. *Energy Sector*. <http://www.dhs.gov/energy-sector>.
6. Marsh, Robert T. Chairman (1997). Critical Foundations Protecting America's Infrastructures*. The Report of the President's Commission, 12.* <https://www.fas.org/sgp/library/pccip.pdf>.
7. Ryan, J. (1998). *The Infrastructure of the Protection of the Critical Infrastructure.* <http://www.iwar.org.uk/cip/resources/pdd63/pdd63-article.htm>.
8. *Presidential Decision Directive/NSC-63* (1998). <http://fas.org/irp/offdocs/pdd/pdd-63.htm>.
9. Moteff, J.D. (2015). *Critical Infrastructures: Background, Policy, and Implementation.* <http://www.iwar.org.uk/news-archive/crs/8087.pdf>.

[1] Суходоля, О.М. *Система захисту критичної енергетичної інфраструктури України: стан та проблеми формування.* <http://nationalsecurity.org.ua/2015/11/ 03/3948/>.

[2] Суходоля, О.М. Захист енергетичної інфраструктури: аналіз української законодавчої бази. *Аналітична записка*. <http://www.niss.gov.ua/articles/1568/>.

10. Barannyk, A. (2016). *Orhanyzatsyia obespechenyia bezopasnosty krytycheskoi ynfrastruktury v SShA.* <http://pentagonus.ru/publ/organizacija_obespechenija_bezopasnosti_kriticheskoj_infrastruktury_v_ssha/19-1-0-1277>.
11. Rudner, M. (2008) *Protecting Critical Energy Infrastructure Through Intelligence, 654-656* <https://wikileaks.org/gifiles/attach/ 131/131113_ ProtectEnergyInfrastructureThr uIntel-Rudner.pdf>.
12. Berkeley, Alfred R., Grayson, Margaret E., Gallegos, Gilbert G. (2008). *Critical Infrastructure Partnership Stratigic Assessment Final Report and Recommendations,* 27. <http://www.dhs.gov/sites/default/files/ publications/ niac-ci-partnership-assessment-final-report-10-14-08-508.pdf>.
13. Hammerli, B., Renda, A. (2010). *Protecting Critical Infrastructure in the EU*, 21. <http://aei.pitt.edu/15445/1/ Critical_Infrastructure_Protection_Final_A4.pdf>.
14. *Proposal for a Council Decision on a Critical Infrastructure Warning Information Network* (2008). <http://eur-lex.europa.eu/legal-content/EN/TXT/ ?uri=celex:52008PC0676>.
15. *Communication from the Commission on a European Programme for Critical Infrastructure Protection* (2006). 1-10. <http://ccpic.mai.gov.ro/ docs/ COM2006%20786final.pdf>.
16. *Communication from the Commission to the Council and the European Parliament Protecting Europe's Critical energy and Transport Infrastructure (modified)* (2009, 6-7). <http://www.eumonitor.nl/9353000/ 1/j9vvik7m1c3gyxp / vi7jgt6cbqy0>.
17. *Protection of critical infrastructure* (2013). <http://ec.europa.eu/energy/en/ topics/infrastructure/protection-critical-infrastructure>.
18. Sukhodolia, O.M. Zakhyst enerhetychnoi infrastruktury: analiz ukrainskoi zakonodavchoi bazy. *Analitychna zapyska.* <http://www.niss.gov.ua/articles/1568/>.
19. Biuriukov, D.S. Pro problemy vdoskonalennia systemy zakhystu krytychnoi infrastruktury v Ukraini. *Analitychna zapyska*. <http://www.niss.gov.ua/articles/1477/>.
20. Biriukov, D.S., Kondratov, S.I., Nasvit, O.I., Sukhodolia, O.M. (2015). *Zelena knyha z pytan zakhystu krytychnoi infrastruktury v Ukraini: analitychna dopovid*. Kyiv: NISD.
21. Yvanchenko, O.V. *CASE-analyz krytycheskykh ənerhetycheskykh ynfrastruktur yspolzovanyem apparata modelyrovanyia polumarkovykh protsessov.* <http://crictecs.csn.khai.edu/documents/17721/198701/CriCTecS _2013.09.24_Presentation_%E2%84%961.pdf/85b83c56-3edd-47e3-b067-af15d121970d>.
22. Sukhodolia, O.M. *Systema zakhystu krytychnoi enerhetychnoi infrastruktury Ukrainy: stan ta problemy formuvannia*. <http://nationalsecurity.org.ua/2015/11/ 03/3948/>.