3. Sharp R. Budgeting for Equity: Gender Budget Initiatives within a Framework of Performance Oriented Budgeting – Режим доступу: http://www.unifem.org/resources/item_detail. – P.11.

4. Даудова Г.В., Таукешева Т.Д. Упровадження гендерно орієнтованого бюджетування в Україні / Г.В. Даудова, Т.Д. Таукешева // Теорія та практика державного управління. – 2017. – № 2(57). – С. 12-19.

5. Ґендерно-орієнтоване бюджетування в Україні: теорія і практика: Метод. посіб. – К.: ФОП Клименко, 2016. – 92 с.

6. Гендерно-орієнтоване бюджетування: аналіз програм, які фінансуються з бюджету, з позиції ґендерної рівності : посібник для працівників органів виконавчої влади та місцевого самоврядування. – К., 2016. – 36 с.

7. Коляда Т.А. Ґенеза методологічних засад бюджетного прогнозування / Т.А. Коляда // Бізнес Інформ. – 2014. – №7. – С. 253-259.

Мельничук Олег Володимирович,
аспірант кафедри глобалістики, євроінтеграції та управління національною безпекою НАДУ при Президентові України

КРИТИЧНА ІНФРАСТРУКТУРА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Виклики воєнного, соціального та політичного характеру, що виникають нині в Україні, обумовлюють неохідність публічного реагування відносно невідкладного прийняття рішень щодо захисту критичної інфраструктури. Глобальні тенденції використання природних ресурсів спричинили невідворотну залежність людства від послуг, які надають інфраструктурні складові. Нині в Україні розробляється закон про захист критичної інфраструктури, де мають бути визначені суб'єкти, об'єкти та структура системи її захисту. Необхідне наукове обгрунтування правових, організаційних, методологічних, технологічних та інших інструментів захисту, режимів функціонування системи захисту залежно від рівня загроз і ризиків при визначенні рекомендацій державі, місцевому самоврядуванню, громадам.

Мета розробки – вивчення світового досвіду, узагальнення наукових надбань щодо відмінності поняття «критична інфраструктура» та визначенння шляхів його удосконалення в Україні.

Сьогодні теорія публічного управління оперує багатьма поняттями, серед яких: «безпека», «міжнародна безпека», «національна безпека», «регіональна безпека», «загрози національній безпеці», «національні

інтереси», «загроза національним інтересам», «система національної безпеки», «система забезпечення національної безпеки» тощо, але окремі поняття заслуговують більш детального розгляду. Такими, зокрема, є «національна безпека», «загрози національній безпеці» та «національні інтереси». У певний період розвитку держави та суспільства є множина різних за пріорітетністю, спрямованістю та можливістю реалізації нагальних потреб, які формують систему національних інтересів. Визначення цієї множини національних інтересів є ключовою передумовою зовнішньої та внутрішньої політики держави.

Підходи щодо класифікації національних інтересів у Західній Європі здебільшого грунтуються на оцінці втрати щодо національної безпеки, до якої може призвести реалізація певної загрози національному інтересу. Правову основу у сфері національної безпеки України становлять Конституція, закони, міжнародні договори, інші нормативно-правові акти. Підходи щодо публічного адміністрування у сфері національної безпеки визначаються Законом «Про основи національної безпеки України» від 19 червня 2003 р. №964-IV, яким визначено сфери національної безпеки: зовнішньополітична; державної безпеки; воєнна; безпеки державного кордону; внутрішньополітична; економічна; соціальна; гуманітарна; науковотехнологічна; екологічна та інформаційна. У цих сферах, на думку законодавців, зароджуються загрози національним інтересам, тобто сфери національної безпеки визначають крізь призму загроз, які є критеріями формування політики щодо національної безпеки.

На нашу думку, визначені Законом національні інтереси не розподілено за вказаними сферами, а наведений перелік потенційних та реальних загроз щодо їх реалізації не відповідає вказаним інтересам, але, як правило, однією із передумов виникнення загрози є наявність національного інтересу. В цьому Законі також наведені терміни, що вживаються в такому значенні:

- національна безпека – захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сферах правоохоронної діяльності, боротьби з корупцією, прикордонної діяльності та оборони, міграційної політики, охорони здоров'я, освіти та науки, науково-технічної та інноваційної політики, культурного розвитку населення, забезпечення свободи слова та інформаційної безпеки, соціальної політики та пенсійного забезпечення, житлово-комунального господарства, ринку фінансових послуг, захисту прав власності, фондових ринків і обігу цінних паперів, податково-бюджетної та митної політики, торгівлі та підприємницької діяльності, ринку банківських послуг,

інвестиційної політики, ревізійної діяльності, монетарної та валютної політики, захисту інформації, ліцензування, промисловості та сільського господарства, транспорту та зв'язку, інформаційних технологій, енергетики та енергозбереження, функціонування природних монополій, використання надр, земельних та водних ресурсів, корисних копалин, захисту екології і навколишнього природного середовища та інших сферах державного управління при виникненні негативних тенденцій до створення потенційних або реальних загроз національним інтересам;

- національні інтереси – життєво важливі матеріальні, інтелектуальні і духовні цінності Українського народу як носія суверенітету і єдиного джерела влади в Україні, визначальні потреби суспільства і держави, реалізація яких гарантує державний суверенітет України та її прогресивний розвиток;

- загрози національній безпеці – наявні та потенційні явища і чинники, що створюють небезпеку життєво важливим національним інтересам. [1]

Історично склалось, що в Україні національна безпека є обєктом держрегулюваннння. Нині відбувається розвиток нового підходу забезпечення безпеки, в основу якої покладені спільні зусилля громадянина, суспільства, бізнесу і держави. В умовах глобалізації гарантоване надання життєво важливих послуг є не лише відповідальністю державних органів.

Тенденції зростання терористичних загроз, кількості та витонченості кібератак, негативних природних та техногенних явищ, драматичні події на сході та півдні України актуалізували питання захисту інфраструктури, життєво важливої для безпеки людини, громадянина, суспільства та держави. У будь-якій з зазначених сфер національної безпеки є базові складові, що забезпечують нормальну роботу важливих для держави та суспільства обєктів, мереж, служб та систем. Нині діє низка правових актів, що врегульовують питання у цій сфері, але досі на національному рівні відсутній системний підхід до управління захистом та безпекою усього комплексу таких систем.

Інфраструкту́ра (лат. infra – «нижче», «під»; structura – «будівля», «розташування») – сукупність споруд, будівель, систем і служб, необхідних для функціонування галузей матеріального виробництва та забезпечення життєдіяльності суспільства. Розрізняють соціальну (школи, лікарні, готелі, громадське харчування, бібліотеки, театри тощо), виробничо-економічну (дороги, канали, порти, транспорт, будівництво, склади, підприємства, системи зв'язку тощо), ринково-інституційну (банки, ринки, компанії, страхові установи, громадські, політичні

організації тощо), іноваційну (технопарки, бізнес-інкубатори тощо) інфраструктуру.

Інфраструктура забезпечує нормальну роботу важливих для держави та суспільства обєктів, мереж, служб і систем, таких як урядові органи, фінансові, податкові, енергетичні, транспортні системи, повітряна та космічна галузь, АЕС, водо забезпечення, водовідведення, великі виробничі підприємства. До критично важливої інфраструктури, як правило, відносять обєкти, мережі, служби та системи, збій у роботі яких позначиться на безпеці, добробуті і здоров'ї людей та суспільства. Експерти Світового банку підкреслюють, що, хоча й необхідно якісно проектувати й будувати будь-яку інфраструктуру, виокремлення категорії критичних об'єктів інфраструктури дозволить приділяти останнім особливу увагу, зменшуючи наслідки від природних та техногенних аварій [2].

Із середини 1990-х років поняття «критична інфраструктура» було введено у правові документи і практику міжнародного спілкування, в науковому й діловому колах. Його значення у країнах дещо відрізняється, проте зазвичай до критичної інфраструктури відносять енергетичні та транспортні магістральні мережі, нафто- й газопроводи, морські порти, канали швидкісного та урядового зв'язку, системи життєзабезпечення (водо- й теплопостачання) мегаполісів, утилізації відходів, служби екстреної допомоги та реагування на надзвичайні ситуації, високотехнологічні підприємства і підприємства ВПК, центральні органи влади. У США критичну інфраструктуру розуміють ширше, включаючи до неї національні символи (пам'ятки культурної спадщини).

Проведений нами аналіз свідчить, що поняття «критична інфраструктура» має близькість визначень як в науковій літературі, так і в законодавстві країн. Можна вирізнити дві основні позиції провідних вітчизняних і зарубіжних фахівців щодо його визначення: об'єкти, необхідні для підтримки життєво важливих суспільних функцій [6, 7, 9]; системи, що забезпечують функції та послуги для життєдіяльності суспільства [3-5, 8], таблиця 1.

Таблиця 1

Наукові визначення поняття «критична інфраструктура»

Автор	Поняття «критична інфраструктура»
Д. Бірюков, С. Кондратов, О. Насвіт, О. Суходоля	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. (Зелена книга з питань захисту критичної інфраструктури в Україні)

І.Уряднікова, С.Чумаченко	Системи, мережі та окремі об'єкти, порушення роботи або руйнування яких може призвести до величезних або незворотних негативних наслідків для економіки, добробуту і здоров'я (термін, використаний в США)
С. Кондратов, Д. Бобро, В. Горбулін та інші.	Системи та ресурси, фізичні або віртуальні, що підтримують функції та послуги, порушення яких призведе до найбільш серйозних негативних наслідків для суспільства, соціально-економічного розвитку та національної безпеки. (Монографія «Розвиток системи захисту критичної інфраструктури в Україні»)
О. Суходоля	Всі об’єкти, які забезпечують нормальне функціонування суспільства, населення і держави. Це об’єкти, зруйнування яких призведе до серйозних наслідків. Мова може йти не лише про мости, електроопори і підстанції, а й про те, що трапилося на Донбасі, коли зникла можливість доносити українську позицію. Мова йде і про банківську інфраструктуру та охорону здоров’я.
A. Lazari	Об'єкти, необхідні для підтримки життєво важливих суспільних функцій (Заг. визначення). Однак, сутність цього визначення краще пояснюється прийняттям універсальних галузевих та перехресних критеріїв, для чіткого визначення того, що є дійсно критичним, через призму посилання на конкретний сектор.
M. Hromada L. Lukas	Критична інфраструктура як система є найважливішою частиною функціональної безперервності суспільства, його економічної та соціальної структури та систем.
P. Auerswald L. M. Branscomb	Інфраструктура є критичною, коли надані послуги є життєво важливими для національної безпеки. Список інфраструктур, які офіційно вважаються критичними в США постійно зростає, додано хімічний сектор, транспорт, об’єкти оборонної промисловості, поштові та судноплавні, інформацію, телекомунікації, фінанси, банківську систему, сільське господарство, харчову галузь, воду, сектор охорони здоров'я, держслужби та служби екстреної допомоги.

Думка вітчизняних вчених («Зелена книга з питань захисту критичної інфраструктури в Україні»; монографія «Розвиток системи захисту критичної інфраструктури в Україні») найповніше відображає сутність поняття «критична інфраструктура». Системний підхід враховує взаємозалежність її обєктів, коли порушення в роботі одного може призвести до порушень у роботі інших, які в свою чергу порушують роботу системи в цілому. Водночас не можна не зауважити, що краще розглядати критичну інфраструктуру за визначеними універсальними критеріїями, що відповідають конкретному сектору.

Більшість розвинених держав самостійно робили спроби дати визначення «критична інфраструктура» та розробили стратегію її захисту. Це повязано з тим, що критична інфраструктура є складним комплексом різноманітних елементів, взаємозалежних у фізичному та віртуальному просторах, та потребує певних управлінських моделей. Розглянемо складові поняття «критична інфраструктура» на основі аналізу джерел [10-20], складено таблицю 2.

Таблиця 2

Контент-аналіз поняття «критична інфраструктура»

Країни	Складові поняття «критична інфраструктура»					
	Послуги	Об’єкти	Системи	Мережі	Активи	Інші
Австралія	-	+	-	+	-	інформтехнології, ланцюжки постачань
Австрія	+	-	-	+	+	інформаційні технології, природні ресурси
Болгарія	-	-	+	-	-	-
Великобританія	+	-	+	-	+	-
Ізраїль	-	-	-	-	-	інфраструктура
Казахстан	-	+	+	-	-	технічні засоби
Канада	+	-	-	+	+	фізичні та інформаційно-технічні засоби
Нідерланди	+	-	-	-	-	продукти, процеси
Німеччина	-	+	-	-	-	організації
Норвегія	-	-	+	-	-	конструкції
Польща	-	+	-	-	-	засоби виробництва, інститути, служби
Росія	-	+	-	-	-	-
США	-	+	+	-	-	-
Україна	-	+	-	-	-	-
Хорватія	+	-	-	+	-	інформтехнології, діяльність, матеріальні блага
Чехія	-	-	+	-	-	-
Швейцарія	-	-	-	-	-	інфраструктура

Японія	-	+	-	-	-	-
Директива Єврокомісії №786	-	+	-	-	-	-

Наведені дані підтверджують, що поняття «критична інфраструктура» містить різні складові залежно від національних потреб та проблем, які різняться залежно від регіону, рівня розвитку держави та інших чинників. Однак, простежується спільна риса критичної інфраструктури різних держав: ключове значення для безпеки громадян, суспільства, держави та нації. Найбільш поширеним є визначення поняття «критична інфраструктура» - об'єкти, які мають настільки важливе суспільне значення, що їх відмова або знищення може викликати істотні порушення, що мають життєво важливе значення для держави та громадян (Австралія, Казахстан, Німеччина, Польща, Росія, США, України, Японія, Директива Єврокомісії №786). Схожими є визначення Ізраїлю та Швейцарії – інфрастуктура, порушення функціонування якої може призвести до значних соціально-економічних потрясінь, вплинути на здоров'я населення, громадські справи, навколишнє середовище, призвести до реалізації загроз національній безпеці країни.

Також поширено визначення «критичної інфраструктури» як комплексу систем, що мають життєво важливе значення для держави, руйнування або недієздатність яких, в тому числі і окремих елементів, матиме згубні наслідки для національної безпеки, економіки, безпеки і здоров'я населення (Болгарія, Великобританія, Казахстан, Норвегія, США, Чеська республіка). У визначеннях, що вживається у цих країнах, складовими поняття також є активи та послуги (Австралія, Великобританія, Канада; Нидерланди та Хорватія).

Система – це сукупність елементів, що характеризуються структурою зв'язками та функціями, які забезпечують цілеспрямований розвиток [21]. Тому активи та послуги можуть бути елементами, сукупність яких складає системи, які в свою чергу є складовими критичної інфраструктури. Аналогічними складовими поняття є й інші: мережі, інформаційні технології, технічні засоби, ланцюжки постачань, природні ресурси, матеріальні блага, засоби виробництва, продукти, організації, конструкції, інститути та служби.

Поширення та виокремлення таких складових як інформаційні технології, мережі, технічні засоби, ланцюжки постачань у визначеннях критичної інфраструктури появ'язані з поширенням інформтехнологій, що призводить до залежності від них громадян, суспільства й держави, уразливостей і загроз.

Поряд з цим, в Нідерландах та Хорватії до складу поняття «критична інфраструктура» входять і супровідні процеси (діяльність), які в разі

порушення або відмови можуть викликати серйозні соціальні негаразди – жертви або економічні збитки та значно вплинути на здоров'я і безпеку громадян або на діяльність влади. Процеси та діяльність об'єктів інфраструктури і є тими зв'язками та функціями, які забезпечують їх цілеспрямований розвиток.

Узявши до відома досвід держав, можливо виокремити поняття критичної інфраструктури: ***сукупність систем, або її елементів (об'єктів) та супровідних процесів, які в разі порушення, відмови або руйнування можуть істотно вплинути на національну безпеку та оборону, природне середовище, економіку, безпеку і здоров'я населення або ефективне функціонування органів державної влади, місцевого самоврядування та громадських організацій.***

У різних країнах прийнято законодачі акти, що розподіляють критичну інфраструктуру на сектори, що в основному збігаються, однак є й відмінності. Так, у США перелік секторів, включених до критичної інфраструктури, є найбільш повним і включає 16 пунктів. Найкоротший в Німеччині – розділена на дві групи, які об'єднують 9 секторів – базову технічну інфраструктуру (водопостачання і водовідведення та видалення відходів, забезпечення енергією, інформаційні та комунікаційні технології, транспорт) та життєво важливу інфраструктуру надання соціально-економічних послуг (парламент та держоргани управління, охорона здоров'я та служби невідкладної допомоги, рятувальні служби, управління у надзвичайних ситуаціях, забезпечення продуктами, правоохоронні органи, фінансовий сектор, страхові компанії, ЗМІ, об'єкти культурної спадщини). Між секторами є взаємозв'язок. Усі соціально-економічні послуги базуються на технічній інфраструктурі, яка залежить від наявності соціально-економічних послуг.

Для України потрібно скласти свій перелік секторів критичної інфраструктури, спираючись на виклики національної безпеки, фінансовий та економічний стан, враховуючи наявні ресурси та необхідность підтримувати і захищати базові функції, для забезпечення безпечного існування людини, суспільства та держави, а також належного захисту національних інтересів.

Наразі в Зеленій книзі з питань захисту критичної інфраструктури в Україні зазначено примірний перелік секторів критичної інфраструктури. Запропоновано 10 секторів: паливно-енергетичний комплекс, транспорт, мережі життєзабезпечення, телекомунікації та зв'язок, фінансово-банківський сектор, органи влади та правопорядку, сектор безпеки і оборони, хімічна промисловість, служби екстреної допомоги та цивільного захисту, харчова промисловість та АПК. Розподіл здійснено відповідно до основних відомств, що відповідають за забезпечення

захисту об’єктів. Недосконаліть цього розподілу полягає в тому, що він ускладнений, сформований на рівні державних органів та не враховує регіональних та місцевих інтересів. Вважаємо більш доцільним розподіл критичної інфраструктури на сектори за сферами життєдіяльності, який є природнім для інфраструктури в цілому, таблиця 3.

Таблиця 3

Сектори критичної інфраструктури (за сферами життєдіяльності)

Назва сектору	Сегменти сектору критичної інфраструктури
Військовий	національна безпека та оборона, військово-промисловий комплекс
Політичний	парламент, органи державної влади, місцевого самоврядування та громадські, політичні організації
Економічний	фінансово-кредитна, комерційно-приватна система
Соціальний	житлово-комунальне господарство, харчування, освіта, охорона здоров’я, культура і мистецтво, спорт
Інформаційний	технічні засоби та інформаційні технології, ланцюжки постачань інформацій, мережі, зв’язок
Екологічний	природні ресуси та охорона навколишнього середовища
Енергетичний	електроенергетика, нафтогазовий комплекс
Виробничий	транспорт, виричничі підприємства, складське господарство, будівництво, сільське господарство
Іноваційний	технопарки, бізнес-інкубатори, система грантів

Після визначення секторів має відбутися складання переліку систем, об’єктів та процесів критичної інфраструктури (її елементів). Його визначення повинно відбуватися, виходячи з потреб та можливостей регіонів відповідно до критеріїв критичності секторів (сегментів), що знайшло відображення в роботах A. Lazari, Д. Бірюкова, С. Кондратова, О. Насвіта, О. Суходолі.

Відповідно до постанови КМУ від 23 серпня 2016 р. №563, до об'єктів критичної інфраструктури відносяться підприємства та установи (незалежно від форм власності) енергетики, хімічної промисловості, транспорту, банків та фінансів, інформтехнологій та телекомунікацій, продовольства, охорони здоров'я, комунального господарства, що є стратегічно важливими.

При визначенні елементів критичної інфраструктури будується ієрархія критеріїв, яка охоплює такі основні групи: державна безпека і оборона; економічна безпека; безпека життєдіяльності та здоров’я населення; національна самоповага та імідж держави.

Для загального розуміння, який об’єкт може бути віднесений до переліку критичних, зазначимо, що ***критичність*** походить від французького Critique та грецького Κριτική τέχνη «мистецтво розбирати,

судження». У Національній стратегії захисту критичної інфраструктури ФРН: ***критичність*** – це відносна міра важливості інфраструктури, що враховує вплив раптового припинення її функціонування або функціонального збою на безпеку постачання, тобто забезпечення суспільства важливими товарами і послугами.

Параметри оцінки критичності мають різну природу та характеризують вплив кризової ситуації на об'єкти критичної інфраструктури з різних боків. Прикладом можуть бути характеристики згідно з Директивою 2008/114/ЄС:

- ✓ масштаб (географічне охоплення території, для якої втрата елементу критичної інфраструктури викликає значну шкоду);
- ✓ взаємозв'язок між елементами критичної інфраструктури;
- ✓ тривалість впливу (як і коли проявлятимуться шкода;
- ✓ вразливість об'єкта до впливу небезпечних чинників;
- ✓ важкість можливих наслідків за показниками в таких групах:

- економічна безпека (вплив на ВВП, розмір економічних втрат, як прямих, так і непрямих, частки продукції на ринку, чисельності зайнятих співробітників, податкових надходжень до бюджету);
- безпека життєдіяльності та здоров'я населення (число постраждалих, загиблих, осіб, які отримали серйозні травми, а також чисельність евакуйованого населення, забезпечення роботи аварійно-рятувальних служб, екстреної допомоги населенню);
- внутрішньополітична й державна безпека (втрата впевненості в дієздатності влади, авторитету держави, порушення управління державою);
- обороноздатність (зниження боєздатності збройних сил, розголошення таємної інформації);
- екологічна безпека (вплив на навколишнє природне середовище) [22].

За рівнем значущості об'єкти можливо поділити на державні, регіональні та місцеві. Крім того, у розвинених державах ідентифікація об'єктів здійснюється на основі методів оцінки загроз та ризиків сталому функціонуванню критичної інфраструктури. Так, у США розроблено методологію оцінки ризиків і загроз електроенергетичній системі на рівні всієї енергосистеми, підсистем і регіональних сегментів, а також окремих об'єктів.

Переліки об'єктів використовуються для планування заходів та у процесі прийняття рішень. Обєктивним є необхідність постійного перегляду переліків, виходячи з факторів: можливі фізичні втрати населення; економічні втрати; величина впливу на життєдіяльність суспільства.

В законодавстві України захист об’єктів, які згідно зі світовою практикою належать до сектору критичної інфраструктури, регламентується численними актами, що носять переважно відомчий характер. Так склалося тому, що кожне відомство бачило певний спектр загроз для підпорядкованих об’єктів і володіло певним набором ресурсів та інструментів для забезпечення їх безпеки.

Перехід від «системи поглядів» на проблему до постановки цілей, завдань, способів та методів здійснення визначено в Стратегії національної безпеки, затвердженої Указом Президента України від 22 червня 2012 р. №389/2012. Зазначено актуальні загрози національній безпеці та пріоритети для забезпечення інформаційної безпеки, кібербезпеки, безпеки критичної інфраструктури та інформресурсів, а проблеми забезпечення безпеки критичної інфраструктури визначено пріоритетами держполітики національної безпеки.

Відповідно до курсу інтеграції України до ЄС вітчизняний сектор безпеки потребує радикальної реформи, що буде відповідати кращим міжнародним практикам та може бути реалізована в концепції критичної інфраструктури, яка активно використовується у провідних країнах ЄС та НАТО. Наразі розроблено та узгоджено проект розпорядження КМУ щодо Концепції створення державної системи захисту критичної інфраструктури, який подано на розгляд уряду.

Результати цієї розробки можуть бути використані при розробці нормативно-правових документів, зокрема, закону про захист критичної інфраструктури. Використання сформованого визначення «критична інфрастуктура» забезпечить компелексний підхід, враховуючи її специфіку, зосереджуючись не лише на сукупності певних обєктів, а й процесах. Це буде запобіжником від можливого «ефекту доміно» при однобічному підході.

Запропонований розподіл критичної інфраструктури на сектори за сферами життєдіяльності є підгрунтям подальших досліджень щодо розроблення критеріїв, оцінювання ризиків та методології віднесення об’єктів до переліку критичної інфраструктури, відповідних секторів та їх сегментів.

Список використаних джерел

1. Закон України «Про основи національної безпеки України» від 19 червня 2003 року № 964-IV // Відом. Верхов. Ради України. – 2003. – № 39.

2. Стихійні лиха та техногенні катастрофи: Превентивні заходи / Всесвітній банк і Організація Об'єднаних Націй; пер. з англ. - М.: А. Паблішер, 2012. - 312 с.

3. Зелена книга з питань захисту критичної інфраструктури в Україні [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/public/File/2015_table/Green%20Paper%20on%20CIP_ua.pdf. – Назва з екрану.

4. Уряднікова І. В. Застосування експертно-аналітичних методів для оцінювання ризиків надзвичайних ситуацій на об'єктах критичної інфраструктури / Уряднікова І. В., Чумаченко С.М. та ін. - Вісник АМУ серія «Техніка», 2015 – Випуск 1 (9) – с. 206 – 216.

5. Developing The Critical Infrastructure Protection System in Ukraine : monograph / [S. Kondratov, D. Bobro, V. Horbulin et al.] ; general editor O. Sukhodolia. – Kyiv : NISS, 2017. – 184 p.

6. Суходоля О.М. В НАНУ представили концепцію створення державної системи захисту критичної інфраструктури. — Українські національні новини / 21 червня 2017. – [Електронний ресурс]. – Режим доступу: http://www.unn.com.ua/uk/news/1672057-v-nanu-predstavili-kontseptsiyu-stvorennya-derzhavnoyi-sistemi-zakhistu-kritichnoyi-infrastrukturi. – Назва з екрану.

7. Lazari A. European Critical Infrastructure Protection. – Springer, 2014. – 154 p.

8. M. Hromada and L. Lukáš, "Conceptual design of the resilience evaluation system of critical infrastructure elements and networks in selected areas in Czech republic", IEEE International Conference on Technologies for Homeland Security, (2012) November 13-15, Boston, USA.

9. P. Auerswald. The Challenge of Protecting Critical Infrastructure / Philip Auerswald, Lewis M. Branscomb Todd, M. La porte, Erwann Michel-kerjan. - Working Paper, October 2005, - № 05-11.

10. Гнатюк С.О., Лядовська В.М. Критерії визначення елементів критичної інфраструктури держави. [Електронний ресурс]. – Режим доступа: http://nauka.zinet.info/23/gnatyuk.php.

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

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

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

14. Безпека критичних інфраструктур [Електронний ресурс].— Режим доступу: http://www.slideshare.net/lukatsky/pir-centercritical-infrastructire-protection.

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

16. USA Patriot Act of 2001 [Електронний ресурс]. – Режим доступу: https://www.gpo.gov/fdsys/pkg/BILLS107hr3162enr/pdf/BILLS107hr3162enr.pdf

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

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

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

20. Гнатюк С. О. Визначення критичної інформаційної інфраструктури та її захисту: аналіз підходів / Гнатюк С. О., Рябий М. О., Лядовська В. М. - Зв'язок. — 2014 № 4, с. 3 – 9.

21. Енциклопедичний словник з державного управління / Ю.В. Сурмін, В.Д. Бакуменко, М.А. Михненко та ін. за ред. Ю.В. Ковбасюка, В.П. Трощинського, Ю.П. Сурміна. – К.: НАДУ, 2010. – 810с.

22. COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/LexUriServ/LexUriServdo?uri=OJ:L:2008:345:0075:0082:EN:PDF. – Назва з екрану.