Міністерство освіти і науки України
Чернівецький національний університет
імені Юрія Федьковича

Факультет історії, політології та міжнародних відносин
Кафедра міжнародної інформації

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ТА ШЛЯХИ УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Дипломна робота

Рівень вищої освіти – другий (магістерський)

Виконала: студентка 6 курсу, групи 604
Спеціальність: 291 Міжнародні відносини, суспільні комунікації та регіональні студії (міжнародні інформація)
Стратійчук Катерина Сергіївна
Керівник: к.політ.н., доцент Осадца І.С.
Рецензент: _____

До захисту допущено:

Протокол засідання кафедри № __

від „____" _____ 2021 р.

зав. кафедри _____ проф. Фісанов В.П.

Чернівці – 2021

ЗМІСТ

ВСТУП

Актуальність дослідження. Світові тенденції до посилення загроз природного і техногенного характеру, активізація терористичної злочинності, збільшення кількості та підвищення складності кібератак, а також пошкодження інфраструктурних об’єктів у східних та південних регіонах України внаслідок збройного конфлікту засвідчують нагальність розгляду питання захисту систем, об’єктів і ресурсів, які є критично важливими для функціонування суспільства, соціально-економічного розвитку держави та забезпечення національної безпеки [120].

Багато держав, в першу чергу економічно розвинуті, вдосконалюють методи та способи використання інформаційних технологій і засобів для деструктивних інформаційних впливів на інформаційні системи об’єктів критичної інфраструктури, під якими в першу чергу сьогодні розуміють атомні і гідроелектростанції, нафто – і газопроводи, національні мережі розподілу електроенергії, транспортні системи національного і світового рівня, загальнодержавні системи зв’язку, галузеутворюючі підприємства тощо [70, с. 44].

Очевидно, що в умовах сучасного надзвичайно інтенсивного розвитку інфраструктури провідних країн світу існує багато об’єктів критичної інфраструктури, виведення з ладу яких може призвести до надзвичайних ситуацій, пов’язаних із загибеллю людей, екологічними катастрофами, заподіянням великих матеріальних та економічних збитків.

Іноземні спецслужби, а також терористичні та кримінальні структури інтенсивно вдосконалюють методи та способи використання інформаційних технологій і засобів, щоб отримати можливість здійснення інформаційних впливів на ресурси систем та мереж державних і недержавних організацій. Тому безпеку промислових об’єктів, зокрема підприємств оборонного комплексу, необхідно розглядати в новому ракурсі, а саме разом з класичними заходами безпеки необхідно забезпечувати інформаційну безпеку автоматизованих систем управління технологічним процесом.

В умовах обмеженості ресурсів та стабільно високої загрози кібератак зі сторони Російської Федерації, виконання покладених на Службу безпеки України завдань по забезпеченню кібербезпеки держави може бути реалізовано, у тому числі, шляхом активного залучення фахівців приватного сектору. Одним із таких завдань, в яких максимально повно можна використати потенціал приватного сектору, є проведення негласної перевірки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів.

Захист об'єктів критичної інфраструктури в Україні врегульований вибірково та, переважно, у підзаконних нормативно-правових актах. Очевидно, що сектор безпеки та оборони України в частині захисту об'єктів критичної інфраструктури потребує реформування, в першу чергу шляхом прийняття відповідного закону та удосконалення діючих нормативно-правових актів в частині, що стосується саме критичної інфраструктури, комплексного управління та підготовку фахівців з питань захисту об'єктів критичної інфраструктури.

Відповідно, **метою** дослідження є вивчення проблем забезпечення та шляхів удосконалення безпеки об'єктів критичної інфраструктури України.

Реалізація поставленої мети досягається шляхом розв'язання наступних дослідницьких **завдань**:

- проаналізувати сучасні наукові підходи до вивчення питання захисту інформаційної безпеки об'єктів критичної інфраструктури країни;
- розглянути загальну систему забезпечення безпеки і захисту об'єктів критичної інфраструктури країни;
- охарактеризувати досвід зарубіжних країн та України стосовно державного управління забезпеченням безпеки об'єктів критичної інфраструктури;
- дослідити нормативно-правове та адміністративне забезпечення безпеки об'єктів критичної інфраструктури в Україні;

- вказати на напрями удосконалення державної політики забезпечення безпекою об’єктів критичної інфраструктури в Україні.

Об’єктом дослідження є суспільні відносини у сфері забезпечення безпеки об’єктів критичної інфраструктури України.

Предметом дослідження виступає розвиток механізмів забезпечення та шляхи вдосконалення безпеки об’єктів критичної інфраструктури України.

Обрана тема наукового дослідження потребує застосування різних наукових методів та підходів для отримання достовірного результату. Саме тому для розв’язання поставлених завдань автор використовував такі загальнонаукові та спеціальні **методи дослідження як**: аналізу та синтезу – для деталізації об’єкта дослідження; узагальнення – для розкриття теоретико-методологічних засад механізмів забезпечення безпеки об’єктів критичної інфраструктури; порівняльний метод та систематизації – для вивчення нормативно-правового та адміністративного забезпечення безпеки об’єктів критичної інфраструктури; системний метод – для розкриття концептуальних основ забезпечення об’єктів критичної інфраструктури; порівняння та узагальнення – при дослідженні особливостей забезпечення безпеки об’єктів критичної інфраструктури; метод моделювання – для розроблення перспективних напрямів застосування механізмів реалізації державної політики безпеки об’єктів критичної інфраструктури та можливих шляхів удосконалення системи безпеки об’єктів критичної інфраструктури України.

Теоретичне і практичне значення роботи полягає у тому, що результати дослідження можуть бути корисними для подальших наукових досліджень з даної проблематики, а також для читання курсів з інформаційної безпеки, теорії прийняття рішень тощо.

Структура й обсяг роботи обумовлені предметом дослідження, його метою і завданнями. Вона складається із вступу, трьох розділів, висновків та списку використаних джерел, який налічує 158 найменувань. Основний текст викладено на 81 сторінках, загальний обсяг роботи становить 101 сторінку.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ

1.1. Сучасні наукові підходи до вивчення питання захисту інформаційної безпеки об'єктів критичної інфраструктури країни

Внаслідок стрімкого розвитку суспільних відносин в епоху глобалізації та інформатизації навіть добре відомі й давно усталені поняття починають набувати свого нового змісту, а значить потребують переосмислення і перегляду. Тож відбувається розширення меж того чи іншого поняття, уточнення його законодавчої дефініції.

Поняття «інфраструктура» має латинське походження, звідки воно розповсюдилося у більшості європейських мов. У сучасній українській літературній мові Академічний тлумачний словник трактує його, як «Сукупність галузей і видів діяльності, що обслуговують як виробничу, так і невиробничу сфери економіки (транспорт, зв'язок, комунальне господарство, загальна і професійна освіта, охорона здоров'я тощо)» [126, с. 686]. Звісно, подібна інтерпретація, яка з'явилася понад 40 років тому, потребує свого оновлення з урахуванням появи реалій, які досі не існували. Також, про це пам'ятати у зв'язку з розвитком науки і техніки, глобалізацією суспільних процесів, інформатизацією, виникненням до того не чуваних загроз національній і міжнародній безпеці.

У спеціалізованих словниках поняття «інфраструктура» тлумачиться на підставі об'єктно-предметних підходів конкретних наук. Так, «Енциклопедичний словник з державного управління» під даним терміном розуміє «Структуру суспільства або організації, комплекс виробничих і невиробничих галузей, які забезпечують умови відтворення та надання послуг технічного, технологічного, соціально-економічного, маркетингового, фінансового, юридичного, інформаційно-комунікативного, освітнього та іншого характеру» [41] Важливо також є те, що це тлумачення вказує на комплексний, взаємозв'язаний характер складових елементів даного поняття. У наведеній дефініції є й дискусійні, подекуди навіть спірні моменти.

Зокрема, багато експертів звертають увагу на тому, що інфраструктура відноситься до сфери послуг, що певною мірою звужує діапазон функціонування поняття. Крім цього, дискусію викликаю і те, що в тлумаченні не враховується можливість існування інфраструктури, зокрема інформаційної, у віртуальному просторі, а це якраз сьогодні напевно найбільш вразлива категорія. Таким чином, наведене тлумачення не можна вважати вичерпним.

На погляд багатьох аналітиків, експертів та фахівців в даній сфері, зокрема і С. Теленика, при описі цього поняття варто було б «…зосередитися на його забезпечувальному, а не обслуговуючому характері. І в цьому є принципова різниця, адже без багатьох послуг можна обійтися або замінити їх іншими, а от якщо йдеться про забезпечення життєво важливих потреб, захист життєво важливих інтересів людини, суспільства, держави, то тут виникають абсолютно інші парадигми» [136].

Поняття критичної інфраструктури сьогодні знаходиться на етапі становлення. Щоправда, правотворча та наукова активність довкола нього повсякчас посилюється, про що говорить значна кількість нових досліджень даного питання.

В окремих нормативних актах запропоновано визначення цього поняття. Так, у Постанові Кабінету Міністрів України «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави» від 23 серпня 2016 року № 563 його охарактеризовано як «Сукупність об’єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу чи руйнування яких може мати вплив на національну безпеку й оборону, природне середовище, призвести до значних фінансових збитків і людських жертв» [108]. У розпорядженні Кабінету Міністрів України від 6 грудня 2017 року № 1009-р визначення поняття критичної інфраструктури сформульовано як «Сукупність об’єктів, які є стратегічно важливими для економіки й безпеки

держави, суспільства, населення та порушення функціонування яких може завдати шкоди життєво важливим національним інтересам України» [120].

Про поняття «критична інфраструктура» йдеться і в Указі Президента України «Про рішення Ради національної безпеки та оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» від 26 травня 2015 року № 287/2015, у якому серед загроз національній безпеці України визначено загрози безпеці критичної інфраструктури, а саме: «Критична зношеність основних фондів об'єктів інфраструктури України та недостатній рівень їх фізичного захисту; недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій; неефективне управління безпекою критичної інфраструктури та систем життєзабезпечення» [135].

Визначення поняття критичної інфраструктури пропонують в окремих публікаціях, цільових дослідженнях та інших працях, підготовлених у зв'язку з актуалізацією проблеми в різні роки з огляду на соціально-економічні, політичні, воєнні й інші умови та чинники.

Що відноситься до категорії критична інфраструктура? Тут перелік може бути досить великий. Досить вичерпно про класифікував дане поняття О. Верголяс, який вказує, що «Критична інфраструктура – це підприємства й установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології, телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки та безпеки держави, суспільства, населення, виведення з ладу або руйнування яких може позначитися на національній безпеці й обороні, природному середовищі, призвести до значних матеріальних і фінансових збитків, людських жертв» [21].

З іншого боку, відомий український дослідник питання захисту об'єктів критичної інфраструктури Д. Бірюков визначає дане поняття наступним чином: «Критична інфраструктура – це сукупність об'єктів, технологій,

державних і наукових структур, порушення регламентної діяльності яких впливає на економічну, соціально-політичну, військову, екологічну безпеки» [14, с. 89].

А С. Теленик акцентує увагу на тому, що «Термін «критична інфраструктура» охоплює об'єкти, системи, мережі або їх частини, порушення функціонування або руйнування яких призведе до найтяжчих наслідків для соціальної та економічної сфери держави, негативно позначиться на рівні її обороноздатності та національної безпеки. Крім того, функціонування критичної інфраструктури в мирний час пов'язують із підтримуванням життєво важливих функцій у суспільстві, захистом базових потреб його членів і формуванням у них відчуття безпеки та захищеності. Критична інфраструктура України – це системи й ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни, забезпечення національної безпеки» [135].

Всі науковці приходять до спільного висновку, що «…сьогодні захист критичної інфраструктури України – це комплекс заходів, реалізований у нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури» [57, с. 11].

На підставі розглянутих різних дефініцій, С. Теленик підсумовує та приходить до висновку, що поняття критичної інфраструктури визначають, враховуючи такі елементи, як: «1) загальне визначення критичної інфраструктури як сукупності об'єктів; 2) ознаки, за якими об'єкти критичної інфраструктури визначаються як такі; 3) можливі впливи на об'єкти критичної інфраструктури та їх наслідки; 4) державні, суспільні інтереси та відносини, яким може бути завдано шкоди [135].

Проте змістове наповнення цих елементів неоднакове, продовжує автор. Це пояснюється тим, що трансформація поняття критичної

інфраструктури відбувається під впливом об’єктивних чинників й обставин. Ці чинники і обставини в свою чергу визначають пріоритетність тих чи тих проблем, пов’язаних із забезпеченням нормального функціонування та захисту об’єктів критичної інфраструктури.

Як бачимо з вище наведених тлумачень, з позицій змісту структурних елементів поняття критичної інфраструктури, вони подекуди носять хаотичний характер, певну неузгодженість між пунктами переліку, неповноту розкриття деяких випадків й правову невизначеність окремих пунктів та положень. Тому, в нових дослідження часто автори вказують на потребі додаткового дослідження й опрацювання даного поняття.

Про це також пише і С. Теленик в одному із своїх останніх досліджень під назвою «Критична інфраструктура як об’єкт адміністративно-правового регулювання». Так, він наголошує, що «Критичну інфраструктуру визначають як: 1) сукупність об’єктів; систем, об’єктів і ресурсів; 2) сукупність об’єктів інфраструктури держави; 3) підприємства й установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології і телекомунікації (електронні комунікації), продовольство, охорона здоров’я, комунальне господарство; 4) сукупність об’єктів, технологій, державних і наукових структур; 5) об’єкти, системи, мережі або їх частини; системи й ресурси, фізичні чи віртуальні, що забезпечують функції та послуги» [135].

Ознаки, за якими певні об’єкти відносять до критичної інфраструктури, продовжує автор визначають як: 1) критично важливі; 2) найбільш важливі; 3) стратегічно важливі. Ну і, як підсумовую дослідник, «Можливі впливи на об’єкти критичної інфраструктури та їх наслідки трактують як: 1) загрози природного й техногенного характеру; 2) терористичні загрози; 3) кібератаки; 4) пошкодження інфраструктурних об’єктів у східних та південних регіонах України внаслідок збройного конфлікту; 5) виведення з ладу або руйнування; 6) порушення функціонування; 7) порушення регламентної діяльності. Їхні наслідки такі: 1) значні матеріальні та фінансові

збитки, людські жертви; 2) найтяжчі наслідки; 3) найсерйозніші негативні наслідки» [135]. З іншого боку, науковець не забуває також описати і державні інтереси і відносини в цій сфері. Він їх характеризує наступним чином: «Суспільні, державні інтереси та відносини, яким може бути завдано шкоди, окреслюють так: 1) функціонування суспільства, соціально-економічного розвитку держави та забезпечення національної безпеки; 2) життєво важливі національні інтереси України; 3) інтереси економіки і безпеки держави, суспільства, населення; 4) національна безпека й оборона, природне середовище; 5) економічна, соціально-політична, військова, екологічна безпека; 6) соціальна й економічна сфери держави; 7) рівень обороноздатності та національної безпеки; 8) життєдіяльність суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки» [135].

Критична інформаційна інфраструктура – сукупність об’єктів критичної інформаційної інфраструктури [117]: сукупність інформаційних систем, інформаційно-телекомунікаційних мереж, автоматизованих систем управління суб’єктів критичної інформаційної інфраструктури, у тому числі мережі електрозв’язку, що використовуються для організації взаємодії таких об’єктів [24; 25; 14]. У Стратегії розвитку інформаційного суспільства в Україні [130], зазначено, що «інформаційна інфраструктура – сукупність різноманітних інформаційних (автоматизованих) систем, інформаційних ресурсів, телекомунікаційних мереж і каналів передачі даних, засобів комунікацій і управління інформаційними потоками, а також організаційно-технічних структур, механізмів, що забезпечують їх функціонування».

При всій близькості визначень цього терміну в законодавстві іноземних країн, існують відмінності у цьому понятті. Під критичною інфраструктурою в США розуміють «Комплекс фізичних та віртуальних активів, систем і мереж, що мають життєво важливе значення для держави, руйнування або недієздатність яких, в тому числі і окремих їх елементів, матиме згубні наслідки для національної безпеки, економіки, безпеки і здоров’я населення,

чи матиме будь-яку комбінацію з перелічених наслідків» [158]. У США до критичної інфраструктури відносять системи, мережі та окремі об'єкти, порушення роботи або руйнування яких може спричинити величезні або навіть незворотні негативні наслідки для економіки, добробуту та здоров'я населення, стабільного перебігу політичних процесів [157]. Концепція захисту критичної інфраструктури реалізована також у таких розвинутих країнах, як: Канада, Австралія, Велика Британія. Зазначимо, що в більшості з них ідентифікація об'єктів критичної інфраструктури здійснюється відповідно до затверджених методів оцінювання загроз та ризиків сталому її функціонуванню [85]. У законодавстві Великобританії, наприклад, критична інфраструктура визначена як: «Найважливіші елементи інфраструктури, а саме активи, об'єкти, системи, мережі, процеси і ключові посадови особи, втрата яких може привести до згубного впливу на: 1) доступність, цілісність або надання основних послуг, в тому числі тих, порушення цілісності яких може привести до втрати життя або виникнення нещасних випадків з урахуванням значних економічних і соціальних наслідків; 2) національну безпеку, національну оборону або функціонування держави» [155]. В окремих державах ЄС критична інфраструктура це «Активи, системи або їх частини, що розташовані в державах-членах Європейського Союзу, які мають важливе значення для основних життєво важливих соціальних функцій, здоров'я, безпеки, економічного або соціального благополуччя людей, а також порушення або руйнування яких матиме значний вплив на спроможність держави виконувати свої функції» [148].

На важливість захисту критичної інфраструктури вперше звернули увагу в США ще в далекому 1995 р. А вже після атак 11 вересня 2001 р. забезпечення захисту та стабільного функціонування життєво важливих об'єктів інфраструктури стало найважливішим і обов'язковим складником національної безпеки розвинутих країн світу. Так, уряд Австралії дав визначення критичної інфраструктури та розробив стратегію стійкості критичної інфраструктури. Під критичною інфраструктурою визначено «Ті

фізичні об’єкти, ланцюги поставок, інформаційні технології і мережі зв’язку, які, якщо вони будуть знищені, деградовані або виявляться недоступними протягом тривалого періоду часу, значно впливатимуть на соціальне життя або економічний добробут нації або на здатність Австралії здійснювати національну оборону і забезпечувати національну безпеку» [149].

На рівні ЄС термін «критична інфраструктура» визначається у двох ключових документах. Перший – «Зелена книга» за Програмою захисту критичної інфраструктури, опублікована у 2005 р. Європейською комісією [152]. Друга – директива Ради ЄС 114 від 8 грудня 2008 р. щодо визначення і позначення європейських КІ і оцінювання необхідності підвищення їх захисту [148]. Директива визначає критичну інфраструктуру як «Актив, систему чи її частину, що має місце в країнах-членах ЄС, вплив яких у разі відмови, інциденту або зловмисного втручання буде поширюватися як на країну, де такий об’єкт розташований, так і на хоча б одну іншу країну-член ЄС». Згідно з цією директивою критичність інфраструктури визначається при «…перевищенні порогових значень впливів на відповідні сектори інфраструктури та її об’єкти». Директива залишає відповідальність за захист критичної інфраструктури національним органам влади. Про все це детально пише у своїй роботі О. Мельничук [85].

З наведених визначень видно, що відмінності у терміні «критична інфраструктура» в різних країнах світу не суттєві. Терміни покликані відобразити національну, організаційну особливість унікальності сфери його застосування, відмінності нормативно правових систем.

Окремі країни, об’єднання держав здійснюють захист національних та колективних інтересів, не обмежуючись своїми кордонами. Крім національних об’єктів критичної інфраструктури, розглядаються також і зарубіжні об’єкти, безпека яких має стратегічне значення для тієї чи іншої держави. У законодавстві ЄС з’явився також термін «європейська критична інфраструктура», який тлумачиться наступним чином: «Це критична інфраструктура, що розташована в державах членах Європейського Союзу,

недієздатність або руйнування якої матиме істотний згубний вплив на принаймні дві держави Союзу» [44].

Критичність можна визначити, розглядаючи елементи чи об’єкти інфраструктури, потоки товарів і послуг, потреби клієнтів, можливості пошукових і рятувальних організацій та ресурси для пом’якшення наслідків. Критерії критичності часто використовуються для визначення та оцінювання інфраструктури для створення інвентаризації, регістрів ризиків та пріоритетів захисту [153]. Критерії критичності розглядали С. Ріналді, Дж. Піренбум, Т. Келлі та ін. для конкретних аспектів, наприклад виміру взаємозалежності, та стосовно системних невдач, наслідків невдач, окремих небезпек або підходу до загального ризику [146].

У США розробили методологію оцінювання ризиків і загроз електроенергетичній системі на рівні всієї енергосистеми, підсистем і регіональних сегментів, а також окремих об’єктів. Федеральне міністерство внутрішніх справ Німеччини використовує оцінювання критичності як попередній крок до виявлення пріоритетних ділянок, надалі відбувається більш детальний аналіз ризиків, уразливості. Однак, у більшості випадків, як вказує О. Мельничук, «Оцінювання критичності інфраструктури є лише іншим визначенням оцінювання ризику, уразливості або оцінювання стійкості інфраструктури, при цьому загальні критерії для визначення критичної інфраструктури та структурованих концепцій аналізу критичності є досі не сформованими» [85].

Ідентифікація об’єктів критичної інфраструктури також передбачає залучення широкого кола учасників, експертів, фахівців та застосування механізмів взаємодопомоги, у тому числі на міжрегіональному рівні, для забезпечення обміну інформацією та координації зусиль щодо використання всіх ресурсів [85].

Критична інформаційна інфраструктура відрізняється від інформаційної інфраструктури включенням автоматизованої системи управління суб’єктів критичної інформаційної інфраструктури та систем

електрозв'язку в якості об'єктів критичної інформаційної інфраструктури [61].

Відповідно до чинного Закону України «Про Національну програму інформатизації» [113] під об'єктом інформатизації доцільно розуміти сукупність інформаційних ресурсів, засобів і систем обробки інформації (відомостей та/або даних [110]), які використовуються відповідно до заданої інформаційної технології, засобів забезпечення, приміщень або об'єктів (будівель, споруд, технічних засобів), в яких ці засоби і системи встановлені, або приміщень і об'єктів, призначених для ведення конфіденційних переговорів [113]. До об'єктів критичної інформаційної інфраструктури доцільно віднести автоматизовані системи управління, що належать державним установам і органам влади, юридичним і фізичним особам-підприємцям, які забезпечують взаємодію зазначених систем або мереж, що функціонують у сфері охорони здоров'я, освіти і науки, транспорту, зв'язку, енергетики, банківській сфері та інших сферах фінансового ринку, паливно-енергетичного комплексу, у галузі атомної енергії, оборонної, ракетно-космічної, гірничодобувної, металургійної, хімічної промисловості і т. д. [61].

У Порядку формування переліку об'єктів критичної інформаційної інфраструктури, затвердженого постановою Кабінету Міністрів України від 09.10.2020 р. № 943, з метою визначення сукупності інформаційних об'єктів і ресурсів, систем і засобів обробки інформації зазначено, що «… всі об'єкти інформаційної інфраструктури (автоматизовані, інформаційні, телекомунікаційні, інформаційно-телекомунікаційні системи, автоматизовані системи управління технологічними процесами), що експлуатуються на об'єкті критичної інфраструктури», а також представлено загальні засади взаємозв'язку Національної програми інформатизації та системи планування економічного і соціального розвитку України [99]. В контексті цього доцільно також відмітити, що у Законі України «Про основні засади кібербезпеки України» [117] для визначення тих же відносин застосовується поняття «об'єкт критичної інформаційної інфраструктури».

Вперше на небезпеці знищення або пошкодження об’єктів критичної інфраструктури наголошено у рішенні РНБО України від 01.03.2014 року «Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України» [114]. Важливість захисту критичної інфраструктури для забезпечення національної безпеки визначена у Стратегії національної безпеки України та рішеннях РНБО України 2016-2017 років. Суттєві кроки у напрямі законодавчого регламентування критичної інфраструктури було зроблено із прийняттям Стратегії кібербезпеки України [129], Закону України «Про основні засади забезпечення кібербезпеки України» [117] та Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави [108].

Інформаційна інфраструктура – це частина інформаційної сфери, яка є складно організованою системою, створюваною та функціонуючою на засадах принципів і механізмів міжнародного та національного правового регулювання суспільних відносин.

Маємо ситуацію, що в Україні на сьогоднішній день законодавчо не визначено єдине поняття критичної інфраструктури та не унормований уніфікований перелік її об’єктів [44]. Зважаючи на відсутність законодавчого визначення терміну «критична інфраструктура», ми пропонуємо ст. 1 Закону України «Про національну безпеку України» доповнити визначенням понять: – критична інфраструктура – це об’єкти, які є стратегічно важливими для економіки і національної безпеки, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних фінансових збитків та людських жертв; – об’єкти критичної інформаційної інфраструктури – це сукупність інформаційно-телекомунікаційних систем державного та приватного сектору, що забезпечують функціонування та безпеку стратегічних інститутів, систем і об’єктів держави (органів центрального та місцевого управління, систем управління енергетикою, транспортом, зв’язком, банківським сектором,

підприємств, під час діяльності яких використовуються та/або виробляються небезпечні речовини тощо) і безпеку громадян (системи управління правоохоронних структур й оборонного сектору тощо), несанкціоноване втручання в роботу яких може загрожувати економічній, екологічній, соціальній та іншим видам безпеки або завдати шкоди міжнародному іміджу держави.

1.2. Аналіз джерельної бази дослідження

Враховуючи важливість питання, його значущість для держави і суспільства, чимало вітчизняних і зарубіжних вчених присвятили свою творчість науковій проблематиці, пов'язаній із різними аспектами забезпечення безпеки об'єктів критичної інфраструктури, діяльності спеціальних суб'єктів, визначення потенційних загроз вказаним об'єктам. З позицій права, важливими є наукові праці таких дослідників, як Д. Бобро, О. Глушкевич, В. Голубєв, О. Єрменчук, Г. Зубко, В. Ліпкан, І. Манжул, О. Суходоля, С. Теленик, В. Цигичко та ін. У полі зору науковців зазвичай знаходяться питання, що умовно можна визначити як надбудову над понятійно-категоріальним апаратом правової науки, оскільки акценти робляться на рекомендаціях щодо захисту об'єктів, інтерпретацію чинних нормативно-правових актів з відповідних питань, а відтак і підготовку пропозицій щодо їх удосконалення.

У цілому тематика взаємодії в науковому плані достатньо повно досліджена в роботах науковців у галузі адміністративного права, зокрема: В. Авер'янова, В. Афанасьєва, О. Бандурки, Д. Бахраха, Ю. Битяка, А. Васильєва, Т. Возної, В. Галунька, В. Гаращука, І. Голосніченка, Є. Додіна, С. Ківалова, З. Кісіль, В. Ковальського, Л. Коваля, В. Козака, Г. Кохан, Є. Кубко, В. Курила, О. Кушнір, Б. Лазарева, К. Левченко, В. Ліпкана, Я. Лизогуба, Л. Морозова, О. Надьон, Н. Нижник, В. Опришка, О. Орлеана, Н. Осипової, О. Полінця, В. Поліщука, П. Рабіновича, В. Ремньова, Ю. Римаренка, Л. Савченко, А. Селіванова, А. Сироти, С. Стеценка, М.

Студенікіної, Ю. Тихомирова, М. Тищенка, Р. Халфіної, В. Цвєткова, В. Чиркіна, Ю. Шемшученка, В. Шестака, К. Шоріної та інших.

Замало таких згадок і теоретичних розробок щодо окреслених питань як у дослідженнях працівників Національного інституту стратегічних досліджень, так і у спеціалізованих дослідженнях, де предметом виступає формування державної системи захисту критичної інфраструктури: Д. Бірюкова, Д. Бобра, О. Власюка, С. Гончара, В. Горбуліна, Д. Дубова, О. Єрменчука, Г. Зубка, С. Іванюти, С. Кондратова, М. Ожевана, А. Семенченка, О. Суходолі, В. Шемаєва та ін.

Окремі аспекти проблематики, зокрема застосування методів наукового пізнання при формуванні правових моделей регулювання суспільних відносин у тих чи інших сферах, знайшли своє відображення в наукових роботах таких дослідників теоретиків права: С. Алексєєв, Д. Бахрах, С. Бобровник, С. Гусарєв, В. Ісаков, В. Копєйчиков, В. Ліпкан, А. Малько, Н. Матузов, П. Рабінович, І. Соколова, В. Сорокін, О. Тихомиров, Л. Томаш, Л. Явич.

Сьогодні, в українському науковому середовищі існує чимала кількість дослідження пов’язаних із адміністративно-правовим регулюванням функціонування об’єктів критичної інфраструктури України [4; 125; 143, с. 40-41; 60; 26; 2; 1]. Перш-за все варто виділити роботу В.Д. Ткаченко та Є.Б. Ручкіна, які вважають, що « …необхідними умовами існування та гармонійного розвитку будь-якого суспільства є узгодження інтересів різних його членів, встановлення і підтримування у стосунках між ними певного встановленого порядку. Основне навантаження в реалізації зазначених функцій лягає на спеціально пристосовану до особливостей суспільного буття розгалужену систему соціальної регуляції, важливе місце в якій посідає правове регулювання, що в загальному вигляді може бути охарактеризовано, як процес дії за допомогою правових норм та інших юридичних засобів на поведінку людей з метою упорядкування, охорони та розвитку суспільних відносин» [137, с. 404].

Дослідження поняття механізму АПР в цілому та окремих його структурних елементів проводили такі вчені-адміністративісти, як В. Авер'янов, С. Алексєєв, Ю. Битяк, В. Галунько, Т. Гончарук, С. Гусаров, Ю. Дьомін, Т. Кашаніна, В. Колпаков, Т. Коломоєць, О. Копиленко, А. Крижанівський, В. Курило, О. Кузьменко, В. Ладиченко, М. Миронюк, А. Монаєнко, Д. Овсянко, С. Стеценко та інші. Водночас, механізм адміністративно-правового регулювання у сфері захисту критичної інфраструктури ще не розглядався.

Проблеми правового забезпечення кібербезпеки критичної інформаційної інфраструктури України неодноразово знаходили відображення у працях О. Баранова, П. Гарасима, К. Бєлякова, С. Божок, І. Діордіци, В. Ліпкана, Н. Коваленка, Б. Кормича, І. Кушнір, О. Малашка, Ю. Максименка, М. Микитюка, Л. Сопільника, М. Стрельбіцького, О. Тихомиров, О. Юдіна та ін. Визнаючи теоретичну і практичну цінність окремих досліджень за проблемою, доцільно відмітити, що у наукових і навчально-методичних працях вищезгаданих та інших українських вчених-юристів існує цілий ряд дискусійних питань і розбіжностей у поглядах щодо вирішення наукових і практичних проблем у сфері правового забезпечення кібербезпеки критичної інформаційної інфраструктури України.

Огляд наукових публікацій за досліджуваною темою дозволяє констатувати, що зараз чітко окреслюються три основні напрями, які представлені найбільш об'ємно. До першого з них можна віднести ті роботи, в яких обґрунтовується необхідність організаційно-правового унормування підготовки фахівців із ЗКІ. Зокрема йдеться про наукові доробки за авторством Д. Бірюкова, Д. Бобра, О. Єрменчука, В. Горбуліна, Ю. Косенко, П. Носова, О. Олійника, О. Суходолі та ін. Показово, що своє відображення дана проблема певною мірою знаходить і в аналітичних доповідях до щорічного послання Президента України до Верховної Ради України, які готуються фахівцями Національного інституту стратегічних досліджень [5; 6].

Другий напрям в умовній класифікації наукових публікацій представлений дослідженнями з питань підготовки фахівців у галузі інформаційних технологій та кібернетичної безпеки. Наразі йдеться про роботи Л. Арсеновича, В. Богуша, В. Бикова, В. Бурячка, Ю. Даника, І. Діордици, Ю. Дмитренка, В. Ліпкана, Ю. Максименко, О. Мандзюка, А. Міночкіна, І. Пархомея, М. Савчука, В. Сисоєва, М. Степанова, Ю. Супрунова, В. Толубка, О. Топчий та ін.

До умовно виділеного третього напряму належать наукові праці, в яких міститься порівняльний аналіз й узагальнення досвіду підготовки фахівців окремих сегментів ЗКІ у зарубіжних країнах. Така проблематика доволі успішно розробляється Б. Бистровою, Є. Брижатим, О. Гадою, А. Демків, Г. Зубко, В. Михайловим, Ю. Приходьком, Т. Сліпченко та ін.

Попри те, що діє низка нормативних актів, які стосуються захисту критично важливих систем, об’єктів і ресурсів, не розроблено єдиного механізму захисту, що на практиці призводить до неузгодженості дій різних суб’єктів, які здійснюють такий захист, несвоєчасного реагування на загрози, для нейтралізації яких потрібна різногалузева консолідація ресурсів, а також нераціонального, безсистемного використання сил і засобів тощо. Із цього приводу Д. Бірюков зазначає, що «В нашому законодавстві є низка категорій об’єктів, виокремлених на підставі їх значущості для економіки, техногенної безпеки, терористичної загрози тощо. У контексті міжнародної практики ці об’єкти (або певну частину цих об’єктів) можна вважати критичною інфраструктурою. Проблему становлять не просто нерозроблення переліків об’єктів чи визначення поняття «критична інфраструктура», а неналагодженість взаємозв’язку між цими категоріями, інформаційного взаємозв’язку між відомствами, брак загального оцінювання на рівні держави ризиків цих об’єктів, спільного підходу до захисту від усіх груп загроз (техногенного, природного та соціально-політичного спрямування). Немає загальної (спільної) бази ресурсів для реагування та запобігання загрозам, яка повинна містити інформацію не тільки від Міністерства надзвичайних

ситуацій, а й від Міністерства регіонального розвитку, будівництва та житлово-комунального господарства України, де збирають інформацію про наявну кількість місць у лікарнях малих міст України та ступінь забезпечення медичним персоналом» [14, с. 76]. Тому потребує перегляду й удосконалення наявний підхід до захисту об'єктів критичної інфраструктури та його правове забезпечення.

Сучасні виклики та пріоритетні завдання сектору безпеки у процесі захисту критичної інфраструктури у своїх наукових працях досліджував Суходоля О. [132]. Проблеми, що стосуються захисту критичної інфраструктури та забезпечення інформаційної безпеки об'єктів критичної інфраструктури розглядались Гончаром С., Леоненком Г., Юдіним О. [27] Проблемні аспекти правового регулювання державно-приватного партнерства у сфері захисту критичної інфраструктури досліджувались Єрменчуком О., Пальчиком М. [43] Проблеми та перспективи впровадження захисту критичної інфраструктури в Україні були проаналізовані Бірюковим Д. [13], Кондратовим С., Насвітом О. [57].

Д. Бірюков в аналітичній доповіді «Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні» наводить у якості можливого прикладу для застосування в Україні досвіду деяких зарубіжних держав в цій сфері. Зокрема, науковець на підставі аналізу міжнародного досвіду визначає, що «Основою забезпечення захищеності й безпеки критичної інфраструктури є вирішення низки питань, з-поміж яких основними виділяє такі: координація і взаємодія органів державної влади та обмін інформацією про загрози; організація державно-приватного партнерства у сфері безпеки; використання ризик орієнтованого підходу при попередженні загроз критичній інфраструктурі» [14, с. 5].

Питання сутності управління безпекою та критичною інфраструктурою розглядали такі вітчизняні учені: В. Абрамов, Д. Бірюков, Д. Бобро, О. Їжак, Г. Ситник, А. Семенченко, О. Суходоля, В. Лядовська, С. Кондратов, С. Кулінська, В. Куйбіда, О. Насвіт, А. Пашков, І. Уряднікова, Л. Щаслива та ін.

Крім того, дослідженню проблемних питань безпеки КІ присвячені праці А. Біаласа, А. Венгера, Д. Гритзаліса, Т. Келлі, А. Лазарі, В. Майєра, Д. Рехака, С. Ріналді, А. Фекете, П. Хокстада та ін.

Становлення та формування сфери кіберзахисту та кібербезпеки в Україні нерозривно пов’язано із забезпеченням сфер захисту інформації та інформаційної безпеки [59; 138; 46; 45; 138; 100; 101]. Окремо варто виділити роботу групи науковців Мартинюк В, , Паламарчук Н., Паламарчук С. та Сівоха О. під назвою «Задачі вдосконалення інформаційної та кібернетичної безпеки об’єктів критичної інфраструктури», які вказують на те, що «Управління інформаційною та кібернетичною безпекою об’єктів критичної інфраструктури ґрунтується на знаннях про стан об’єктів управління, стан середовища функціонування і про впливи, які відбуваються» [81].

РОЗДІЛ 2. СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ КРАЇНИ: МІЖНАРОДНИЙ ДОСВІД ТА УКРАЇНСЬКІ РЕАЛІЇ

2.1. Загальна система забезпечення безпеки і захисту об'єктів критичної інфраструктури країни

Сучасне суспільство стрімко розвивається, що постійно призводить до різних загроз, які в основному спричинені стихійними лихами, технічними аваріями чи людським фактором, тероризмом чи злочинними діями тих же людей. Отже, перед людством в цілому та державами зокрема постає питання про заходи щодо захисту економічних та соціальних елементів інфраструктури, причому воно є абсолютно необхідними. На особливому рахунку в цій ситуації є об'єкти критичної інфраструктури, які мають особливе значення для держави та суспільства. Недієздатність таких об'єктів призведе до змін у житті людей, тривалих перебоїв у постачанні сировинних продуктів, серйозних порушень громадської безпеки чи інших значних драматичних наслідків [88; 89].

На думку всіх дослідників даної тематики, то «Якщо дивитися конкретно на об'єкти критичної інфраструктури та їх захист, то тут необхідно передбачити та розробити заходи щодо, які б мінімізували та усунули шкоду, але, перш за все, профілактичні заходи, які можуть запобігти серйозним аваріям спочатку або хоча б мінімізувати їх наслідки» [38].

Окремо варто сказати про те, що загроза пошкодження критично важливого об'єкта інфраструктури залежить від взаємного положення джерела небезпеки та об'єкта впливу його небезпечних факторів у просторі та часі (для стаціонарних об'єктів лише у просторі). З іншого боку, час небезпеки становлять загрозу лише тоді, коли вони можуть завдати шкоди конкретним об'єктам. Небезпека або кілька різних небезпек становлять загрозу для критично важливого об'єкта інфраструктури, лише якщо їх небезпечні фактори можуть впливати на нього. Наприклад, «Для людей

загроза виникає, коли вони працюють на об’єкті підвищеної небезпеки або в зоні забруднення, а для рухомих об’єктів – коли вони під час небезпечної події знаходяться в зоні впливу небезпечних чинників» [51; 142].

Ступінь загрози життю населення в даній місцевості та, відповідно, критичній інфраструктурі залежить від ступеня її небезпеки, а також від географічних та часових факторів. «Якщо об’єкт перенести за межі небезпечної території, загрози для нього не буде, хоча небезпека території залишатиметься. Загроза життєдіяльності з часом змінюється: вона може виникати, збільшуватися, зменшуватися. Безпека населення, різних об’єктів та навколишнього середовища та об’єктів критичної інфраструктури у разі можливих техногенних аварій та стихійних лих у надзвичайних ситуаціях встановлюється оцінкою ризику для окремого підприємства чи території порівняно з відповідними нормативними параметрами» [66; 142].

Як діють відповідно до завданої шкоди після кризової ситуації. В першу чергу особам що відповідальні за це потрібно спрогнозувати наслідки надзвичайної ситуації. Прогнозування наслідків надзвичайних ситуацій для об’єктів критичної інфраструктури здійснюється в кілька етапів, точніше 3 етапи.

Детально про кожен з цих випадків у своїй роботі пише Д.Г. Бобро. Він зазначає, що «На І етапі встановлюють параметри впливів − значущих вражаючих факторів, що викликають основні руйнування й ураження, з характеристиками, що зазвичай приймаються з використанням існуючих методик. На ІІ етапі встановлюють закони ураження − опору елементів ризику впливів, під якими розуміють залежності ймовірності ураження від інтенсивності прояву вражаючих факторів, застосовуючи для їх формалізації ті чи інші функції, відповідні даній надзвичайній ситуації. На ІІІ етапі прогнозування дається оцінка наслідків сполучення моделей впливу і законів ураження (руйнування/пошкодження). Використовуючи цей методологічний підхід, оцінюються наслідки майже всіх стихійних лих та техногенних аварій для прийняття рішень щодо організації екстреної евакуації населення з

районів надзвичайних ситуацій та його життєдіяльність у безпечних районах, залучення сил та засобів Державної служби України з надзвичайних ситуацій різного рівня для ліквідації надзвичайної ситуації. Вплив факторів впливу на об’єкти критичної інфраструктури та людей при аваріях та катастрофах з можливими наслідками описано за допомогою моделей. Моделі впливу − це залежність, що визначають розміри потенційної небезпеки (негативного впливу), а також розподіл інтенсивності вражаючих факторів. При цьому потенційну небезпеку можна описати у вигляді аналітичних, табличних або графічних залежностей» [17].

Параметри факторів які спричиняють кризову ситуацію для об’єктів критичної інфраструктури залежать від видів надзвичайних ситуацій, тобто від типів небезпечних процесів, що призводять до наслідків, які розрізняються як масштабами, так і видом.

Передумовою конкретизації та визначення необхідних заходів захисту об’єктів критичної інфраструктури є постійна співпраця між державою та інфраструктурними організаціями. В такій ситуації держава залишається гарантом внутрішньої безпеки та виступає посередником в рамках інформаційно-комунікаційних процесів. З іншого боку інфраструктурні організації, як правило, лише вони здатні вживати ефективні заходи захисту, оскільки володіють найповнішою інформацією щодо даної кризової ситуації та мають найбільше можливих елементів вирішення цієї проблеми (як технічно так і фахово). З огляду на це, перед відповідними структурами, що керують процесом управління в кризових ситуаціях стоять завдання та певні зобов’язання щодо прийняття конкретних заходів усунення наслідків від дії даної кризової ситуації. Також, як доповнюють українські та міжнародні експерти та науковці, які ретельно описують таку ситуацію, перед цими органами стоїть завдання створення системи контролю, наприклад, «системи ризик-менеджменту, що дозволяють на ранній стадії помітити тенденції і факти, що представляють собою загрозу для подальшого існування суспільства» [58; 79; 122].

До таких кризових ситуацій відносять ризиковані операції та порушеннями положень нормативно-правових актів, що призводять до них, загрози стихійних лих чи терактів тощо. Всі вони можуть суттєво вплинути на подальше існування підприємства, організації, цілої мережі організацій, секторів економіки та країн в цілому.

З іншого боку, слід детальніше розібратися із описом необхідних критичних заходів щодо захисту інфраструктурних об'єктів, які належать перш за все до категорії критичних. Найперше, слід розуміти про відповідальність інфраструктурних організацій, які повинні захищати свої об'єкти від потенційних загроз та приймати необхідні заходи. Ці «обов'язки» інфраструктурних організацій в різних країнах по різному прописані – в деяких наприклад, частково закріплені законодавчо (загальні обов'язки інфраструктурних організацій або ж, відповідно, специфічні обов'язки). В інших країнах це можуть бути елементи загальних заходів захисту власних підприємницьких інтересів та як правило відображені в принципах управління власною структурою. Про це пишуть Д. Бобро та О. Єрменчук [17; 42].

Заходи щодо припинення несанкціонованих дій з боку сторонніх осіб – сьогодні є невід'ємною частиною захисту об'єктів критичної інфраструктури, особливо коли ми згадуємо про інформаційну підтримку діяльності цих об'єктів або ж кібербезпеку підприємства в цілому. Правда часто такі ситуації відбувають як внаслідок навмисних дій, так і через певні стихійні явища чи аварії на підприємствах (вибухи, природні стихійні явища, витік небезпечних речовин тощо) [38].

Головним завданням розробки концепції основних заходів захисту об'єктів критичної інфраструктури сьогодні все ж є захист життя людини за рахунок зниження рівня вразливості критичних елементів інфраструктури стосовно природних явищ, подій, спричинених технічними поломками або людськими прорахунками, а також зменшення рівня вразливості до актів тероризму чи злочинів. Вдало про це пише О. Запорожець, яка підсумовує

свою думку наступним чином «Концепція основних заходів захисту повинна враховувати стандартизовані будівельні, організаційні, кадрові та технічні заходи безпеки» [55; 57; 88].

Дослідники питань сфери критичної інфраструктури спільно приходять до висновку, що, як пишуть С. Домбровська, Н. Нижник та В. Олуйка, «Діюча система національної та регіональної безпеки, перш за все, у природно-техногенній, екологічній, військовій сферах недостатньо ефективно вирішує проблеми захисту життєво важливих інтересів особистості, суспільства та держави, оскільки вона не є цілісною, достатньою, раціонально організованою та ефективно керованою» [32; 39].

Крім того, як доповнює М. Домарацький, «Цей компонент системи забезпечення національної безпеки працює в основному на оперативній основі. По суті, всі органи, що забезпечують національну безпеку, працюють в одному режимі реагування» [38].

Науковці приходять до певного розуміння та відповідного тлумачення поняття «раціональна структура системи громадської безпеки», що в першу чергу базується на таких поняттях як «регіональна безпека» «критично важливі об’єкти» тощо. А це в свою чергу допомагає визначити елементи захисту критично важливих об’єктів України в надзвичайних ситуаціях та терористичних актах. Слід мати на увазі, що раціональність досягається за рахунок системи функціонування всіх задіяних в даному процесі складових державного механізму реагування на такого роду кризові ситуації. А це підтверджує думку, що «Функціонування окремих компонентів регіональної системи безпеки є найважливішою частиною методології національної безпеки» [38].

У різній літературі з формування та функціонування системи національної безпеки детально описано даний процес, причому фахівці вказують на можливість використання для аналізу питань національної безпеки в контексті захисту об’єктів критичної інфраструктури різних наукових підходів, щоправда найчастіше використовуються методи теорії

прийняття рішень або ж теорії організації державних органів. На це звертає увагу Сунгуровський М. у своїй роботі «Методологічний підхід до формування системи національної безпеки України» [131].

Як основа, для процесу прийняття та реалізації рішень у сфері забезпечення національної безпеки в нашій країні залишаються Конституція України та велика кількість нормативно-правових актів, зокрема [47; 48; 49; 50; 52; 53; 51; 54].

У процесі державного управління об’єктами критичної інфраструктури, як зазначає в своїй роботі Б. Бобро [17] та О. Мельниченко [84] слід виділяти «два рівні, дві ієрархічно пов’язані складові», кожна з яких має свій зміст. Зокрема, перший рівень (перша складова управління) включає «управлінську діяльність аналітичного, науково-прогностичного й організаційного характеру. Її результатом, насамперед, є визначення стратегій управління зовнішніми, наприклад, техногенними впливами, а також організація механізму їх реалізації з урахуванням соціальних, економічних та інших факторів» [17; 84]. А другий рівень процесу ДСЗКІ стосується організаційно-технічних систем. На думку авторів, основними елементами системи управління на цьому рівні стають: «функціональний контур і інформаційні технології, методи та засоби підготовки та прийняття управлінських рішень, методичний апарат аналізу й оцінки ризику з урахуванням соціальних, економічних та інших аспектів» [17; 84].

Формування системи державного управління процесом захисту критичних об’єктів тісно пов’язані з виробленням основних напрямів регіональної політики органів місцевого самоврядування у сфері забезпечення критично важливих об’єктів України в надзвичайних ситуаціях та терористичних актах. Вироблення такої регіональної політики носить собою багаторівневий процес, який повинен враховувати велику кількість різних як природніх явищ так і інших факторів, що можуть суттєво вплинути на загальну систему управління цим процесом. На цьому зокрема наголошують В. Могильченко [56] та В. Вакуленко [19].

За останні роки з’явилося ряд робіт українських дослідників питань формування системи забезпечення безпеки населення та захисту критично важливих об’єктів України при надзвичайних ситуаціях та терористичних актах. Всі вони, узагальнивши попередні роботи з цих проблем, стверджують, що ДСЗКІ підпорядкована дії великого і тісно пов’язаних між собою кола закономірностей. Їх вони (М. Домарацький, С. Домбровська та С. Бєлай) об’єднують в дві великі групи – соціально-економічного і організаційного характеру будівництва системи [38; 39].

Так, група соціально-економічного характеру «…відображає зв’язок формування системи забезпечення безпеки населення та захисту критично важливих об’єктів України в надзвичайних ситуаціях та терористичних актах із зовнішніми та внутрішніми умовами розвитку суспільства та держави» [12]. На думку, найважливішими закономірностями в цій групі є «відповідність організації системи рівню розвитку України, її економічному потенціалу, відповідність напрямів формування системи реальних небезпек особистості, суспільства та держави в економічній, соціальній, екологічній, природній та техногенній сферах, а також цілям державної політики сталого розвитку та єдність інтересів усіх груп населення щодо захисту від надзвичайних ситуацій» [56].

Щодо групи закономірностей організаційного характеру, як вказує В. Могильченко, то її особливостями формування системи заходів по захисту населення та об’єктів критичної інфраструктури стає «пряма залежність ефективності функціонування системи від рівня розвитку економічних та правових механізмів діяльності стосовно забезпечення безпеки населення та захисту критично важливих об’єктів України в надзвичайних ситуаціях та терористичних актах, залежність організаційної структури сил системи від завдань, що вирішуються, та рівня їх технічного оснащення, залежність ефективності управління заходами щодо попередження та ліквідації надзвичайних ситуацій від організації системи на всіх рівнях та відповідність організації, складу сил та засобів, фінансових та матеріальних ресурсів

ступеня небезпеки та наслідкам аварій, катастроф та стихійних лих, а також небезпеки терористичних актів» [56].

За останні роки Україна значно змінила свій підхід до вирішення питання державної системи захисту об’єктів критичної інфраструктури. Було прийнято відповідне законодавство щодо регулювання та управління процесом забезпечення захисту критичної інфраструктури. Основні організаційні функції з даних питань покладено на Державну службу України з надзвичайних ситуацій. Серед великої кількості контролюючих та організаційних функцій ДСНС України веде реєстр критично важливих об’єктів, проводить моніторинг ситуації на них та за діяльністю державних органів виконавчої влади та місцевого самоврядування [80; 98].

Також ДСНС України постійно моніторить так звані «потенційно небезпечні об’єкти», які попадають під контроль готовності до запобігання та ліквідації надзвичайних ситуацій. Така оцінка проводитися з урахуванням класу небезпеки об’єкта (частота проведення, методи перевірки, ліцензовані фахівці відповідної категорії).

Для зручності ведення моніторингу ситуації за станом державного забезпечення системи захисту об’єктів критичної інфраструктури в Україні здійснюється паспортизація територій та небезпечних об’єктів, що стало основою для обліку та контролю над територіями та небезпечними об’єктами для запобігання та ліквідації надзвичайних ситуацій. Від повноти та правильності заповнення таких паспортів, як зазначає М. Домарацький, залежить оперативність реагування державою та приватним сектором на можливі виклики спричинені техногенною катастрофою чи іншими загрозами щодо захисту КІ [38].

Окремо, для формування в Україні державної системи захисту об’єктів критичної інфраструктури, встановлюються технічні регламенти, які визначають вимоги до об’єктів технічного регулювання на цьому наголошує в іншій своїй роботі М. Домарацький [36]

Основною метою всіх заходів та методів для захисту критично

важливих об’єктів насамперед є запобігання надзвичайним ситуаціям. Тому, в першу чергу проводяться заходи фізичного захисту від зовнішніх і внутрішніх впливів на ці об’єкти.

Таким чином, якщо підсумувати, то в Україні основні принципи функціонування державної системи захисту критичної інфраструктури наступні: «захист населення та територій від надзвичайних ситуацій природного та техногенного характеру; проведення науково-дослідних та дослідно-конструкторських робіт з виявлення закономірностей виникнення надзвичайних ситуацій природного та техногенного характеру, залежності рівнів ризику та зменшення збитків від дій органів виконавчої влади, керівників підприємств та організацій усіх форм власності; створення регіональної системи виявлення, оцінки, прогнозування та моніторингу надзвичайних ситуацій природного характеру та техногенних ситуацій; підвищення ефективності заходів щодо ліквідації надзвичайних ситуацій природного та техногенного характеру, терористичних актів; підвищення рівня підготовки населення та фахівців територіальної підсистеми ДСНС України до дій щодо запобігання та ліквідації надзвичайних ситуацій; розробка та застосування економічних механізмів управління безпекою (ліцензування, декларування, страхування, визначення пільг та диференційованих ставок платежів тощо) на потенційно небезпечних об’єктах та регулювання їх діяльності для вирішення питань безпеки; впровадження компенсаційних заходів (відшкодування збитків за рахунок виплат за страховими полісами з благодійних, стабілізаційних і ін. спеціальних фондів, державна допомога) при виникненні надзвичайних ситуацій; прийняття та впровадження регіональних цільових програм у сфері забезпечення безпеки, запобігання та ліквідації надзвичайних ситуацій; управління безпекою на основі узгодженої діяльності органів державної влади на загальнодержавному, регіональному та промисловому рівнях. [80; 84].

Як бачимо, формування системи забезпечення безпеки об’єктів критичної інфраструктури в Україні підпорядковане дії різного ола закономірностей. Доцільно поєднувати їх, поділивши попередньо на дві великі групи, які відображають соціально-економічний та організаційний характер формування системи.

2.2. Досвід зарубіжних країн стосовно державного управління забезпеченням безпеки об’єктів критичної інфраструктури

Зважаючи на тему дослідження та проблеми, які нам варто вирішити в питанні захисту об’єктів критичної інфраструктури, досить важливим є питання вивчення міжнародного досвіду ДСЗКІ. Це стало більш важливим останніми роками, коли у світі періодично з’являються кризові ситуації та періодично повторюють інформаційні атаки на об’єкти КІ [13; 105].

Однією з провідних країн світу сьогодні у боротьбі з інформаційним загрозами залишається США. Терористичні акти, а особливо 2011 р., на американців спонукали їх до активного пошуку нових підходів в організації державного управління системою захисту різних сфер суспільного життя, зокрема і критичної інфраструктури. Тому, ще в 2003 р. було оголошено про створення Єдиної національної системи управління в умовах надзвичайних ситуацій. На думку багатьох науковців такий підхід дозволив значно змінити комплекс організаційних заходів у цьому напрямку а це в свою чергу мало позитивний ефект для всієї країни загалом [38].

З огляду на це, за каденції останніх Президентів США (особливо Обами, Трампа та Байдена) проводиться активна політика запобігання терористичних актів., основою якої стали скоординовані дії загальнонаціонального масштабу. Такі речі було запроваджено ще в період Президента Джорджа Буша молодшого. Насамперед варто згадати про проведення ще в далекому 1997 р. спільно Міністерством енергетики країни та ЦРУ масштабних заходів протидії «екстремістських акцій», як їх тоді називали.

Ю. Лермонтова у своєму дослідження згадує передумови появи в США наприкінці 90-х рр. XX ст. системи захисту країни від різного роду атак на об'єкти критичної інфраструктури. Для цього в країні постійно велася різнопланова робота, основні зусилля якої було спрямовано на напрацювання механізмів взаємодії різних державних структур у запобіганні, виявленні та знешкодженні можливих таких атак на об'єкти критичної інфраструктури країни. Автор наводить перелік недоліків-проблем, що проявилися під час проведення однієї з імітаційних газових атак в метро Нью-Йорка у 1995 р. Серед них Ю. Лермонтова вказує наступні: «…відсутність чіткої координації між організаціями, які брали участь у боротьбі з технологічним тероризмом, роз'єднаність зусиль, боротьба між різними структурами за фінансування, швидке витрачання наявних запасів вакцин, антибіотиків, антидотів, дезінфектантів та інших витратних матеріалів, брак спеціально підготовлених і імунізованих фахівців, у тому числі з числа правоохоронних органів для оперативного відправлення в інфіковану місцевість, відсутність практичного досвіду поводження з ізольованими людьми, які зазнали впливу вражаючих факторів, неефективність існуючих профілактичних заходів щодо запобігання виникнення та нейтралізації паніки серед населення» [71, с. 192-195].

З метою запобігання таких та подібних ситуацій в США було видано Президентом країни в 1998 р. дві керівні Директиви PDD 62 «Боротьба з тероризмом» і PDD 63 «Захист критичних інфраструктур», основну увагу в яких було зосереджено на швидкому реагуванні на можливі виклики внаслідок терористичних атак, їх протидії, рятувальних діях різних органів та служб, захист населення, пом'якшення негативних наслідків від такого роду атак, підвищення життєздатності та стійкості функціонування критичної інфраструктури в різних надзвичайних та кризових ситуаціях тощо [9; 13; 76].

Пізніше, у вересні 2001 р., виступаючи перед Конгресом, президент Буш оголосив про необхідність створення нового федерального відомства −

Міністерства внутрішньої безпеки, − яке координувало б роботу багатьох органів (більше 20 федеральних відомств та понад 170 тисяч службовців), що займаються питаннями безпеки. Також було запропоновано значно збільшити фінансування відповідних структур, розширити їх права, перерозподілено завдання та функцій у системі федеральних органів виконавчої влади США у галузі забезпечення внутрішньої безпеки країни, децентралізацію організації кризового управління. Паралельно Конгресом США було прийнято десять законопроектів та резолюцій щодо міжнародних та внутрішніх юридичних аспектів боротьби з тероризмом. Все це було виведено в один закон під назвою «Патріотичний акт», який практично одноголосно був підтриманий обома палатами конгресу [38].

Серед іншого в цьому законі особливе місце було відведено поняттю тероризм та системі притягнення до відповідальності за вчинення терористичних актів. Все це дало значний поштовх до підвищення готовності федеральних та місцевих органів влади, а також приватного сектору реагувати на широкий спектр різних загроз критичній інфраструктурі [9; 141].

В законодавстві США також існує пункт про незалежність штатів, і відповідно права губернатора кожного штату приймати рішення на регіональному рівні, наприклад при виникненні надзвичайної або іншій кризовій ситуації. Згідно із законами кожного штату, губернатор оголошує надзвичайну ситуацію або надзвичайний стан або виданням спеціального указу, або шляхом заяви про це через засоби масової інформації (декларацію). Указ або декларація зазвичай містить опис причин лиха, його розташування всередині штату і повноважень, згідно з яким губернатор оголошує надзвичайну ситуацію (надзвичайний стан) [38]. Група науковців на чолі з В.Н. Цигічко вказує на наступні надзвичайні права губернатора штату у надзвичайних ситуаціях «Необхідність використання Національної гвардії, посилення правового захисту та отримання додаткового

фінансування – три основні причини, щоб губернатор оголосив надзвичайну ситуацію (надзвичайний стан)» [105; 141].

З іншого боку, як зазначають дослідники «У деяких штатах губернаторські декларації про надзвичайні ситуації (надзвичайний стан) можуть бути необхідним кроком для надання державних коштів місцевим органам влади. Ця потреба може бути логічним обґрунтуванням для оголошення надзвичайної ситуації, навіть якщо реального реагування на надзвичайні ситуації не потрібно. Це також може забезпечити політичний тиск, необхідний для оголошення надзвичайного стану (надзвичайної ситуації) у ситуації, коли немає інших гарантій для офіційного оголошення такої ситуації» [105, с. 273−280].

У випадку оголошення надзвичайного стану (надзвичайної ситуації) більшість законів штату дозволяють губернатору делегувати спеціальні повноваження та обов’язки керівнику органу управління кризових ситуацій або відповідному міністру уряду штату [38].

Сучасні умови в Україні, процес реформування країни як на національному, так і на регіональному рівнях потребують необхідності пошуку оптимальної системи громадської безпеки та захисту об’єктів критичної інфраструктури. На цьому наголошує український науковець В.М. Вакуленко [19; 83]. І в цьому випадку, як зазначає автор, особливої уваги заслуговує хід процесу реформування державної влади в Україні найближчим часом.

На окрему, особливу увагу заслуговують у процесі захисту об’єктів критичної інфраструктури питання забезпечення кібербезпеки критичної інфраструктури. І тут нам в нагоді теж стане існуючий досвід в зарубіжних країнах. Як зазначають Бірюков Д. та Бобро Д. «Для кожної конкретної сфери заходи захисту, що застосовуються, повинні відповідати цілям безпеки, часто відмінним від конфіденційності, цілісності або доступності інформаційних ресурсів» [13; 17].

Але, не варто також забувати і про те, що заходи захисту КІ часто

корегуються внаслідок обмеження наявних ресурсів або вимогами функціональної безпеки. Найчастіше це потребує регулювання співпраці фахівців, які беруть активну участь в системі захисту. Найбільш актуальною така співпраця є в ситуації з захистом об'єктів критичної інфраструктури приватних підприємств. Напрошується відповідна кооперація державного та приватного секторів у сфері захисту об'єктів критичної інфраструктури. Про це детально ідеться в роботі В.Л. Бурячка під назвою «Інформаційна та кібербезпека: соціотехнічний аспект» [18; 124].

Дослідники управління кібербезпекою критичної інфраструктури з точки зору взаємодії між державою та приватним сектором на сьогодні визначають три основні типи стратегій, що використовуються процесі управління. І. Костюк в роботі «Україна в фокусі кібератак» вказує на те, що «…вибір тієї чи іншої стратегії визначається спільною розробкою регулюючих та виконавчих органів у галузі національної безпеки, кібербезпеки та безпеки окремих компонентів критичної інфраструктури» [65; 124].

Першим розглянемо централізований підхід управління кібербезпекою критичної інфраструктури. В цьому випадку існує державний орган або департамент в країні, який одноосібно відповідає за забезпечення кібербезпеки критичної інфраструктури. Тоді як інші установи можуть консультувати цей департамент або брати участь у заходах, пов'язаних із забезпеченням кібербезпекою критичної інфраструктури, але не мають вирішального впливу на регулювання цієї діяльності. Для прикладу, такий варіант управління широко використовується в Німеччині, Італії, Чехії, Естонії. Тоді, основну відповідальність за управління несе безпосередньо керівник департаменту, щоправда можуть бути певні виключенні, але вони повинні бути чітко прописані та задокументовані [13; 40; 42].

Так, у Німечиині в Стратегії кібербезпеки йдеться про наступне «Захист найважливіших інформаційних інфраструктур є пріоритетом кібербезпеки. Вони є центральним компонентом майже всіх критичних

інфраструктур і набувають все більшого значення. Громадськість і приватний сектор мають створити удосконалену стратегічну й організаційну основу для більш тісної координації на основі інтенсивного обміну інформацією» [38]. Головним органом у контролі за виконанням положень цієї Стратегії виступає Федеральне управління з питань інформаційної безпеки Німеччини. Щоправда його діяльність теж підконтрольна Федеральному міністерству внутрішніх справ країни. У випадку ж критичної ситуації чи в країні в цілому, чи в одній із земель Німеччини дії всіх органів координує Федеральне відомство з питань інформаційної безпеки [13; 40; 42].

На відміну від Німеччини, в Чехії всім процесом координації дій по захисту об'єктів критичної інфраструктури керує Управління Національної Безпеки. В його функції входить захист від кібератак на об'єкти критичної інфраструктури, управління системою допуску до безпеки об'єктів та керування криптографічним захистом систем. Безпосередньо сам захист об'єктів здійснюється Національним центром кібербезпеки, який є складовим елементом Управління Національної Безпеки. У разі виникнення ситуації, що відноситься до категорії надзвичайного стану, Управління виступає в якості провідного повноважного органу, який координує роботу інших відомств по обробці цього інциденту [13].

В багатьох країнах світу не існує спеціального регулятора у сфері кібербезпеки критичної інфраструктури. Таким прикладом є Латвія. Головним органом в системі із захисту критичної інфраструктури є Інститут реагування на інциденти безпеки інформаційної технології Латвійської Республіки. Проте, разом з ним існують ще і Служба державної безпеки країни, Бюро по захисту Конституції, які також виконують координуючу роль разом з Інститутом реагування на інциденти безпеки інформаційної технології Латвійської Республіки. Вони в межах своїх окремих повноважень, також спільно «…ведуть координацію питань оцінки і управління поточними інформаційними ризиками для критичної інфраструктури» [38].

Також, як зазначає Бурячок В.Л., «Активна співпраця регулятора і національного органу із забезпечення кібербезпеки критичної інфраструктури є показником відкритості регулятора, його обізнаності про короткострокові галузеві потреби у заходах безпеки та готовності будувати відносини з приватним сектором» [18]. Так, згідно із дослідженням профілів кіберблагополуччя Міжнародного союзу електрозв'язку, наведеного в своїй монографії М.Б. Домарацьким, «…з 129 країн, в яких який існує офіційний орган, відповідальний за питання кібербезпеки, 90 мають офіційний департамент з питань кібербезпеки критичної інфраструктури. Для 11 з цих 90 країн він і є цим уповноваженим органом. Якщо розглянути тільки ті країни, які мають офіційно прийняту стратегію або політику кібербезпеки критичної інфраструктури, то їх кількість зменшиться до 64 з 196 країн, для яких описані профілі кіберблагополуччя. Серед цих 64 лише 7 країн не розрізняють спеціалізований і основний орган, відповідальний за питання кібербезпеки критичної інфраструктури» [38].

Проте, така форма організації управління захисту об'єктів критичної інфраструктури має один великий недолік, а саме під час критичних ситуацій спостерігаються проблеми з побудовою відносин з приватним сектором через існування спільних (єдиних для всіх) вимог щодо впровадження до реалізації процедур та заходів незалежно від специфіки конкретної галузі критичної інфраструктури. Як зазначають деякі експерти із кіберзахисту, в такому випадку «Власники приватних об'єктів, класифікованих як критична інфраструктура для забезпечення кібербезпеки, можуть неохоче ділитися інформацією про свої випадки кібербезпеки» [9].

В такій ситуації завжди краще працює (як показав міжнародний досвід) принцип залучення представників певної сфери критичної інфраструктури до розробки заходів захисту критичної інфраструктури. З цією метою у багатьох країнах світу уряди диверсифікують методи захисту критичної інфраструктури шляхом залучення в процес захисту зацікавлених сторін критичної інфраструктури. Так, як пише Д. Бірюков, «Німецький регулятор

Federal Office for Information Security реалізує програму UP Kritis. А вже в рамках цієї програми успішно реалізується співпраця між галузями промисловості і державою на основі взаємної довіри. Вони обмінюються ідеями та досвідом і навчаються одне у одного забезпеченню захисту критичної інфраструктури. Всі сторони діють разом і таким чином знаходять кращі рішення» [13].

Цю думку підтверджує вище наведене дослідження профілів кіберблагополуччя Міжнародного союзу електрозв'язку, наведеного в своїй монографії М.Б. Домарацьким, а саме: «В 51 країні зі 196 реалізована офіційна програма або ініціатива щодо міжвідомчої співпраці з питань кібербезпеки критичної інфраструктури. Також у 51 країні певною мірою було реалізовано програму обміну інформацією, що стосується кібербезпеки критичної інфраструктури між державою та приватним сектором. В обох випадках майже в третині країн ці ініціативи підтримуються спеціальними управліннями захисту критичної інфраструктури. У цьому випадку захист критичної інфраструктури знаходиться в компетенції декількох відділів і груп, що співпрацюють, або міжвідомчого комітету. Ці відомства, що співпрацюють, відіграють роль координуючого органу» [38]. У цьому випадку відповідальність за безпеку критичної інфраструктури лежить на одному відомстві або розподіляється між декількома. Так функціонує система захисту критичної інфраструктури в Австрії, Франції, Польщі, Фінляндії, Австралії, Канаді та багатьох інших країнах.

Як приклад, автор цікавої для нашого дослідження аналітичної записки Д. Бобро наводить Австрію, в якій Федеральна канцелярія Австрії та Федеральне міністерство внутрішніх справ розподіляють відповідальність за захист критичної інфраструктури на стратегічному рівні. Якщо конкретніше, то Бобро вказує на їх роботу наступним чином: «За управління та координацію роботи різних відомств несе відповідальність Група управління кібербезпеки (англ. «Cyber Security Steering Group», CSSG), що складається зі

співробітників зі зв'язків Ради національної безпеки (англ. «National Security Council») і експертів кібербезпеки міністерств, представлених у Раді національної безпеки. На операційному рівні відповідна координуюча структура розділена на «внутрішнє коло» і «зовнішнє коло». Зокрема, внутрішнє коло включає в себе кілька державних установ, найбільш важливими з яких є такі, як Центр кібербезпеки (англ. «Cyber Security Center»), Центр кіберзахисту (англ. «Cyber Defense Center»), GovCERT, MilCERT, Центр компетенції у сфері кіберзлочинності (англ. «Cyber Crime Competence Center», C4). Зовнішнє коло включає в себе приватні організацій та національний департамент, специфічні для сфери критичної інфраструктури» [17].

Схожа ситуація спостерігається і в Франції, де головним органом координації питань захисту найважливіших складових критичної інфраструктури є Генеральний секретаріат з питань оборони і національної безпеки (франц. «Secretariat general de la defense et de la securite nationale», SGDSN). Як описує французькі реалії В. Бурячок «SGDSN є міжвідомчою організацією і знаходиться під керівництвом прем'єр-міністра Франції. Ще одне утворення − ANSSI (франц. «Agence nationale de la securite des systemes d information») − міжвідомче агентство, що перебуває під керівництвом Стратегічного комітету SGDSN. Ці два основні агентства відповідають за всі аспекти захисту критичної інфраструктури. Офіційно у них немає інших форм співпраці з іншими державними установами. ANSSI співпрацює з приватним сектором у 18 різних робочих групах» [18].

В загальному схожою є ситуація і сусідній з Україною Польщі, де головну відповідальність за захист критичної інфраструктури покладається на Центр державної безпеки (RCB), а заходи щодо організації загального процесу управління захистом об'єктів критичної інфраструктури проводяться шляхом співпраці між державними органами та операторами критичної інфраструктури. В Польщі також існує базовий документ, що регламентує питання захисту об'єктів критичної інфраструктури – Стратегія національної

безпеки Республіки Польща, в якій зазначається, що захист критичної інфраструктури є обов'язком операторів та власників, і ця відповідальність підтримується державною та адміністративною спроможністю [38].

Із вище наведених прикладів стає зрозуміло, що цей тип стратегії більше орієнтований на поділ обов'язків, і в деяких випадках на партнерство відповідального за кібербезпеку критичної інфраструктури органу і відомств, обізнаних про особливості конкретних складових критичної інфраструктури. Кожне таке відомство, у свою чергу, несе відповідальність за вибудовування відносин з великими підприємствами регіону, важливими в цьому регіоні [9].

І нарешті останній тип стратегії ведення державної політики щодо захисту об'єктів критичної інфраструктури, в основі якого стоїть принцип дотримання державою «доктрини субсидіарності». Це на практиці означає повну передачу відповідальності за захист власникам та операторам об'єктів критичної інфраструктури. Сьогодні в світі немає великої кількості країн, що сповідують даний принцип ДСЗКІ. Цей підхід реалізується втаких країнах Ірландія та Швейцарія. Так, стратегія кібербезпеки Ірландії декларує наступне: «Внаслідок різних форм власності й експлуатації різних систем інформаційних критичних технологій, держава не може взяти на себе особисту відповідальність за захист кіберпростору і прав громадян в мережі Інтернет. Власники та оператори інформаційно-комунікаційних технологій несуть головну відповідальність за захист своїх систем та інформації про своїх клієнтів» [38]. В Ірландії немає відомства, відповідального за кібербезпеку критичної інфраструктури взагалі. На відміну від Ірландії, як зазначає М.Домарацький у своєму іншому дослідженні, в Швейцарії єдиною державною установою, яка хоча б якось може контролювати та регламентувати процес захисту об'єктів критичної інфраструктури є Центр обліку та аналізу захисту інформації є національним інформаційним центром для обміну даними про загрози та інциденти між приватним та державним секторами [36, с. 91-92]. Автор також говорить про те, що «…заснований на саморегуляції принцип, ідеально відповідає різноманітності потреб

критичної інфраструктури, але неможливо уникнути інцидентів кібербезпеки, багато з яких матимуть серйозні наслідки, якщо критична інфраструктура буде пошкоджена» [36, с. 92]. Тому, підсумовуючи, можна сказати, що метод управління кібербезпекою критичної інфраструктури, який залучує до відповідних процесів кілька компетентних сторін за участю координуючого органу, виглядає оптимальним на сьогодні принципом. Однак, як стверджують українські та закордонні науковці, «На практиці не завжди вдається уникнути ані жорсткості авторитарного підходу, ані неузгодженості розвитку, властивого саморегулюванню» [9].

Щоправда, дехто х науковців вражає за доцільне говорити про проміжний підхід, що передбачає часткову передачу відповідальності зацікавленим сторонам критичної інфраструктури, зокрема власникам або операторам критичних інфраструктурних систем. В такому випадку, державний контроль здійснюється лише стосовно найважливіших підприємств та організацій. Частково такий підхід використовується французький регулятор ANSSI. В такому випадку, вважає Д. Бірюков, «Безпека при такому підході частково регулюється запитами ринку. Недолік полягає в первісній відсутності мотивації невеликих і середніх компаній піклуватися про кібербезпеку, принаймні, до першого серйозного інциденту» [13]. Наприклад, як описує даний процес С.О. Гнатюк, «Поки-що практика планомірного кіберзахисту промислових підприємств, об’єктів водопостачання та енергетики не надто поширена, хоча подібні підприємства та об’єкти повною мірою використовують інформаційні і комунікаційні технології, включаючи Інтернет, в організації своїх ключових процесів» [23].

Оскільки інформований вибір стратегії управління кібербезпекою критичної інфраструктури можливий лише для тих держав, які знаходяться в самому початку цього шляху, то можна з впевненістю говорити про сталу систему керування процесом ДСЗКІ у переважній більшості розвинених країн світу. Так, згідно з даними Міжнародного союзу електрозв’язку,

офіційний департамент із захисту критичної інфраструктури так чи інакше працює в більшості країн світу [38].

2.3. Формування державної системи захисту об'єктів критичної інфраструктури в Україні

Формування державної системи захисту критичної інфраструктури (ДСЗКІ) є першочерговим завданням держави з огляду на ті виклики, що сьогодні стоять перед Україною. Такий процес вимагає формування чіткої системи ДСЗКІ, що дозволяє виробити найбільш ефективну модель функціонування системи. Від успішності його розв'язання, у подальшому багато в чому залежатиме характер інтеграції політики у сфері національної безпеки. Тому, на думку деяких авторів, сьогодні в Україні сформувалися наступні пріоритети з питань захисту критичної інфраструктури, а саме необхідність формування єдиної державної політики у сфері захисту критично важливих об'єктів та інфраструктури в Україні [14, с. 2], необхідність імплементації в Україні кращих світових практик в галузі захисту критичної інфраструктури, щодо забезпечення стійкості, адекватної сучасним викликам і загрозам [150], забезпечення координації дій, взаємодії та обміну інформацією при створенні державної системи захисту критичної інфраструктури [62] тощо.

Сьогодні, з'явилося багато досліджень з питань формування ДСЗКІ, але, все ж залишаються слабо описаними питання щодо принципів формування ДСЗКІ.

Варто в першу чергу слід зазначити, що в наукових колах фахівців, що займаються даними питаннями існує ряд різних теорій, щодо принципів реалізації функціонування ДСЗКІ.

Найбільш часто, в таких роботах мова йде про те, що діяльність у сфері державного управління, в тому числі і діяльність в сфері захисту об'єктів критичної інфраструктури, має базуватися саме на принципах. В першу чергу варто правильно вибудувати державну політику у сфері ЗКІ, а це часто не йде

в унісон з принципами забезпечення безпеки та стійкості критичної інфраструктури в нашій країні [95]. З іншого боку, принципи формування ДСЗКІ не обов'язково збігаються з принципами функціонування даної системи [14]. Тому науковці, юристи, та фахівці із інформаційної безпеки наполегливо відстоюють думку, щодо потреби удосконалення формування ДСЗКІ.

Тут варто згадати монографію О.П. Єрменчука [43], в якій згадуються такі принципи, як співпраця з громадянським суспільством, здійснення державно-приватного партнерства у сфері захисту критичної інфраструктури, індикативні керівні принципи для підготовки планів, принципи побудови системи захисту критичної інфраструктури.

А Д.С. Бірюков [14] у своїй роботі віддає перевагу іншим принципам, зокрема планування безпеки, залишковому принципу, принципу групування, принципам ідентифікації критичної інфраструктури, європейським принципам.

На нашу думку, все ж найбільш детально принципи ДСЗКІ розписані в колективній роботі «Developing The Critical Infrastructure Protection System in Ukraine» за загальною редакцією О.М. Суходолі, в якій науковці виділяють зокрема і основні принципи формування політики захисту критичної інфраструктури [150], до яких вони також включили принципи координованості, методологічної єдності, державно-приватного партнерства, конфіденційності, міжнародної співпраці, принципи економічних відносин та їх змін, загальні принципи захисту критичної інфраструктури, принципи державної політики у сфері захисту критичної інфраструктури, фундаментальні принципи роботи, принципи взаємодії та співробітництва органів державної влади, приватного бізнесу, суспільства та держави, принципи функціонування державної системи, широко визнані принципи процесу планування, узгоджені принципи управління для різних етапів кризи, правові, організаційні, фінансово-економічні принципи, принципи законодавства ЄС. Як бачимо, досить детальний та вичерпний перелік, який

дозволяє дослідникам даної теми зважено та ґрунтовно підходити до вивчення проблем удосконалення формування ДСЗКІ.

Щоправда, навіть самі дослідники на чолі з О.М. Суходолі, вказують на те, що їх перелік є доповненням принципів, що згадувалися в роботі 2012 р. іншої групи українських науковців під назвою «Зелена книга з питань захисту критичної інфраструктури в Україні» [57]. В ній теж мова йде про схожі принципи координованості, єдності методологічних засад, державно-приватного партнерства, забезпечення конфіденційності, міжнародного співробітництва.

Науковці, на чолі з тим же О.М. Суходолі, зважаючи на динаміку та розвиток інформаційної сфери, доповнили своє дослідження новими розробками і видали іншу монографію [95], в якій вони змінили підхід до розгляду принципів, і побудували аналіз удосконалення формування ДСЗКІ вже на базі таких принципів, як «…принципи та вимоги щодо співпраці із країнами партнерами винятково крізь призму посилення стійкості цих партнерів, принципи формування стійкості суспільства, принципи готовності та управління в кризових ситуаціях на урядовому, регіональному та муніципальному рівнях, організаційні принципи, національні керівні принципи для забезпечення готовності, принципи розбудови стійкості місцевих громад та компаній, принципи інформаційного обміну» [95].

Окремо варто звернути увагу на дану проблему в контексті загальноукраїнського рівня. Основою для цього стане Концепції створення державної системи захисту критичної інфраструктури, в якій говориться наступне: «створення державної системи захисту критичної інфраструктури потребує нормативно-правового врегулювання основоположних принципів її функціонування». Цю думку підтверджено також і в проекті Закону України «Про критичну інфраструктуру та її захист», де визначено принципи функціонування ДСЗКІ, а саме мова йде про [95, с. 210]: координованість, єдність методологічних засад захисту критичної інфраструктури, державно-

приватну взаємодію, забезпечення конфіденційності, міжнародне співробітництво.

Слід також розглянути класифікацію принципів, визначених у іншому нормативному документі, а саме «Концепції створення державної системи захисту критичної інфраструктури». Дана Концепція була розроблена та затверджена Розпорядженням Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р [120]. Зокрема, в ній встановлено групу принципів, на яких базується досягнення мети самої Концепції. До них віднесено такі пункти як [120]:

«1) взаємодію суб'єктів державної системи захисту критичної інфраструктури;

2) підвищення рівня власних спроможностей громадян, суб'єктів господарювання, установ та організацій, уразливих до припинення або погіршення функціонування критичної інфраструктури;

3) будівництво та експлуатацію об'єктів критичної інфраструктури з дотриманням вимог (інженерно-технічних, організаційних, експлуатаційних тощо) стосовно їх стійкого функціонування у різних режимах функціонування критичної інфраструктури;

4) обмін інформацією між суб'єктами державної системи захисту критичної інфраструктури про загрози критичній інфраструктурі;

5) здійснення державно-приватного партнерства у сфері захисту критичної інфраструктури;

6) сприяння міжнародному співробітництву у сфері захисту критичної інфраструктури з урахуванням глобальних та регіональних безпекових процесів;

7) розроблення та удосконалення законодавства у сфері захисту критичної інфраструктури з урахуванням норм і стандартів НАТО, а також положень річних національних програм під егідою Комісії Україна-НАТО на відповідні роки».

Спробуємо дещо детальніше проаналізувати деякі з пунктів зазначених в Концепції принципів. Це дасть нам можливість краще усвідомити механізм сучасного формування державної системи захисту критичної інфраструктури в Україні.

По-перше, взаємодія суб'єктів державної системи захисту критичної інфраструктури. Тут перш за все мова йде про те, що «створення ДСЗКІ має відбуватись синхронно із розвитком правової та безпекової політики держави, а також з урахуванням рівня спроможностей складових сектору безпеки і оборони держави» [134]. Саме такий підхід, на думку автора роботи «…сприятиме формуванню сприятливих умов для всебічного розвитку інтересів особи, суспільства і держави. При цьому, на це і спрямована діяльність ДСЗКІ. Відтак, необхідність на концептуально нових підходах здійснювати перегляд усієї системи публічного управління, зумовлює потребу і в застосуванні нових підходів до створення ДСЗКІ, оскільки архітектура даної системи має створити умови, за яких відбуватиметься узгодження дій суб'єктів, які будуть виконувати різні функції і ролі та розуміти, яким чином досягати визначених цілей у сфері ЗКІ» [134].

Більш детально дані процеси у своїй роботі описали В.А. Ліпкан та О.В. Кушнір. Вони у своїй монографії роблять розгорнутий науковий аналіз цієї категорії з позицій теоретико-методологічних основ [75]. Автори детально описують принцип взаємодії як «відображення взаємозв'язків між різними об'єктами, для характеристики форм людського буття, людської діяльності й пізнання» [75]. Це дещо виходить за рамки самого поняття «взаємодія», яке описано у Великому тлумачному словнику сучасної української мови, де цей термін характеризується як «взаємний зв'язок між предметами в дії а також погоджена дія між ким-, чим-небудь» [20, с. 125].

З огляду на це тлумачення та відсутність в Україні спеціального закону про ЗКІ виникають певні складнощі, пов'язані із окремими нормативними положеннями, а це в свою чергу, як зазначає Теленик С.С. у своїй роботі

[134] «…інколи призводять до дублювання функцій та повноважень тих чи інших суб'єктів, які на сьогодні залучені до діяльності у сфері ЗКІ».

Для кращого розуміння процесу, варто згадати про дослідження Національного інституту стратегічних досліджень, який у своїй аналітичній доповіді за назвою «Про забезпечення координації дій, взаємодії та обміну інформацією при створенні державної системи захисту критичної інфраструктури» вказує наступне: «Наявні механізми та процедури взаємодії за умов, коли окреме міністерство (відомство) має забезпечувати реагування на «свій» набір загроз та небезпек і несе відповідальність за функціонування «своєї» системи безпеки (кризового реагування), не дозволяють досягти рівня координації дій, взаємодії та обміну інформацією, адекватного цілям та завданням захисту національної КІ» [62, с. 5-6].

По-друге, щодо пункту про підвищення рівня власних спроможностей громадян, суб'єктів господарювання, установ та організацій, уразливих до припинення або погіршення функціонування критичної інфраструктури. Цей принцип за своїм призначенням вказує на те, що держава не може і не повинна брати на себе абсолютно всю відповідальність за функціонування ДСЗКІ. Як аргумент щодо цього варто навести приклади провідних державах світу, які вже створили відповідні системи захисту критичної інфраструктури, громадяни та представники приватного сектору є повноправними учасниками процесу забезпечення захисту критичної інфраструктури [134]. Але, як вказує Теленик С.С. у своїй роботі, «…для впровадження зазначеного принципу слід спочатку визначитися, що саме має стати сферою самозабезпечення й самозахисту, а що діє за принципами субсидіарності» [134]. Відповідно найперше що слід зробити, як вважають експерти, якомога більшу кількість громадян та громадських організацій постаратися залучити до забезпечення стійкості КІ. Правда, постійно варто пам'ятати про вимоги Закону України «Про державну таємницю» щоб не попасти в ситуацію витоку секретної інформації про об'єкти критичної інфраструктури країни.

По-третє, будівництво та експлуатація об’єктів критичної інфраструктури з дотриманням вимог (інженерно-технічних, організаційних, експлуатаційних тощо) стосовно їх стійкого функціонування у різних режимах. Фахівці з даних питань вважають цей принцип одним із основних, ну і відповідно одним із найскладнішим щодо реалізації. Це спричинено тим, що існують певні перепони, які суттєво можуть завадити дотриманню основних норм даного принципу. В першу чергу це фактор морального устарівання та зношення об’єктів КІ. Як приклад фахівці, зокрема і С. Теленик, говорять, що «Більшість із зазначених об’єктів були побудовані за часів СРСР, коли діяли абсолютно інші стандарти, а також були кардинально інші уявлення про можливі загрози таким об’єктам» [134]. Він також нагадав і про розкиданість виробничих елементів в Радянському Союзі, що не дозволяло прив’язувати певну галузь до регіону чи конкретної республіки, наприклад, складові елементи функціонування українських атомних електростанцій в радянський період вироблялися на території сучасної Росії і навпаки в Україні розміщувалися підприємства по виготовленню запчастин для авіації, центром якої все ж варто в радянський період було вважати саме Росію і т.д. і т.п. [15].

Наступне, по-четверте, обмін інформацією між суб’єктами державної системи захисту критичної інфраструктури про загрози критичній інфраструктурі. З одного боку, як говорять дослідники даного питання, цей принцип є складовою першого принципу взаємодії, а його виокремлення в переліку зумовлено важливістю такої діяльності [134]. Сьогодні це питання законодавчо повністю не унормовано через відсутність єдиного координаційного суб’єкта, який сприяв би своєчасному розповсюдженню необхідної інформації та здійснював на її підставі подальшу координацію дій [134]. Десь на допомогу певним чином приходить Закону України «Про державну таємницю», який частково відповідає на питання визначення переліку суб’єктів функціонування ДСЗКІ, які відповідальні за обмін відповідною інформацією. А ще варто згадати про ст. 7 Закону України «Про

режим іноземних інвестицій», в якій встановлено певні обмеження щодо можливості здійснення іноземних інвестицій [107]. Проте, як зазначає С. Теленик, «…в законодавстві відсутні положення, які б системно регулювали питання інвестування в об'єкти КІ, незалежно від виду власності, в якій вони перебувають як єдиний майновий комплекс, а також щодо кола суб'єктів, які можуть виступати бенефіціарними власниками таких об'єктів» [134].

П'яте – здійснення державно-приватного партнерства у сфері захисту критичної інфраструктури. Цей принцип, як і попередній, також перебуває у нерозривному зв'язку із принципом взаємодії, підвищенням рівня власних спроможностей громадян, суб'єктів господарювання, установ та організацій, тобто першим принципом. Він реалізується на базі того підходу, що держава та її органи несуть відповідальність за забезпечення національної безпеки. Гарно даний принцип описав Роберт Кларкат та Сімон Хакім в своїй роботі «Публічно-приватне партнерство: будова, захист і відновлення», в якій вони розглядають «ролі публічно-приватного партнерства у ЗКІ, будови публічно-приватного партнерства, участі приватних агенцій у захисті соціальної інфраструктури, ролі державно-приватного партнерства у дотриманні повітряного контролю як квазі-приватних корпорацій» [154]. Інші науковці Дімітріс Гріцаліс і Джордж Стерджіопулус в своїй праці «Безпека критичної інфраструктури та стійкість» акцентують увагу на «питанні державно-приватного партнерства у сфері кібербезпеки в контексті формування національної системи стійкості» [151]. Окремо варто також нагадати про те, що під час такої співпраці держави та приватного бізнесу не варто забувати про заходи щодо недопущення проникнення представників спеціальних служб іноземних держав і здійснення ними шпіонажу, підготовки терористичних актів; здійснення контррозвідувального, оперативно-розшукового забезпечення діяльності об'єктів КІ тощо. Тобто варто вибудувати такі відносини між бізнесом та державою на взаємовигідних умовах, щоб це дало поштовх до нових можливостей розвитку секторі КІ.

По-шосте – сприяння міжнародному співробітництву у сфері захисту критичної інфраструктури з урахуванням глобальних та регіональних безпекових процесів.

Глобалізаційні процеси відіграють все більш важливу роль у діяльності людини зокрема і функціонування державних інститутів в цілому. Також вони не оминули і впливу на сектор КІ. Міжнародне співробітництво, зокрема у сфері захисту критичної інфраструктури конструктивно вплинуло на галузь. Загрози терористичних актів, дистанційного протиправного втручання в роботу систем і механізмів через мережу Інтернет спричинили зростання масштабів можливих наслідків. Відтак, протистояння подібним загрозам і викликам потребує об'єднання зусиль на міждержавному рівні. Україна намагається сьогодні активно використовувати міжнародну співпрацю у вигляді вивчення досвіду провідних держав світу, консультативної та технічної допомоги міжнародних партнерів, проведення спільних заходів тощо. На допомогу таким прагненням стають міжнародні договори в сфері захисту об'єктів КІ [134]. А найбільш прогресивним досвідом у цій сфері сьогодні являється досвід Європейського Союзу, де у 2004 було висунуто вимогу щодо підготовки загальної стратегії охорони та захисту критичних інфраструктур та ухвалено Повідомлення про охорону та захист критичних інфраструктур в рамках боротьби проти тероризму, в якому було викладено пропозиції щодо можливих заходів Співтовариства щодо попередження, підготованості та реагування на терористичні акти, пов'язані з критичними інфраструктурами [109]. Також, 17 листопада 2005 року Європейською Комісією було ухвалено Зелену книгу з питань європейської програми охорони та захисту критичних інфраструктур, яка визначала декілька можливих варіантів політики щодо створення такої програми та Інформаційної мережі попередження щодо загроз критичній інфраструктурі [109].

Пізніше, 8 грудня 2008 року ЄС також ухвалив Директиву Ради Європейського Союзу 2008/114/ЄС про ідентифікацію і визначення

європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту [109], яка стала першим кроком поступового підходу до ідентифікації і визначення європейських критичних інфраструктур. Тобто, як бачимо вже достатньо давно ЄС активно працює над виробленням нормативно-правової бази у сфері захисту КІ.

Звісно ж, такий підхід необхідно впровадити і в Україні, оскільки це «…дозволить сформувати ефективну систему ДСЗКІ із налагодженням стійких комунікаційних зв'язків між усіма суб'єктами за умови збалансування інтересів кожного із таких суб'єктів для досягнення цілей ЗКІ та обрання найбільш оптимальних моделей та інструментарію захисту» [134]. Окрему роль в даному процесі має відіграти Служба безпеки України, як одного з ключових суб'єктів ДСЗКІ.

Ну і не варто також забувати, що для нашої країни сьогодні міжнародне співробітництво у сфері захисту критичної інфраструктури стало мабуть найбільш необхідним інструментом залучення і коштів і кращих закордонних ідей в сферу захисту об'єктів КІ.

Ну і на кінець, по-сьоме, співробітництво України з Організацією Північноатлантичного договору (НАТО). Його початком стало підписання ще у 1997 р. Хартії [140], а у 2001-му відповідного Указу Президента України. Вже тоді свідомою частиною українського суспільства було визначено ставлення України до НАТО як до «найбільш ефективної структури колективної безпеки у сучасному світі» [31], а недавні події щодо російської агресії проти України цю думку підтвердили повністю.

НАТО, крім військового консультування України, також надає постійну допомогу у вирішення цивільних питань, надзвичайних ситуацій та катастроф, аспектів безпеки у сфері довкілля, включаючи ядерну безпеку, використання космічного та повітряного простору [134]. Ми співпрацюємо останніми роками з НАТО багато і різних сферах, а починаючи від 2011 року щорічно приймаються Річні національні програми співробітництва Україна-НАТО. В цих програмах детально розписані сфери співробітництва між

Україною та НАТО, серед яких і впровадження сучасної, захищеної, стабільної ІТ-інфраструктури, здійснення на системній основі вдосконалення законодавства України, зокрема в частині визначення пріоритетності для інфраструктурних проектів та у сфері безпеки постачань природного газу, функціонування високотехнологічної та ефективної інфраструктури енергопостачання, підвищення рівня професійної компетентності працівників об'єктів критичної інфраструктури та багато іншого.

Отже, кожен з принципів, представлених у «Концепції створення державної системи захисту критичної інфраструктури», є вкрай актуальним і важливим. Вони не суперечать і не дублюють переліку принципів, визначених Європейською Програмою захисту критичної інфраструктури [147], у якій іде мова про такі принципи як субсидіарності, взаємної доповнюваності, конфіденційності, співробітництва із зацікавленими сторонами, співмірності, секторального підходу.

Таким чином, з вище наведеного можна зробити висновок, що сьогодні Україна намагається тримати постійно руку на пульсі щодо питань захисту об'єктів критичної інфраструктури. Це дозволяє нам швидко та ефективно реагувати на нові вив клики, що постійно з'являються в даній сфері, іти в ногу з провідними європейськими стандартами в цій галузі та ставати привабливими для інвестування в КІ.

РОЗДІЛ 3. СТАН АДМІНІСТРАТИВНО-НОРМАТИВНОГО ЗАБЕЗПЕЧЕННЯ ТА ШЛЯХИ УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

3.1. Нормативно-правове забезпечення безпеки об'єктів критичної інфраструктури в Україні

Зважаючи на глобалізаційні процеси у сучасному світі, трансформацію поняття сили у сучасних геополітичних викликах перед державами, вирішення всіх стратегічних питань потребує комплексного підходу, комплексних стратегій. Така ж ситуація спостерігається і в питаннях захисту об'єктів критичної інфраструктури. Комплексність передбачає насамперед використання нормативно-правових заходів щодо запобігання сучасним викликам у сфері ДСЗКІ. На цьому наголошують як українські, так і закордонні дослідники в даній сфері, зокрема [92; 93; 94; 97; 104]. Це спонукає держави до необхідності, перш за все, створення державної системи захисту критичної інфраструктури.

Отже, розуміючи потреби часу, для формування якісного адміністративно-правового регулювання суспільних відносин у сфері захисту критичної інфраструктури доцільно було б перш за все проаналізувати кращі міжнародні зразки регулювання в даній сфері захисту інформації та зрозуміти українські реалії такого процесу. Зокрема, на цьому наголошує автор дисертації з даних питань С. Теленик [134]. Також варто нагадати, що сьогодні в Україні ще не ухвалено відповідного профільного закону, а лише активно формується національна система стійкості, тому цей процес є досить динамічним, і в контексті можливих викликів, може докорінно видозмінитися. Проте базовим документом, що регламентує та формує бачення національної ДСКЗІ, є Концепція створення державної системи захисту критичної інфраструктури затверджена розпорядженням Кабінету Міністрів України від 6 грудня 2017 року № 1009-р. Окрім цього, варто також згадати і про проект Закону України «Про критичну інфраструктуру та

її захист», як одного з базових документів, що регламентує діяльність в цій сфері.

Так, у проекті Закону України «Про критичну інфраструктуру та її захист», зазначено, що «…метою державної політики у сфері захисту критичної інфраструктури є забезпечення безперебійного та стійкого функціонування об'єктів критичної інфраструктури України, запобігання проявам актів несанкціонованого втручання, прогнозування та запобігання кризовим ситуаціям з негативним впливом на об'єкти критичної інфраструктури, а також підвищення рівня захисту, удосконалення заходів безпеки та стійкості цих об'єктів від існуючих загроз» [111].

Сьогодні, в українському науковому середовищі існує чимала кількість дослідження пов'язаних із адміністративно-правовим регулюванням функціонування об'єктів критичної інфраструктури України [125; 143, с. 40-41; 26; 2]. Варто перш-за все варто виділити роботу В.Д. Ткаченко та Є.Б. Ручкіна, які вважають, що « …необхідними умовами існування та гармонійного розвитку будь-якого суспільства є узгодження інтересів різних його членів, встановлення і підтримування у стосунках між ними певного встановленого порядку. Основне навантаження в реалізації зазначених функцій лягає на спеціально пристосовану до особливостей суспільного буття розгалужену систему соціальної регуляції, важливе місце в якій посідає правове регулювання, що в загальному вигляді може бути охарактеризовано, як процес дії за допомогою правових норм та інших юридичних засобів на поведінку людей з метою упорядкування, охорони та розвитку суспільних відносин» [137, с. 404].

Загалом, переважна більшість вітчизняних науковців під правовим регулюванням (у тому числі під адміністративно-правовим регулюванням) розуміють « …сукупність способів та засобів цілеспрямованого правового (у тому числі адміністративно-правового) впливу держави на суспільні відносини, метою якого є упорядкування та урегулювання цих відносин в інтересах людини, суспільства та держави» [134]. При цьому,

адміністративно-правове регулювання, як зауважують наступні науковці [1; 26], це перш за все «…цілеспрямований вплив за допомогою адміністративно-правових засобів на суспільні відносини для забезпечення прав, свобод і публічних законних інтересів фізичних та юридичних осіб, нормального функціонування громадянського суспільства та держави».

Окремо, в літературі зустрічається формулювання та оцінка поняття механізм адміністративно-правового регулювання у сфері захисту критичної інфраструктури. Тут мова йде про те, що він є різновидом механізмому загального правового механізму та спрямований на забезпечення реалізації ДСЗКІ. Наприклад, на цьому наголошує С. Теленик у своїй роботі [134]. Автор, у своїй роботі стверджує, що механізм адміністративно-правового регулювання у сфері ЗКІ «є узгодженою системою адміністративно-правових засобів, метою якої є здійснення упорядкування та унормування суспільних відносин у сфері захисту критичної інфраструки» [134]. При цьому до ознак механізму адміністративно-правового регулювання він відносить «обумовленість метою реалізації державної політики у сфері ЗКІ; реалізація через діяльність суб'єктів у сфері ЗКІ (тобто наявність ефективного механізму АПР у сфері ЗКІ є обов'язковою умовою функціонування ДСЗКІ); виступає системою взаємоузгоджених адміністративно-правових норм, принципів, форм права (актів законодавства), а також форм, за допомогою яких нормативність права переводиться в упорядкованість суспільних відносин, задоволення публічних інтересів суб'єктів ДСЗКІ; встановлюється і забезпечується правопорядок, спрямованість на упорядкування суспільних відносин у сфері ЗКІ; пріоритет національних інтересів тощо» [134].

Зважаючи на світові тенденції, в Україні поступово, як зазначають дослідники даного питання, також запроваджується механізм адміністративно-правового регулювання у сфері захисту критичної інфраструктури. В першу чергу це спостерігається у вигляді послідовних кроків по формуванню та застосуванні адміністративних та правових заходів, за допомогою яких відбувається правове регулювання суспільних відносин у

сфері захисту об’єктів критичної інфраструктури, причому за останні роки все більше уваги приділяється питанням залучення міжнародного капіталу та інституціоналізації державних підприємств [3].

Отже, як бачимо, набуває актуальності процес вивчення механізму адміністративно-правового регулювання у сфері захисту критичної інфраструктури. Для кращого розуміння цього науковці пропонують розглядати його складові. Досить вдало це описав в своєму дослідження С. Теленик, який розглядає наступні складові елементи механізму адміністративно-правового регулювання, а саме: «1) норми права, що регулюють суспільні відносини у сфері ЗКІ – розрізнені чинні норми права, акти галузевого (інституційного) законодавства, які визначають компетенцією окремих суб’єктів щодо реалізації того чи іншого завдання у різних сферах ЗКІ; 2) акти реалізації норм права – процес фактичного втілення правових норм у сфері ЗКІ через безпосередню діяльність суб’єктів захисту критичної інфраструктури; 3) правові відносини – поступово набувають все чіткіших рис вольові суспільні відносини у сфері ЗКІ, що виникають на основі норм права — правові відносини у сфері ЗКІ» [134]. Крім того, він ще і говорить про функціональні складові механізму адміністративно-правового регулювання у сфері ЗКІ « …юридичний факт – конкретні життєві обставини, які зумовлюють виникнення, зміну або припинення адміністративно-правових відносин у сфері ЗКІ; правова свідомість суб’єктів захисту критичної інфраструктури – система відображення правової дійсності у поглядах і почуттях, уявленнях про ефективність права як регулятора суспільних відносин у сфері ЗКІ; акти тлумачення; акти застосування» [134].

Аналогічно , С. Телеником, більшість дослідників говорять про те, що для України зараз важливо закінчити процес прийняття необхідного законодавства в сфері захисту об’єктів критичної інфраструктури, а вже потім переходити до стадії «суб’єктивних прав та юридичних обов’язків із розподілом відповідних повноважень та відповідальності». Одна з таких

робіт це праця В.А. Ліпкана щодо завдань законодавства у сфері національної безпеки України [74; 72], в якій він наголошує на задачах, що можуть бути закладені у законодавство про захист критичної інфраструктури. Серед них, автор виділяє цілу групу проблем, що так і не були вирішені до моменту написання ним своєї роботи, це зокрема: «…концептуалізувати феномен захисту критичної інфраструктури як такий, визначивши його вихідні параметри та характеристики, чинники, що впливають на його розвиток, виділивши потенційні та реальні загрози та небезпеки, а також сформувавши засади для формування ДСЗКІ; актуалізувати проблему створення ДСЗКІ як найбільш ефективного засобу забезпечення національних інтересів у найважливіших сферах інфраструктури; легітимізувати не лише процес забезпечення захисту критичної інфраструктури, але й створення і функціонування самої державної системи ЗКІ, яка має складатися із державної і недержавної підсистем на засадах державно-приватного партнерства; розробити правові засади для створення ДСЗКІ із визначенням органу державної влади, відповідального за координацію дій у сфері захисту критичної інфраструктури; визначити адміністративно-правовий статус суб'єктів захисту критичної інфраструктури; створити систему моніторингу для відстеження ризиків і своєчасної нейтралізації передумов, що створюють загрозу об'єктам критичної інфраструктури; розробити та закріпити чіткі критерії та методологію віднесення об'єктів інфраструктури до критичної інфраструктури, порядку їх паспортизації та категоризації, реєстру та обліку; розробити методологію проведення оцінки загроз та небезпек об'єктам критичної інфраструктури, визначити спеціальний державний правоохоронний орган, відповідальний за проведення аналізу та оцінки загроз критичній інфраструктурі з боку інших держав тощо» [16]. Як бачимо перелік досить великий, причому це далеко не всі пункти, проблемні питання про які говорить автор.

Все ж таки, за роки незалежності нашої держави, Україні вдалося значно просунутися у питанні вирішення проблем захисту об'єктів критичної інфраструктури, зокрема адміністративного регулювання питання. Початком даного процесу стало схвалення Верховною Радою України у 1991 Концепції (основи державної політики) національної безпеки України [63], яка серед іншого регулювала питання суспільних відносин у сфері національної безпеки країни. Після цього в Україні з'явилося чимало праць, в яких дослідники вказували на важливість без пекових питань, зокрема і в сфері захисту об'єктів критичної інфраструктури [7; 11; 64; 67; 69; 73; 144]. Всі вони, і як вже було зазначено вище у роботі, в Україні нажаль не спостерігається поки-що «упорядкованості та етапності у сфері захисту критичної інфраструктури», а це не дозволяє провести необхідні комплексні управлінські дії [134].

Останніми роками, зважаючи на різні фактори, зокрема постійні атаки на об'єкти критичної інфраструктури, в Україні було визначено потребу в розробці та прийнятті окремого нормативно-правового акта під назвою «Концепція створення державної системи захисту критичної інфраструктури», метою якого стало б визначення основних напрямів, механізмів і строків комплексного правового регулювання та створення системи державного управління у сфері захисту критичної інфраструктури. Як зазначає В.А. Ліпкан «Вона становить виключно важливу роль (після Конституції України та щорічних Послань Президента України до Верховної Ради України) у системі нормативно-правових актів, які регулюють суспільні відносини у сфері захисту критичної інфраструктури. А стратегії, доктрини, закони, програми, положення тощо мають розроблятися на виконання даної Концепції» [73, С. 90-91].

Для кращого розуміння існуючої ситуації в сфері ДСЗКІ варто детальніше проаналізувати існуючі в Україні сьогодні нормативно-правові акти у сфері національної безпеки, в яких якраз і розглядаються питання Адміністративного управління безпекою об'єктів критичної інфраструктури

в Україні. Перш за все, це Концепція (основи державної політики) національної безпеки від 1997 року [63], в якій крім всього іншого згадуються сфери, які потребують захисту в інформаційному аспекті. Тут і політична, і економічна, і соціальна, і військова, ну і звісно інформаційна сфери розглядалися. Причому, важливим в тому документі було те, що вже у 1997 р. наголошувалося на необхідність « …розробки і впровадження необхідних засобів та режимів отримання, зберігання, поширення і використання суспільно значущої інформації, створення розвиненої інфраструктури в інформаційній сфері», тобто в даному документі було виділено сфери, в яких мова йшла про появу та необхідність захисту інфраструктуру в інформаційній сфері [63]. Як вважають дослідники, даний документ став базовим, стратегічним у подальшій розробці нормативно-правових актів, які регулюють суспільні відносини у сфері національної безпеки.

Пізніше в Україні було прийнято низку нормативно-правових актів, де зокрема згадувалося про вирішення адміністративного управління питаннями захисту об’єктів КІ. Це Конституція України, Закон України «Про національну безпеку України», послання Президента України [133] тощо. Але наступним елементом історичного прийняття в Україні нормативно-правових актів в ДСЗКІ є звісно ж Закон України «Про основи національної безпеки України» від 19 червня 2003 року [116], яким було скасовано дію аналізованої вище Концепції. В ньому, серед іншого, мова йшла про дещо змінився перелік сфер, в яких мова йшла про захист об’єктів, які відносяться до категорії критичної інфраструктури. Зокрема, це такі сфери як: зовнішньополітична; внутрішньополітична; сфера державної безпеки; економічна; екологічна; науко-технологічна; сфера безпеки державного кордону; інформаційна; соціальна і гуманітарна сфери [116].

В порівнянні із Концепцією 1997 р. зникла політична сфера, натомість замість неї з’явилося дві нові сфери: внутрішньополітична та зовнішньополітична. Також з’явилися ще і сфера державної безпеки та

гуманітарна сфера. Нажаль, як показав досвід та проблеми із нашою сусідкою Російською Федерацією, помилково із переліку було виключено воєнну сферу, що законотворцями аргументувалося як певний елемент демілітаризації нашої країни, а також відсутністю на той момент зовнішніх загроз. І взагалі, як зазначають деякі українські дослідники даного питання, на момент прийняття даного закону в Україні спостерігалася певна деградація Збройних Сил, що також і відобразилося на не включенні воєнної сфери до переліку [134].

Наступним важливим документом в даному питанні є Стратегія національної безпеки України 2015 р. [118]. До актуальних загроз національній безпеці України в ній вже було віднесено: «агресивні дії Росії, що здійснюються для виснаження української економіки і підриву суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території; неефективність системи забезпечення національної безпеки і оборони України; корупція та неефективна система державного управління; економічна криза, виснаження фінансових ресурсів держави, зниження рівня життя населення; загрози енергетичній безпеці; загрози інформаційній безпеці; загрози кібербезпеці і безпеці інформаційних ресурсів; загрози безпеці критичної інфраструктури; загрози екологічній безпеці» [118], тобто, як бачимо, у Стратегії національної безпеки України в 2015 р. вперше при визначенні актуальних загроз національній безпеці було виділено як окрему сферу об’єктів критичної інфраструктури.

Мабуть, ще більш важливим в тексті даної Стратегії було те, що крім перелік актуальних загроз національній безпеці України було виокремлено види інфраструктур, щодо яких існують перераховані загрози. Це: «агресивні дії іноземних держав, що здійснюються для виснаження української економіки і підриву суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території – інституційна, регіональна, місцева та локальна інфраструктура, загроза функціонування ДСЗКІ; неефективність системи забезпечення національної безпеки і оборони

України – недостатня ефективність державної системи захисту критичної інфраструктури; корупція та неефективна система державного управління – інституційна інфраструктура, інфраструктура державного управління; економічна криза, виснаження фінансових ресурсів держави, зниження рівня життя населення – економічна та промислова інфраструктура; загрози енергетичній безпеці – енергетична інфраструктура; загрози інформаційній безпеці – інформаційна інфраструктура, інформаційно-телекомунікаційна; загрози кібербезпеці і безпеці інформаційних ресурсів – кібернетична інфраструктура; загрози безпеці критичної інфраструктури: 1) критична зношеність основних фондів об'єктів інфраструктури України та недостатній рівень їх фізичного захисту; 2) недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій; 3) неефективне управління безпекою критичної інфраструктури і систем життєзабезпечення» [118].

Таким чином, в рамках Стратегії 2015 року визначено та нормативно закріплено суспільні відносини у сфері захисту критичної інфраструктури. Як бачимо, вже в цьому документі вперше в Україні з'являється поняття «захист критичної інфраструктури», її виділено в окремий статус, що дало можливість законодавцям розробити та узгодити з іншими нормами окреме нормативно-правове забезпечення, що стосується захисту критичної інфраструктури як самодостатньої та самостійної сфери. У цій Стратегії також важливо було і те, що в ній виділено не лише окрему сферу об'єктів критичної інфраструктури, але і наведено безпосередні загрози, що їм можуть загрожувати. На це звертають увагу українські та закордонні дослідники даного питання, зокрема С. Теленик [134].

В подальшому в Україні було прийнято Законі України «Про національну безпеку України» від 20.07.2018 р., в якому в пункті 4 статті 3 чітко виділяється такі сфери національної безпеки і оборони, як [112]: «воєнна безпека; зовнішньополітична безпека; державна безпека; економічна безпека; інформаційна безпека; екологічна безпека; кібербезпека тощо».

Дослідники звертають увагу на той факт, що в цьому законі було окремо виділено стратегічні документи, що регулюють вище зазначені суспільні відносини, а саме: «Стратегія національної безпеки України; Стратегія воєнної безпеки України; Стратегія кібербезпеки України; Стратегічний оборонний бюлетень України; Стратегія громадської безпеки та цивільного захисту України; Стратегія розвитку оборонно-промислового комплексу України» [112].

Найновішим документом на сьогодні в Україні з питань врегулювання суспільних відносин в сфері захисту об'єктів критичної інфраструктури є Стратегії національної безпеки України 2020 року, яка була затверджена Указом Президента України. В ній мова зокрема іде і про перелік поточних та прогнозованих загроз національній безпеці та національним інтересам України з урахуванням зовнішньополітичних та внутрішніх умов [119]. А якщо бути точним, то ідеться про наступне: « …посилюються загрози для критичної інфраструктури, пов'язані з погіршенням її технічного стану, відсутністю інвестицій в її оновлення та розвиток, несанкціонованим втручанням у її функціонування, зокрема фізичного і кіберхарактеру, триваючими бойовими діями, а також тимчасовою окупацією частини території України» [119].

Серед іншого, в цьому документі, а точніше в розділі 3 « …до основних напрямів зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки віднесено створення державою ефективної системи безпеки та стійкості критичної інфраструктури, заснованої на чіткому розподілі відповідальності її суб'єктів та державно-приватному партнерстві» [119]. Це одна з перших формулювань в українському законодавстві, де прямо йде мова про створення державою ефективної системи безпеки та стійкості критичної інфраструктури. Водночас, не слід поки говорити про те, що питання державної системи захисту об'єктів критичної інфраструктури вирішено, а швидше цей процес лише розпочато, що все ж дає нам надію на перегляд напрямів і заходів

державної політики в сторону перспектив побудови дієвої моделі захисту об’єктів критичної інфраструктури в нашій державі.

3.2. Адміністративне управління безпекою об’єктів критичної інфраструктури в Україні

У зв’язку з світовими тенденціями останніх десятиліть у сфері ДСЗКІ Україна також почала приділяти значну увагу створенню власної системи захисту об’єктів критичної інфраструктури. Зокрема, було сформовано збірник матеріалів міжнародних експертів під назвою «Зелена книга», в якій висвітлювалися питання захисту критичної інфраструктури у світі [14; 57]. В цій роботі, на використанні міжнародного досвіду робився акцент та заклик до української влади щодо побудови чіткої системи з нормативно-правової та, що більш важливо, адміністративної складової державної системи захисту об’єктів критичної інфраструктури.

Практично, це стало можливим після останньої редакції нового Закону України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII, в яком зокрема багато уваги відведено саме питанням забезпечення захисту об’єктів критичної інфраструктури. Також пізніше, як вже було написано вище в попередньому параграфі, було підготовлено проект Закону «Про критичну інфраструктуру та її захист», який був покликаний забезпечити формування необхідної для цього нормативно-правової бази [50; 121].

Відповідальним за розробку Закону «Про критичну інфраструктуру України та її захист» [121] було Міністерство розвитку економіки, торгівлі та сільського господарства України. В цьому законі прописано пункт, згідно якого забезпечення захисту критичної інфраструктури є складовою забезпечення національної безпеки України.

Якщо ж говорити більш глобально, то в нашій країні передбачено комплексне створення державної системи захисту критичної інфраструктури на базі новітніх підходів до вирішення питань державного управління в цій

галузі, зокрема вироблення сучасних інноваційних підходів до управління ризиками безпеки критичної інфраструктури та оптимізоване застосування наявних ресурсів, гнучке і швидке реагування на інциденти і кризи [35]. Згідно оприлюднених планів, на це завдання відведено період з 2017 по 2027 роки.

Провідною структурою з питань забезпечення захисту об'єктів критичної інфраструктури в Україні є Служба безпеки України, яка серед іншого забезпечує захист економічної безпеки держави виходячи з того, що економічні злочини в сучасних умовах є однією з ключових загроз для об'єктів критичної інфраструктури. Базовим документом, що регламентує її діяльність є Закон України «Про службу безпеки України» 25 березня 1992 року № 2229-XII із останніми змінами і доповненнями. Згідно даного документу Службу безпеки України наділена повноваженнями щодо захисту об'єктів критичної інфраструктури [54]. Щоправда, деякі повноваження Служби безпеки України більш точно (детально) розписані в новому проекті Закону «Про критичну інфраструктуру України». Зокрема мова йде про інструменти впливу на їх діяльність, вектори діяльності СБУ, що дозволять їй більш ефективно захищати об'єкти критичної інфраструктури від різних загроз та викликів [121].

Але ключовим державним органом в Україні щодо управління критичною інфраструктурою є Державна служба України з надзвичайних ситуацій. Серед різноманітних завдань ДСНС України є і такі, що відносяться до питань ДСЗКІ, а саме: «організація та здійснення заходів щодо реагування на надзвичайні ситуації; координація діяльності інших органів державного управління, місцевих органів виконавчої та адміністративної влади у сфері запобігання та ліквідації надзвичайних ситуацій, забезпечення пожежної, виробничої та радіаційної безпеки, цивільної оборони; забезпечення в межах своєї компетенції мобілізаційної готовності органів та підрозділів до надзвичайних ситуацій, виконання завдань у системі територіальної оборони України; розвиток матеріально-

технічної бази та підтримання високої ступені бойової готовності органів та підрозділів з надзвичайних ситуацій та інші» [30; 84].

Керує загальною системою органів і підрозділів з надзвичайних ситуацій безпосередньо Міністр внутрішніх справ, який у тісній співпраці і персональній відповідальності перед Кабінетом Міністрів України виконує завдання, що покладаються на підрозділи ДСНС у випадку надзвичайних ситуацій. Серед величезної кількості функціональних обов'язків Міністр внутрішніх справ також координує роботу підрозділів ДСНС щодо питань захисту об'єктів критичної інфраструктури [68; 87]. Окремо варто сказати про діяльність територіальних органів та підрозділів ДСНС України, які в межах своєї території та відповідно до своїх обов'язків оперативно повинні реагувати на виклики та ризики щодо захисту об'єктів критичної інфраструктури, запобігання, виявлення та припинення терористичної діяльності на об'єктах ДСНС України, а також ліквідації наслідків терористичних актів [56; 82; 145].

На думку багатьох дослідників питань захисту інформаційного простору України, підрозділи ДСНС повинні стати більш важливим елементом захисту ніж вони є сьогодні. Особливо це відноситься до регіональних підрозділів, які повинні миттєво реагувати на нові виклики щодо питань державної системи захисту об'єктів критичної інфраструктури. Відповідно «Формування територіальних органів та підпорядкованих підрозділів ДСНС України стало результатом усвідомлення на державному рівні відповідних завдань управління, незадоволеність станом законності в регіонах України та низьким ступенем ефективності роботи територіальних підрозділів державних органів виконавчої влади» [22; 96]. Також важливим сьогодні в контексті реформи децентралізації (передача значних повноважень на місця) в Україні стає підпорядкованість підрозділів ДСНС України регіональним лідерам (керівнику регіонального відділення, начальнику місцевого МВС, губернатору, голові обласної ради та депутатському складу, мерам міст та ОТГ). Варто згадати і про можливість внесення певних змін у

діяльність відповідних органів місцевими органами влади з метою кращого реагування на сучасні виклики та загрози. Так, зокрема прикордонні регіони, індустріальні регіони є сьогодні більш вразливими в питаннях захисту об'єктів критичної інфраструктури. Головне, щоб в цій ситуації не відбулося певної ситуації не підконтрольності та нерозберихи у вирішенні важливих питань, що потребуватимуть їх швидкого вирішення. На регіональному рівні також сьогодні з'явилася можливість підвищити ефективність державної політики у сфері громадської безпеки та захисту критичних об'єктів у надзвичайних ситуаціях та терористичних актах використовуючи новітні технології та можливості законодавства України. Нажаль, в українських реаліях цей процес передачі повноважень на місця дещо затягнувся в силу різних обставин. Щоправда такий же непростий шлях проходили і інші країни світу, тому, перейнявши кращий досвід міжнародних процесів пере розподілення повноважень органів управління державною системою захисту об'єктів критичної інфраструктури, в Україні також вийде оптимізувати весь процес відповідно до регіональних особливостей [96]. Як вважають дослідники, зокрема М.Б. Домарацький «Є достатньо підстав вважати, що у міру формування системи територіальних органів та підпорядкованих підрозділів ДСНС України ефективність управління «по вертикалі» зростатиме. Представники Президента можуть фактично отримувати статус представників держави в регіонах, вирішуючи при цьому завдання представництва Президента, територіальної державної адміністрації та органів місцевого самоврядування» [35].

З огляду на це, ще одним важливим завданням для побудови чіткої системи державної системи захисту об'єктів критичної інфраструктури є створення зрозумілих та ефективних зв'язків для взаємодії держави і суспільства, інститут Президента та місцевими адміністраціями, мешканцями всіх населених пунктів, суспільства в цілому.

Події останніх років, періодичні хакерські атаки на об'єкти критичної інфраструктури, використання вірусу в своїй діяльності – все це підтверджує

думку багатьох фахівців з питань захисту об’єктів критичної інфраструктури про важливість захисту об’єктів саме щодо кібербезпеки.

Всі фахівці з питань захисту КІ визнають можливість активного використання сучасних інформаційно-комунікаційних технологій для ведення зокрема і терористичних актів, які в першу чергу спрямовані саме на об’єкти критичної інфраструктури [18; 124]. Тут особливе місце відведено об’єктам національної інфраструктури в якості потенційних мішеней. Зважаючи на устарівання таких об’єктів в нашій країні через фізичне зношування та недофінансування державою, що призводить до повної втрати функціональності, може в цілому вплинути на стан національної безпеки і спричинити надзвичайні ситуації певного рівня і масштабу на об’єктах критичної інфраструктури. Щороку в нас в країні ведеться дискусія серед громадян щодо проблем в енергетиці, газовій сфері тощо. Одним із найбільш хвилюючих запитань вже на протязі багатьох років залишаються питання «Чи не замерзнемо ми взимку?», «Чи не буде віялових відключень через нехватку вугілля на теплоелектростанціях?» і т.д. і т.п. До цих питань ще можна добавити проблеми, що можуть виникнути в наслідок саме кібератак на об’єкти критичної інфраструктури і в першу чергу для операторів найважливіших об’єктів енергетичної інфраструктури [65; 124].

Сьогодні у світі існує чимало різних визначень кібертероризму. Так, під кібертероризмом зазвичай розуміють незаконні атаки і загрози атаки на комп’ютери, мережі і збережену в них інформацію в цілях залякування чи примусу держави або її населення та реалізації певних політичних або соціальних цілей [34]. У нашому випадку, можна визначити кібертероризм і як «Тероризм, пов’язаний з кіберпростором, а кібертеракти як терористичні акти, спрямовані на кіберінфраструктуру, зокрема, на системи управління найважливішими об’єктами» [18; 23].

В даному контексті важливим для нашого дослідження стає позиція Міністерство національної безпеки США, яке в своїх базових документах визначає найважливіші об’єкти державної інфраструктури як «Системи і

активи – фізичні і віртуальні, значення яких настільки велике, що обмеження їх дієздатності або їх руйнування може призвести до послаблення безпеки, економіки, соціального благополуччя або соціальної безпеки, нанесення шкоди довкіллю або якого-небудь поєднання цих несприятливих явищ у будь-якій федеральній юрисдикції, юрисдикції штату, регіональній, територіальній або місцевій юрисдикції» [35].

Зі свого боку Директива Національного інституту досліджень Європарламенту і Єврокомісії з «Мережевої та інформаційної безпеки», від 07 грудня 2015р. визначає та встановлює конкретні вимоги щодо управління ризиками. В ній ідеться крім іншого і про поданням даних про інциденти на об'єкти критичної інфраструктури. Серед найбільш часто атакованих об'єктів автори дослідження виділяють такі сфери критичної інфраструктури, як: «енергетика (електрика, природний газ і нафтопереробна продукція); кредитно-фінансові заклади і біржі; транспорт: повітряний, морський, залізничний; охорона здоров'я; інформаційні і комунікаційні технології (ІКТ); органи державного управління» [37].

Українське суспільство добре відчуло на собі всі проблеми, пов'язані з кібертероризмом, причому це були і енергетична сфера і фінансова, органи державного управління. В даному контексті особливо важливо підтримував надійну роботу та зберігати стабільність в енергетичному секторі, наприклад, необхідно постійно підтримувати стабільну роботу електромереж, оскільки в разі збоїв чи цілеспрямованих атак наслідки можуть проявитися швидко а усунення їх займати досить великий проміжок часу [8; 14; 76]. Ну і не варто звісно забувати, що саме з використанням електричних мереж та відповідним доступом до Інтернет сучасні зловмисники намагаються атакувати об'єкти критичної інфраструктури [78].

Варто погодитися з думкою М. Домарацького, що «Енергія необхідна для роботи всіх секторів, тому аварії в системі електропостачання майже неминуче позначаються на функціонуванні різних об'єктів. В якості прикладу можна розглянути бензозаправні станції, які часто не оснащуються

аварійними джерелами електроживлення високої ємності, а, відповідно, відключення електроживлення може призвести до обмеження чи навіть до зупинки їхньої роботи. Далі бензозаправні станції можуть виявитися не в змозі забезпечувати паливом транспортні засоби та аварійні генератори, які необхідні для роботи інших найважливіших об'єктів інфраструктури, тим самим впливаючи на роботу енергетичного та транспортного секторів» [37].

Автор також акцентує увагу залежності національних інтересів, державної безпеки від безпосереднього втручання зловмисників в роботу електромереж, а саме: «Без резервного, постійного та/або альтернативного енергопостачання лікарні, банки та державні установи можуть виявитися не в змозі продовжити свою роботу, а значить, будуть порушені: сектор охорони здоров'я; фінансовий і страховий сектори; сектор державного управління і адміністрування» [37].

Тут також варто нагадати, що в Україні сьогодні функціонує велика кількість ядерних електростанцій, що ставить нашу країну від їх роботи в певну залежність. При будь-якому збої в роботі атомних електростанцій в Україні є велика ймовірність отримати складну ситуацію в енергетиці країни в цілому. На відміну від нашої держави 94,3% світового енерговиробництва припадає на неядерні енергоносії. А це робить об'єкти без ядерної енергетичної інфраструктури головними мішенями для різного роду атак та можливих диверсій. Тому, розуміючи таку залежність та вразливість даного сектору, багатьма країнами світу робиться акцент на захисті тих об'єктів критичної інфраструктури, які являються найбільш вразливими і часто атакованими кіберзлочинцями. Для прикладу, така ситуація прописана в одному з базових документів ОБСЄ під назвою «Керівництво по передовій практиці захисту найважливіших об'єктів неядерної енергетичної інфраструктури від терористичних актів у зв'язку з погрозами, які виходять від кіберпростору» [77; 123].

Для запобігання таких ситуацій в багатьох країнах світу використовується система превентивних та антикризових заходів управління,

що застосовуються для захисту найважливіших об’єктів критичної енергетичної інфраструктури. Як правило, такі заходи узгоджуються на міжнародному рівні задля не допущення збоїв в роботі систем різних країн світу. У деяких країнах уряди розробляють спеціальні галузеві плани [35]. У Сполучених Штатах спеціальні галузеві плани розроблені для кожного сектору, включаючи енергетичний і сектор комунікацій.

Україна намагається також іди в ногу з часом і приймати відповідні рішення, які б дозволили якісно захищати національні системи і відповідно реагувати на сучасні виклики. Прийнята ще у 2015 р. «Стратегія Національної безпеки України» розглядає енергетичний сектор на макроекономічному рівні, і тому вона визначає загрози енергетичній безпеці лише як: «спотворення ринкових механізмів в енергетичному секторі; недостатній рівень диверсифікації джерел енергоносіїв і технологій; криміналізацію та корумпованість енергетичної сфери; недієву політику енергоефективності та енергопостачання» [25; 33; 139].

Щоправда, кібератаки на регіональні обленерго, зокрема Прикарпаття обленерго, Київобленерго і Чернівціобленерго спонукали керівництво відповідних структур внести зміни в законодавство і вже в 2016 р. в «Концепції розвитку сектора безпеки і оборони України» сфера енергетики розглядаються як можлива мета атак. Зокрема, в цьому документі йдеться про кіберзагрози «автоматизованим системам державного та військового управління, об’єктам критичної інформаційної інфраструктури» [35].

Як бачимо з вище наведених даних, більшість країн світу намагається адаптуватися до вимог часу, що дозволить їм оперативно реагувати на виклики та загрози щодо захисту об’єктів критичної інфраструктури. Україна, переймаючи такий досвід, теж долучилася до когорти країн світу у питаннях боротьби з забезпечення інформаційної безпеки об’єктів критичної інфраструктури. Причому це відноситься як до нормативно-правової бази, так і адміністративного регулювання даних процесів. Деякі країни не мають спеціального регулятора у сфері захисту об’єктів критичної інфраструктури.

Сьогодні перед державною владою в Україні першочерговим є завдання комплексного захисту системи об’єктів критичної інфраструктури – нормативно-правового (прийняття необхідного законодавства в сфері безпеки об’єктів критичної інфраструктури) та адміністративного (налагодження чіткою структури управління як на національному, так і на регіональному рівнях).

3.3. Напрями удосконалення державної політики забезпечення безпекою об’єктів критичної інфраструктури в Україні

Забезпечення безпеки та безперебійного функціонування об’єктів критичної інфраструктури значною мірою залежить від так званого «людського фактора». Саме рівень підготовленості фахівців, їхні компетенції, розуміння специфіки діяльності об’єктів критичної інфраструктури та механізмів ефективної реалізації своїх функцій, а також уміння налагоджувати та здійснювати взаємодію багато в чому зумовлюють успіх справи захисту критичної інфраструктури в цілому. Водночас слід розуміти, що зазначені якості не з’являються самі по собі. Сподівання лише на отриману освіту чи власний життєвий або професійний досвід, без урахування особливостей, властивих сфері захисту критичної інфраструктури або окремому об’єкту критичної інфраструктури, для пізнання яких необхідний тривалий період роботи в галузі, також може призвести до серйозних наслідків як для окремого об’єкта, так і для держави загалом. Тому виникає необхідність в упорядкуванні адміністративно-правових засад підготовки та підвищення кваліфікації фахівців із захисту критичної інфраструктури.

Переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Функціонування об’єктів критичної інфраструктури в такому специфічному середовищі, як кіберпростір, пов’язане з уразливістю і загрозами і вимагає розробки нового інструментарію. Поряд з інцидентами

природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб. Неодмінною умовою вирішення питань щодо забезпечення інформаційної та кібербезпеки є розуміння того, що держава знаходиться в нерозривному зв'язку і взаємодії з іншими структурами і суб'єктами, що відображається законодавчими, організаційними та технічними (технологічними) аспектами /рівнями взаємодії. Управління інформаційною та кібернетичною безпекою об'єктів критичної інфраструктури ґрунтується на знаннях про стан об'єктів управління, стан середовища функціонування і про впливи, які відбуваються [86].

Об'єкти критичної інфраструктури піддається різним типам загроз – природних або спричинених необережною поведінкою людини, деякі загрози можуть мати своєю метою терористичні цілі. Всі ми ще добре пам'ятаємо ситуацію з кібератакою на об'єкти критичної інфраструктури у всьому світі з метою отримання викупу, що є прикладом комерційної діяльності, яка може серйозно вплинути на об'єкти критичної інфраструктури, наприклад через шифрування даних користувачів та вимагання оплати в обмін на розблокування даних, як це було з відомим вірусом NotPetya в 2017 р. [65].

Пріоритетні напрями забезпечення безпеки критичної інфраструктури: комплексне вдосконалення правового підґрунтя захисту критичної інфраструктури, створення системи державного управління її безпекою; посилення охорони об'єктів критичної інфраструктури, зокрема енергетичної і транспортної; налагодження співробітництва між суб'єктами захисту критичної інфраструктури, розвиток державно-приватного партнерства у сфері запобігання надзвичайним ситуаціям та реагування на них; розроблення й запровадження механізмів обміну інформацією між державними органами, приватним сектором і населенням стосовно загроз критичній інфраструктурі та захисту чутливої інформації в цій сфері; профілактика техногенних аварій, оперативне й адекватне реагування на них,

локалізація і мінімізація їх наслідків; розвиток міжнародного співробітництва в цій сфері [118].

Загрози для об’єктів критичної інфраструктури також можуть бути пов’язані із злочинною поведінкою та непрямим чином. Оскільки країни покликані захищати об’єкти критичної інфраструктури від різних рівнів ризику, ключовим питанням є наступне, то, з іншого боку, постає запитання щодо необхідності прийняття урядами країн світу єдиного плану, який здатен охопити всі можливі загрози. Все це повинно б базуватися на існуючій міжнародно-правовій базі. Серед країн, які прийняли стратегії об’єктів критичної інфраструктури, більшість застосовують підхід з урахуванням усіх небезпек. Це означає, як описують А.М Полєжаєв та Ю.П. Стародуб, що «Стратегічні цілі та організаційні структури сформовані таким чином, щоб враховувати випадкові, навмисні та природні загрози для об’єктів критичної інфраструктури в цілому. Основне обґрунтування застосування такого підходу полягає в тому, що ті самі процеси управління ризиками та співробітництва, а також механізми реагування на кризи можуть широко застосовуватися для реагування на всі види загроз взаємозамінним чином» [98.; 127].

Підходи з урахуванням всіх небезпек застосовуються такими країнами, як Канада і Великобританія. Інші країни використовують змішаний підхід. Наприклад, Австралія, розробила специфічні керівні принципи щодо захисту об’єктів критичної інфраструктури від терористичних актів. Як описують цей процес Д. Бобро і О. Єрменчук «Керівні принципи доповнюють загальну стратегію країни щодо забезпечення безпеки об’єктів критичної інфраструктури, яка розширює сферу її дії через охоплення інших небезпек» [17; 42].

Більшість країн, у тому числі ті, що не мають спеціальних стратегій, присвячених захисту об’єктів критичної інфраструктури, розглядають ці питання в різних політичних нормативних документах, запроваджених різними урядовими установами. Ці документи зазвичай включають в себе

національну стратегію і політику боротьби з тероризмом. Хоча «…ці різні політики могли бути прийняті в різний час і різними державними установами, вкрай важливо, щоб вони стали всіма частинами зв'язкового посилання та підходу до захисту об'єктів критичної інфраструктури» [19].

Враховуючи різноманітність підходів між різними існуючими стратегіями захисту об'єктів критичної інфраструктури та кібербезпеки, як згадує М. Домарацький, Міжнародний союз електрозв'язку в даний час очолює зусилля сумісно з різними глобальними учасниками по створенню загального довідкового керівництва національних стратегій з кібербезпеки. Автор звертає увагу на основні цілі даного документу, як базового в питаннях захисту об'єктів критичної інфраструктури, зокрема Домарацький пише, що цей документ покликаний серед іншого і: «дати країнам чітке уявлення про цілі та зміст національної стратегії кібербезпеки; окреслити в загальних рисах існуючі моделі та ресурси захисту критичної інфраструктури; спрямовувати країни в процесі розробки своїх стратегій та оцінки стратегії» [38].

Окрім вищезазначеного, до національної політики належить також і державна політика захисту об'єктів критичної інфраструктури. Зокрема, коли розробляється національна стратегія щодо захисту об'єктів критичної інфраструктури, важливо скласти повний перелік всіх національних політик, що мають до неї відношення. Можуть існувати деякі політичні та нормативні структури, що стосуються інфраструктури в цілому. Необхідно визначити роль і місце існуючих нормативних рамок в загальних цілях захисту об'єктів критичної інфраструктури. Так для дотримання відповідних міжнародно-правових актів, як вказують українські науковці Г. Ситнік, , Бобро «Країни розробили цілий ряд політик, законів, положень, стратегій, планів та заходів щодо підвищення безпеки хімічних, біологічних, радіологічних та ядерних об'єктів та відповідної інформації» [9; 10; 17].

Визначаючи основні завдання забезпечення інформаційної безпеки об'єктів критичної інфраструктури, як підсумовує С. Гончар «Можна

зазначити, що першочерговим є завдання створення дієвого механізму координації зусиль органів влади та підрозділів організацій, які повинні забезпечувати інформаційну безпеку відповідних об'єктів» [28].

Крім того, необхідно впроваджувати ряд істотних заходів на державному, регіональному та галузевому рівнях з організаційного, нормативно-правового та науково-методичного забезпечення. Як показує досвід розвинутих країн, дослідження механізмів захисту інформації об'єктів критичної інфраструктури включає на перших кроках етап ідентифікації (визначення) елементів, які повинні розглядатися в якості об'єктів критичної інфраструктури. Разом з тим важливим напрямком забезпечення захисту інформації на об'єктах критичної інфраструктури є запровадження відповідного управлінського впливу. Щоправда, аналіз українського правового поля в даній сфері вказує на недостатність національних та галузевих стандартів щодо забезпечення інформаційної безпеки об'єктів критичної інфраструктури України.

Як ми вже писали вище, що із важливих перспективних напрямків удосконалення державної політики забезпечення безпекою об'єктів критичної інфраструктури в Україні є процес підготовки фахівців в даній сфері. Як пише С. Теленик «Саме рівень підготовленості фахівців, їхні компетенції, розуміння специфіки діяльності об'єктів критичної інфраструктури та механізмів ефективної реалізації своїх функцій, а також уміння налагоджувати та здійснювати взаємодію багато в чому зумовлюють успіх справи захисту критичної інфраструктури в цілому. Водночас слід розуміти, що зазначені якості не з'являються самі по собі. Сподівання лише на отриману освіту чи власний життєвий або професійний досвід, без урахування особливостей, властивих сфері захисту критичної інфраструктури або окремому об'єкту критичної інфраструктури, для пізнання яких необхідний тривалий період роботи в галузі, також може призвести до серйозних наслідків як для окремого об'єкта, так і для держави загалом. Тому виникає необхідність в упорядкуванні адміністративно-

правових засад підготовки та підвищення кваліфікації фахівців із захисту критичної інфраструктури» [134].

Насамперед йдеться про те, що сфера захисту об'єктів критичної інфраструктури не вичерпується лише категорією ІТ-спеціалістів. Водночас, адміністрування освітнього процесу щодо кадрового забезпечення об'єктів критичної інфраструктури на всіх рівнях за різними профілями, включаючи управлінський персонал, насамперед, має здійснюватися на підставі чітко сформульованого наукового обґрунтування.

Досягненню поставленою мети, як пише С. Теленик, сприятиме розв'язання таких завдань як: «1) аналіз нормативно-правових актів, якими регулюються суспільні відносини у сфері підготовки та підвищення кваліфікації вказаної категорії фахівців; 2) відстеження кореляції даних національних класифікаторів, зокрема «Класифікатора видів економічної діяльності" (КВЕД) і «Класифікатора професій» (КП) та переліку галузей знань і спеціальностей, затверджених постановою Кабінету Міністрів України від 29 квітня 2015 р. № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти», із суб'єктами ЗКІ за категоріями відповідних фахівців; 3) встановлення причин, що перешкоджають ефективності процесу підготовки кадрів для сфери ЗКІ; 4) формулювання пропозицій щодо удосконалення чинної нормативно-правової бази з досліджуваного питання» [134].

Питання щодо підготовки фахівців із захисту критичної інфраструктури є актуальним для будь-якої держави, причому різні держави по-різному вирішують дане питання. Так, згідно аналітичної доповіді під назвою «Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури», згідно інформаційного запиту в Google за ключовими словами «training critical infrastructure protection» було отримано близько 47 млн. 500 тис. посилань [95, с. 78]. У 2020 році ця цифра зросла до 206 млн. посилань [156]. Подібне багатократне зростання є чи не найпереконливішим свідченням, як пишуть фахівці з Національного

інституту стратегічних досліджень, «Актуальності проблеми у всьому світі. Водночас, не зважаючи на окремі спільні методики й технології підготовки фахівців, кожна держава має свої специфічні особливості. Ці особливості зумовлюються, насамперед, встановленим порядком і правилами, закріпленими на рівні нормативно-правових актів» [95, с. 78].

Слід зазначити, що на даний час підготовка, перепідготовка, підвищення кваліфікації фахівців урегульована Законом України «Про освіту» [115], а також спеціальними законами «Про професійно-технічну освіту» про які детально пише у своїй роботі відомий український фахівець в сфері інформаційної безпеки Г. Почепцов [103], «Про вищу освіту» [106]. З огляду на це підвищення кваліфікації, що тлумачиться як «набуття особою нових та/або вдосконалення раніше набутих компетентностей у межах професійної діяльності або галузі знань» [115] є одним із елементів освіти дорослих, включених до післядипломної освіти поряд зі спеціалізацією, перепідготовкою та стажуванням.

Що ж до формування напрямів підготовки, то цей процес також є багаторівневим. У своїй основі він здійснюється, насамперед, відповідно до окремих національних класифікаторів. Так, в Україні одним із найголовніших регуляторних документів, що впливає на визначення напрямів підготовки фахівців та процедури здійснення державного замовлення є «Класифікатор видів економічної діяльності» [90].

Ще одним нормативним документом, який впливає на формування й реалізацію напрямів підготовки фахівців із ЗКІ, є «Класифікатор професій» [91]. Одразу слід зазначити, що в межах даного дослідження до уваги беруться не всі працівники об’єктів критичної інфраструктури, а лише ті, до функціональних обов’язків яких входить реалізація функцій щодо прямого (безпосереднього), а не опосередкованого захисту критичної інфраструктури [134].

Окремо варто виділити шляхи вдосконалення державної системи інформаційного та кібернетичного захисту об’єктів критичної

інфраструктури. Їх також умовно можна поділити на декілька категорій, а саме: розробка та прийняття необхідних нормативних документів (переліку об’єктів критичної інфраструктури держави; плану заходів щодо реалізації Стратегії кібербезпеки України; протоколу спільних дій основних суб’єктів забезпечення кібербезпеки, суб’єктів кіберзахисту та власників (розпорядників) об’єктів критичної інформаційної інфраструктури під час попередження, виявлення, припинення кібератак та кіберінцидентів), організаційне узгодження діяльності суб’єктів забезпечення інформаційної та кібернетичної безпеки об’єктів критичної інфраструктури (розробка відомчих документів щодо визначення вимог до кіберзахисту ОКІ; визначення повноважень посадових осіб (введення підрозділів), відповідальних за забезпечення інформаційної та кібернетичної безпеки; визначення порядку ведення та використання державного реєстру кіберінцидентів та технічне (технологічне) забезпечення інформаційної та кібернетичної безпеки об’єктів критичної інфраструктури (створення систем (підсистем) забезпечення безпеки ОКІ згідно вимог нормативних та відомчих документів; визначення показників забезпечення інформаційної та кібернетичної безпеки об’єктів критичної інфраструктури; адаптація (розробка) засобів управління інформацією і подіями безпеки (SIEM) відповідним вимогам; формалізація підходів керування ОКІ з врахуванням вимог відомчих документів (на прикладі вимог визначених)) [102].

ВИСНОВКИ

У результаті проведеного дослідження можна підсумувати, що в українській науці існує значний масив наукових досліджень і концепцій, які створюють основи для формулювання державної системи захисту об’єктів критичної інфраструктури.

З’ясовано наявні та перспективні методологічні підходи до вивчення правового змісту понять «критична інфраструктура», «захист критичної інфраструктури», а також встановлено, що правовий зміст даних понять залишається сьогодні остаточно не визначеним.

В роботі зазначено, що Україна володіє достатньо потужним інфраструктурним потенціалом, зважаючи на що вона перетворилася сьогодні на суб’єкта міжнародного інфраструктурного потенціалу з необхідністю державної системи захисту об’єктів критичної інфраструктури. Ступінь готовності та здатності до захисту визначені перш за все нормативно-правовою та адміністративними заходами захисту від існуючих та потенційних загроз.

Події останніх років, періодичні хакерські атаки на об’єкти критичної інфраструктури, використання вірусу в своїй діяльності – все це підтверджує думку багатьох фахівців з питань захисту об’єктів критичної інфраструктури про важливість захисту об’єктів саме щодо кібербезпеки.

Всі фахівці з питань захисту критичної інфраструктури визнають можливість активного використання сучасних інформаційно-комунікаційних технологій для ведення зокрема і терористичних актів, які в першу чергу спрямовані саме на об’єкти критичної інфраструктури. Тут особливе місце відведено об’єктам національної інфраструктури в якості потенційних мішеней. Зважаючи на устарівання таких об’єктів в нашій країні через фізичне зношування та недофінансування державою, що призводить до повної втрати функціональності, може в цілому вплинути на стан

національної безпеки і спричинити надзвичайні ситуації певного рівня і масштабу на об’єктах критичної інфраструктури.

Для запобігання таких ситуацій в багатьох країнах світу використовується система превентивних та антикризових заходів управління, що застосовуються для захисту найважливіших об’єктів критичної інфраструктури.

Більшість країн світу намагається адаптуватися до вимог часу, що дозволить їм оперативно реагувати на виклики та загрози щодо захисту об’єктів критичної інфраструктури. Україна, переймаючи такий досвід, теж долучилася до когорти країн світу у питаннях боротьби з забезпечення інформаційної безпеки об’єктів критичної інфраструктури. Причому це відноситься як до нормативно-правової бази, так і адміністративного регулювання даних процесів. Деякі країни не мають спеціального регулятора у сфері захисту об’єктів критичної інфраструктури.

Однією з провідних країн світу сьогодні у боротьбі з інформаційним загрозами залишається США. Терористичні акти, а особливо 2011 р., на американців спонукали їх до активного пошуку нових підходів в організації державного управління системою захисту різних сфер суспільного життя, зокрема і критичної інфраструктури.

Дослідники управління кібербезпекою критичної інфраструктури з точки зору взаємодії між державою та приватним сектором на сьогодні визначають три основні типи стратегій, що використовуються процесі управління, а саме централізований, диверсифікований та дотримання державою «доктрини субсидіарності».

Виявлено еволюцію адміністративного та нормативно-правового регулювання державної системи захисту критичної інфраструктури в Україні. Обґрунтовано взаємозалежність між розвитком законодавства у сфері національної безпеки і адміністративно-правовим регулюванням державної системи захисту критичної інфраструктури. Визначено та детально охарактеризовано завдання законодавства у сфері захисту критичної

інфраструктури. Базовими на сьогодні в Україні є наступні нормативно-правові акти: Стратегія національної безпеки різних років, Закони України «Про основи національної безпеки України», «Про національну безпеку України» та ін.

В нашій країні передбачено комплексне створення державної системи захисту критичної інфраструктури на базі новітніх підходів до вирішення питань державного управління в цій галузі, зокрема вироблення сучасних інноваційних підходів до управління ризиками безпеки критичної інфраструктури та оптимізоване застосування наявних ресурсів, гнучке і швидке реагування на інциденти і кризи.

Визначено місце та роль СБУ в державній системі захисту об’єктів критичної інфраструктури, до основних функцій якого входить планування та реалізацію заходів державної політики у сфері захисту об’єктів критичної інфраструктури, стратегічне планування застосування сил СБУ з метою захисту об’єктів критичної інфраструктури, проведення експертної оцінки загроз та ризиків критичній інфраструктурі, визначення заходів із запобігання їх реалізації та реагування на них тощо. Подано конкретні пропозиції щодо удосконалення законодавства у сфері захисту критичної інфраструктури в частині повноважень СБУ.

Але ключовим державним органом в Україні щодо управління критичною інфраструктурою є Державна служба України з надзвичайних ситуацій. Керує загальною системою органів і підрозділів з надзвичайних ситуацій безпосередньо Міністр внутрішніх справ, який у тісній співпраці і персональній відповідальності перед Кабінетом Міністрів України виконує завдання, що покладаються на підрозділи ДСНС у випадку надзвичайних ситуацій. На думку багатьох дослідників питань захисту інформаційного простору України, підрозділи ДСНС повинні стати більш важливим елементом захисту ніж вони є сьогодні. Особливо це відноситься до регіональних підрозділів, які повинні миттєво реагувати на нові виклики щодо питань державної системи захисту об’єктів критичної інфраструктури.

Запропоновано конкретні заходи удосконалення законодавства у сфері захисту критичної інфраструктури в контексті підвищення ефективності адміністративно-правового регулювання ДСЗКІ. Окреслено напрями удосконалення підготовки та підвищення кваліфікації фахівців із захисту критичної інфраструктури. Підкреслено, що питання забезпечення безпеки та стійкості критичної інфраструктури є одним із найважливіших для національної безпеки держави. Значною мірою діяльність у цій сфері залежить від професіоналізму, рівня освіченості і компетентності відповідних фахівців.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Адміністративне право України : підручник / за ред. Т. О. Коломоєць, Г. Ю. Гулєвської ; Держ. ВНЗ «Запорізький нац. ун-т». М-во освіти і науки України. Київ : Істина, 2009. 475 с.

2. Адміністративне право України в сучасних умовах (виклики початку XXI століття) : монографія / [В. В. Галунько та ін.] ; за заг. ред. д-ра юрид. наук, доц. В. В. Галунька ; Херсон. юрид. ін-т Харків. нац. ун-ту внутр. справ. Херсон : Херсонська міська друкарня, 2010. 378 с.

3. Актуальні проблеми фінансового управління : глобальні тенденції і національна політика / за ред. Т. І. Єфименко ; ДННУ «Акад. фін. управління». Київ, 2018. 496 с.

4. Алексеев С. С. Механизм правового регулирования в социалистическом государстве. М. : Юрид. лит., 1966. 483 с.

5. Аналітична доповідь до щорічного послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2017 році». Київ : НІСД, 2017. 928 с.

6. Аналітична доповідь до щорічного послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2018 році». Київ : НІСД, 2018. 688 с.

7. Батюк В. Еволюція концепцій міжнародної і національної безпеки. Спостерігач. 1996. № 25. С. 2–13.

8. Беззубов Д. О. Правова структура та принципи побудови системи національної безпеки в Україні / Д. О. Беззубов // Держава і право. Юридичні і політичні науки. – 2011. – Вип. 51. – С. 231–236.

9. Безопасность критических инфраструктур [Електронный ресурс]. – Режим доступу: http://www. slideshare.net/demidovov/1803201437129875

10. Безпека як категорія і функція державного управління / Г. П. Ситнік // Вісн. Нац. академії держ. управління. – 2004. – № 1. – С. 350–357.

11. Белов П. Какой должна быть концепция национальной безопасности. Обозреватель. 2000. № 1. С. 8–10.

12. Бєлай С. В. Державні механізми протидії кризовим явищам соціально-економічного характеру: теорія, методологія, практика : монографія / С. В. Бєлай. – 2015. – 249 с.

13. Бірюков Д. Концепція захисту критичної інфраструктури як елемент загальноєвропейської безпекової політики / Д. Бірюков // Наукові записки. – К. : Інститут політичних і етнонаціональних досліджень імені І. Ф. Кураса НАН України, 2013. – № 6 (68). – С. 106−115.

14. Бірюков Д. С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні/ Аналітична доповідь / Д. С. Бірюков, С. І. Кондратов. – К. : ПП «Видавництво «ФЕНІКС», 2012. – 92 с.

15. Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. Стратегічні пріоритети. Серія : Економіка. 2015. № 4 (37). С. 83–93.

16. Бобро Д. Г. Методологія оцінки рівня критичності об’єктів інфраструктури. Стратегічні пріоритети. 2016. № 3 (40). С. 77–86. URL: http://www.niss.gov.ua/public/File/Str_prioritetu/SP_3_40_16.pdf.

17. Бобро Д. Г. Удосконалення методології ранжування об’єктів критичної інфраструктури та їх віднесення до критичної інфраструктури : аналітична записка [Електронний ресурс] / Д. Г. Бобро. – Режим доступу : http://www.niss.gov.ua/content/articles/files/krutuchna_infra-a7636.pdf

18. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко та ін. ; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. − К. : ДУТ, 2015.

19. Вакуленко В. М. Державна регіональна політика : навч. посіб. / В. М. Вакуленко, Н. М. Гринчук. – К. : Вид-во НАДУ. – 64 с.

20. Великий тлумачний словник сучасної української мови / [уклад. і голов. ред. В. Т. Бусел]. Київ ; Ірпінь : Перун, 2003. 1440 с.

21. Верголяс О. Реформування системи захисту та підвищення стійкості критичної інфраструктури України в розрізі актуальних загроз [Електронний ресурс] / О. Верголяс. – Режим доступу: https://coolyanews.info/reformuvannyasistemi-zahistu-ta-piidvischennya-stiijkostii-kritichnoyi-iinfrastrukturi-ukrayinii-v-rozriiziiaktual.html

22. Виживання в умовах надзвичайних ситуацій / П. Б. Волянський, О. Г. Барило, С. О. Гур'єв та ін. − Х. : ФОП Панов А.М., 2016. − 189 с.

23. Гнатюк С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С. О. Гнатюк // Безпека інформації. − 2013. − Т. 19. − № 2. − С. 120.

24. Гнатюк, С. О., Рябий, М. О., & Лядовська, В. М. (2014). Визначення критичної інформаційної інфраструктури та її захисту: аналіз підходів. Зв'язок, 4, 3–7

25. Гнатюк, С. О., Сидоренко, В. М., & Дуксенко, О. П. (2015). Сучасні підходи до виявлення та ідентифікації найбільш важливих об'єктів критичної інфраструктури. Безпека інформації, 21(3), 269–275. doi: 10.18372/2225-5036.21.9690

26. Голосніченко І. П., Стахурський М. Ф. Адміністративне право України: основні поняття : навч. посіб. Київ : ГАН, 2005. 231 с.

27. Гончар С. Ф., Леоненко Г. П., Юдін О. Ю. Теоретико-методологічний аспект забезпечення інформаційної безпеки об'єктів критичної інфраструктури. Вісник Національного університету «Львівська політехніка». Комп'ютерні системи та мережі, 2014. № 806. С. 34-39: веб-сайт. URL: http://nbuv.gov.ua/UJRN/VNULPKSM_2014_806_8

28. Гончар С.Ф. Шляхи удосконалення державної політики забезпечення інформаційної безпеки критичної інфраструктури України : матеріали круглого столу «Державне реагування на загрози національним інтересам України: актуальні проблеми та шляхи їх розв'язання». – К.: НАДУ, 2014. — С. 92-95.

29. Горбулін В. П. Засади національної безпеки України / В.П. Горбулін, А. Б. Качинський. – К. : Інтертехнологія, 2009. – 272 с.

30. Гурне Б. Державне управління / Б. Гурне. – К. : Основи, 1993. – 165 с.;

31. Державна програма співробітництва України з Організацією Північноатлантичного Договору (НАТО) на 2001-2004 роки : затв. указом Президента України від 27 січ. 2001 р. Офіційний вісник України. 2001. № 5. Ст. 175.

32. Державне управління в Україні: наукові, правові, кадрові та організаційні засади : навч. посібник / за заг. ред. Н. Р. Нижника, В. М. Олуйка. Л. : Вид-во Національного університету «Львівська політехніка», 2002. – 352 с.

33. Дзьобань О. П. Національна безпека в умовах соціальних трансформацій: методологія дослідження та забезпечення : монографія / О. П. Дзьобань. – Х. : Константа, 2006. – 440 с.

34. Діордіца І.В. Поняття та зміст кібертероризму [Електронний ресурс]. – Режим доступу: https://goal-int.org/ponyattya-ta-zmist-kiberterorizmu/

35. Домарацький М. Б. Нормативне й адміністративне забезпечення державного регулювання критичної інфраструктури в Україні: аналіз і оцінка / М. Б. Домарацький // Вісник Національного університету цивільного захисту України. – 2020. – Вип. 1(12). – С. 470–475.

36. Домарацький М. Б. Особливості категоріювання об’єктів критичної інформаційної інфраструктури / М. Б. Домарацький // Фінансова система та економічна безпека: стан, проблеми, ефективність: збірник тез наукових робіт учасників міжнародної науково-практичної конференції для студентів, аспірантів та молодих учених. - К.: Аналітичний центр «Нова Економіка», 2019. – Ч. 2. – С. 91–92.

37. Домарацький М. Б. Специфіка державного регулювання критичної інфраструктури в Україні / М. Б. Домарацький // Публічне управління та митне адміністрування. – 2020. − № 2(25). – С. 24–46.

38. Домарацький М.Б. Державне управління забезпеченням безпеки критичної інфраструктури в Україні .– Рукопис. – Дисертація на здобуття наукового ступеня кандидата наук з державного управління за спеціальністю 25.00.05 – державне управління у сфері державної безпеки та охорони громадського порядку. Національний університет цивільного захисту України, Харків, 2020. – 259 с.

39. Домбровська С. М. Державне управління у сфері безпеки соціально- еколого-економічних систем : монографія / С. М. Домбровська, В. В. Коврегін, А. Л. Помаза-Пономаренко, О. М. Колєнов, – Х. : НУЦЗУ, 2017. – 244 с.

40. Дубов Д.В. Майбутнє кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців : аналітична доповідь / Д.В. Дубов, М.А. Ожеван. − К. : НІСД, 2012. − С. 22.

41. Енциклопедичний словник з державного управління / уклад. : Ю. П. Сурмін, В.Д. Бакуменко, А. М. Михненко та ін.; за ред. Ю.В. Ковбасюка та ін. – К. : НАДУ, 2010. – 820 с.

42. Єрменчук О. П. Сутність та зміст поняття «інфраструктура» в контексті захисту критичної інфраструктури / О. П. Єрменчук // Бюлетень Міністерства юстиції України. – 2017. − № 11 (193). – С. 35–40.

43. Єрменчук О.П., Пальчик М.Л. Проблемні аспекти правового регулювання державно-приватного партнерства у сфері захисту критичної інфраструктури. Інформаційна безпека людини, суспільства, держави. 2019. № 2 (26). С. 40-49.

44. Жевелєва І.С. Правові засади забезпечення інформаційної безпеки об’єктів критичної інфраструктури [Електронний ресурс] / І. Жевелєва // International scientific journal "Internauka." Series: "Juridical Sciences". – Режим доступу: https://www.inter-nauka.com/uploads/public/1591638358216.pdf

45. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” (із змінами). [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94

46. Закон України “Про основні засади забезпечення кібербезпеки України”. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua /laws/show/2163-19

47. Закон України «Про внесення змін до деяких законодавчих актів України у зв’язку з прийняттям Кодексу цивільного захисту» від 02.10.2012 № 5404-VI [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/5404-17

48. Закон України «Про Загальнодержавну цільову програму захисту населення і територій від надзвичайних ситуацій техногенного та природного характеру на 2013-2017 роки» від 07.06.2012 № 4909-VI [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/4909-17

49. Закон України «Про зону надзвичайної екологічної ситуації» від 13.07.2000 № 1908-III [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/1908-14; Закон України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2469-19#Text

50. Закон України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2469-19#Text

51. Закон України «Про об’єкти підвищеної небезпеки» від 18.01.2001 № 2245-III [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/2245-14

52. Закон України «Про правовий режим надзвичайного стану» від 16.03.2000 № 1550-III [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/1550-14

53. Закон України «Про правовий режим території, що зазнала радіоактивного забруднення внаслідок Чорнобильської катастрофи» від

27.02.1991 № 791а-XII [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/791%D0%B0-12

54. Закон України «Про Службу безпеки України» від 25 березня 1992 року № 2229-XII [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2229-12#Text

55. Запорожець О. І. Безпека життєдіяльності / О. І. Запорожець. – К. : Центр навчальної літератури, 2013. – 448 с.

56. Захист населення і територій від надзвичайних ситуацій. Техногенна та природна небезпека / За загальною редакцією В. В. Могильниченка. – К. : КІМ, 2007. – 636 с.

57. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар. експерт. нарад / упоряд.: Д. С. Бірюков, С. І. Кондратов ; за заг. ред. О. М. Суходолі. – Київ : НІСД, 2015. – 176 с.

58. Иванов А.А. Риск-менеджмент : Учебно-методический комплекс / А.А. Иванов, С.Я. Олейников, С.А. Бочаров. – М. : Изд. центр ЕАОИ, 2008. – 193 с.

59. Кібербезпека держави: час перезавантаження. Радіо Свобода 27 червня, 2017 [Електронний ресурс]. – Режим доступу: http://safe-city.com.ua/kiberbezpeka-derzhavy-chas-perezavantazhennya/.

60. Ківалов С. В., Біла Л. Р. Адміністративне право України : навч.-метод. посіб. [2-ге вид., переробл. і доп.]. Одеса : Юрид. літ., 2002. 312 с.

61. Ковалів М. Правове забезпечення кібербезпеки критичної інформаційної інфраструктури України / Мирослав Ковалів, Руслан Скриньковський, Юрій Назар, Сергій Єсімов, Іван Красницький, Христина Кайдрович, Святослав Князь, Юлія Кемська // Traektoriâ Nauki = Path of Science. – 2021. - Vol. 7. - № 4. - S. 2011-2018.

62. Кондратов С. І. Про забезпечення координації дій, взаємодії та обміну інформацією при створенні державної системи захисту критичної інфраструктури : аналіт. доп. Київ : НСІД, 2018. 30 с.

63. Концепція (основи державної політики) національної безпеки України : постанова Верховної Ради України від 16 січ. 1997 р. № 3/97 ВР. Відомості Верховної Ради України. 1997. № 10. Ст. 85.

64. Концепція національної безпеки: між тоталітаризмом і демократією. Підтекст. 1996. №3 (7). С. 13–18.

65. Костюк І. Україна в фокусі кібератак [Електронний ресурс] / І. Костюк. − Режим доступу : https://scienceukraine.com/sciblogs/ukraina-v-fokusi- kiberatak

66. Кочетков К. Е. Аварии и катастрофы. Предупреждение и ликвидация последствий / К. Е. Кочетков. – М. : АСВ, 2012. – 320 с.

67. Кравець Є. Національна безпека України: до концепції законодавства. Вісник АН України. 1994. № 1. С. 83–90.

68. Кринична І. П. Державне управління процесами запобігання та профілактики надзвичайних ситуацій: праксиологічний досвід І. П. Кринична // Актуальні проблеми державного управління : зб. наук. пр. – ДРІДУ НАДУ, 2013. – № 1 (16). – С. 80–88.

69. Кучма Д. Я. Методологические основы концепции национальной безопасности Украины. Наука і оборона : зб. наук. матеріалів. Київ, 1995. Вип. 1. С. 39–51.

70. Леоненко Г.П., Юдин А.Ю. Проблемы обеспечения информационной безопасности систем критически важной информационной инфраструктуры Украины // Information Technology and Security. – 2013. – Вип. 1(3). – С. 44.

71. Лєрмонтова Ю. Зарубіжний досвід державного управління екстреною медичною допомогою в надзвичайних ситуаціях / Ю. Лєрмонтова // Державне управління та місцеве самоврядування. – 2012. – № 4 (15). – С. 191– 198.

72. Ліпкан В. А. Адміністративно-правове регулювання національної безпеки України : монографія. Київ : Текст, 2008. 440 с.

73. Ліпкан В. А. Концепція національної безпеки України: підходи до формування. Вісник прокуратури. 2003. № 10. С. 85–92.

74. Ліпкан В. А. Національна безпека України : нормативно-правові аспекти забезпечення : монографія. Київ : Текст, 2003. 180 с.

75. Ліпкан В. А., Кушнір О. В. Правові та організаційні засади взаємодії суб'єктів протидії торгівлі людьми : монографія / за заг. ред. В. А. Ліпкана. Київ : О. С. Ліпкан, 2013. 376 с.

76. Лозинська Т. М. Державне управління: методологія дослідження та діяльності / Теоретико-методологічні засади наукових досліджень в галузі державного управління : монографія / Т М. Лозинська ; за заг. ред. д. філос. н., проф. В. В. Корженка. – Дніпропетровськ : Комплектавтодор, 2011. – С. 151–171.

77. Лугунін О. Є. Статистика. Економічна та соціальна статистика : курс лекцій / О. Є. Лугунін. – Херсон : МУБіП, 2003. – 99 с.

78. Луценко М. М. Оцінка обстановки у надзвичайних ситуаціях / М. М. Луценко. – Х. : ХНАДУ, 2009. – 183 с.

79. Любанов А. Риск-менеджмент / А. Любанов, С. Филин, А. Чугунов // Ресурсы. Информация. Снабжение. Конкуренция. – 1999. – № 5. – С. 45–55.

80. Малишева Н. Надзвичайна ситуація / Н. Малишева // Юридична наука, 2002. – С. 54–57.

81. Мартинюк В,В., Паламарчук Н.А., Паламарчук С.А., Сівоха О.М. Задачі вдосконалення інформаційної та кібернетичної безпеки об'єктів критичної інфраструктури [Електронний ресурс] / В.В. Мартинюк та ін. // Збірник наукових праць ВІТІ № 2 – 2020. – С. 54-63. – Режим доступу: http://www.viti.edu.ua/files/zbk/2020/6_2_2020.pdf

82. Махутов Н. Эффективность мер по снижению опасности при чрезвычайных ситуациях / Н. Махутов, А. Костін // Проблеми безпеки при надзвичайних ситуаціях. – 1997. – Вип. 10. – С. 28–40.

83. Мельник О.В. Розуміння категорії «національна безпека» у вітчизняному та зарубіжному правознавстві / О.В. Мельник // Держава і право. Юридичні і політичні науки. – 2007. – Вип. 38. – С. 147–153.

84. Мельниченко О. А. Надзвичайні ситуації техногенного характеру: сутність та засоби державного управління / О. А. Мельниченко // Вісник Національного університету цивільного захисту України. Серія. Державне управління. – 2014. – Вип. 2 (2). – С. 149–156.

85. Мельничук О. Управління критичною інфраструктурою держави: базові методи та критерії ідентифікації об'єктів [Електронний ресурс] / О. Мельничук // Державне управління та місцеве самоврядування, 2019, Вип. 3 (42). – С.13-27. – Режим доступу: http://www.dridu.dp.ua/zbirnik_dums/2019/2019_03(42)/4.pdf

86. Методика оцінки кіберстійкості об'єктів критичної інфраструктури / Гончар С. Ф., Комаров М. Ю. // Безпека соціально-економічних процесів в кіберпросторі: матеріали Всеукр. наук.-практ. конф. (Київ, 27 берез. 2019 р.). – Київ: Київ. нац. торг.-екон. ун-т, 2019. – с. 49.

87. Михайлов А. М. Надзвичайні ситуації природного, техногенного й соціального характеру, захист від них [Електронний ресурс] / А. М. Михайлов. – Режим доступу: repo.sau.sumy.ua/.../Теоретичні%20засади%20ризику%20т

88. Настюк В. Я. Адміністративно-правові режими у сфері національної безпеки та протидії тероризму : монографія / В. Я. Настюк. – К. : НКЦ «Ін-т операт. діяльн. та держ. Безпеки», 2008. – 245 с.

89. Наукові засади захисту населення і територій від наслідків лісових пожеж з радіаційно небезпечними факторами : монографія / С. І. Азаров, С. А. Єременко, В. Л. Сидоренко, та ін. ; за заг. ред. П. Б. Волянського. − К. : ТОВ «Інтердрук», 2016. − 203 с.

90. Національний класифікатор України. Класифікатор видів економічної діяльності (КВЕД). ДК 009: 2010. [Чинний від 2012-01-01]. URL: https://registral.kiev.ua/kved.]

91. Національний класифікатор України. Класифікатор професій (КП). ДК 002: 2010 ; із змін., затвердженими наказом Міністерства економічного розвитку і торгівлі України від 15 лют. 2019 р. № 259. [Чинний 2010-11-01]. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/rada/show/va327609-10#n5.

92. Нижник Н. Р., Машков О. А. Системний підхід в організації державного управління. Київ : УАДУ, 1998. 160 с.

93. Нижник Н., Черленяк І. Синергетично-рефлексивна модель соціальної самоорганізації та управління. Вісник НАДУ. 2003. № 3. С. 5–14.

94. Новиков А. М., Новиков Д. А. Методология : словарь системы основных понятий. М. : ЛИБРОКОМ, 2013. 208 с.

95. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналіт. доп. / Д. Г. Бобро, С. П. Іванюта, С. І. Кондратов, О. М. Суходоля ; за заг. ред. О. М. Суходолі. Київ : НІСД, 2019. 224 с.

96. Офіційний веб-сайт Державної служби України з надзвичайних ситуацій [Електронний ресурс]. – Режим доступу: http://www.dsns.gov.ua/ua/Vnutrishniy-audit.html

97. Парсонс Т. Система современных обществ / [пер. с англ.]. М. : Аспект-Пресс, 1997. 564 с.

98. Полєжаєв А. М. До питання обліку системи моніторингу і прогнозування надзвичайних ситуацій техногенного характеру / А. М. Полєжаєв // А. М. Полєжаєв // Системи озброєння і військова техніка. - 2013. − № 3. − С. 139−142.

99. Порядок формування переліку об’єктів критичної інформаційної інфраструктури (Україна), 09.10.2020, № 943. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/943-2020-п#Text

100. Постанова Кабінету Міністрів від 23 серпня 2016 р. № 563 “Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави”

101. Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 “Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури”

102. Постанова Правління Національного банку України від 28.09.2017 року № 95 “Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України” [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/v0095500-17.

103. Почепцов Г. Інформаційні війни в закритих і відкритих системах. URL: http://www.academy.gov.ua/doc/zmi_pro_nas/publ/publ_2013_06_30.pdf.

104. Прангишвили И. В. Системный подход и общесистемные закономерности. М. : Синтег, 2000. 528 с.

105. Приходько Р. В. Закордонний досвід регулювання запобігання і ліквідації надзвичайних ситуацій на регіональному рівні / Р. В. Приходько, О. А. Ященко // Вісник Національного університету цивільного захисту України. Серія. Державне управління. – 2016. – Вип. 2 (5). – С. 272–282.

106. Про вищу освіту : Закон України від 01лип. 2014 р. Відомості Верховної Ради України. 2014. № 37–38. Ст. 2004.

107. Про державну підтримку інвестиційних проектів із значними інвестиціями в Україні: Закон України від 17 груд. 2020 р. № 1116-IX. Верховна Рада України : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/1116-20#Te

108. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави [Електронний ресурс] : Постанова Кабінету Міністрів України від 23 серп. 2016 р. № 563. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/563-2016-%D0%BF

109. Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту

: директива Ради Європейського Союзу 2008/ 114/ ЄС від 8 груд. 2008 р. Офіційний вісник Європейського Союзу. 2008. L 345. С. 75. URL: http://zakon2.rada.gov.ua/laws/show/984_002-08.

110. Про інформацію (Україна), 02.10.1992, № 2657-XII. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

111. Про критичну інфраструктуру та її захист : проєкт Закону України реєстр. № 10328 від 27 трав. 2019 р. Верховна Рада України : [сайт]. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996.

112. Про Національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII. Офіційний вісник України. 2018. № 55. Ст. 1903. URL : https://zakon.rada.gov.ua/laws/show/2469-19#n355.

113. Про Національну програму інформатизації (Україна), 04.02.1998, № 74/98-ВР. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/74/98-вр#Text

114. Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України: Рішення Ради національної безпеки і оборони України від 1.03.2014: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/n0001525-14

115. Про освіту : Закон України від 5 верес. 2017 р. № 2145-VIII. Голос України. 2017. № 178–179. 27 вересня.

116. Про основи національної безпеки України : Закон України 19 черв. 2003 р. № 964-IV. Відомості Верховної Ради України. 2003. № 39. Ст. 351. (Із змінами, внесеними згідно із Законом № 3200-IV від 15 груд. 2005 р. Відомості Верховної Ради України. 2006. № 14. Ст. 116).

117. Про основні засади забезпечення кібербезпеки: Закон України від 5.10.2017 № 2163-VIII: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

118. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» : указ

Президента України від 26 трав. 2015 р. № 287/2015. Верховна Рада України : [сайт]. URL: http://zakon3.rada.gov.ua/laws/show/287/2015.

119. Про Стратегію національної безпеки України : указ Президента України від 14 верес. 2020 р. № 392/2020. Президент України : [сайт]. URL : https://www.president.gov.ua/documents/3922020-35037.

120. Про схвалення Концепції створення державної системи захисту критичної інфраструктури [Електронний ресурс] : розпорядження Кабінету Міністрів України від 6 груд. 2017 р. № 1009-р. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/1009-2017-%D1%80

121. Проект Закону про критичну інфраструктуру та її захист // Верховна Рада України (офіційний веб-портал) [Електронний ресурс]. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996

122. Рогов М. А. Риск-менеджмент / М. А. Рогов. – М. : Финансы и статистика, 2001. – 120 с.

123. Саврас І. З. Статистичні методи в державному управлінні : навч. посіб. / І. З. Саврас. – Львів : ЛРІ НАДУ, 2010. – 132 с.

124. Самые громкие кибератаки на критические инфраструктуры [Електронний ресурс].– Режим доступу : https://habrahabr.ru/company/panda/blog

125. Скакун О.Ф. Теория государства и права : учебник. Харьков: Консум ; Ун-т внутр. дел, 2000. 704 с.

126. Словник української мови. Академічний тлумачний словник (1970–1980). Київ : Академічна думка. 1980. Т. 11. С. 686.

127. Стародуб Ю. П. Структура та методологія управління ризиками надзвичайних ситуацій природного та техногенного характеру / Ю. П. Стародуб, А. П. Гаврись, Я. І. Федюк // Управління проектами та розвиток виробництва : зб. наук. пр. – Луганськ : Вид-во СНУ ім. В. Даля, 2014. – № 1(49). – С. 25–32.

128. Стратегія забезпечення кібербезпеки в гібридній війні [Електронний ресурс]. – Режим доступу: //lexinform.com.ua/dumka-eksperta/strategiya-zabezpechennya-kiberbezpeky-v-gibrydnij-vijni/]

129. Стратегія кібербезпеки України: Указ Президента України від 15.03.2016 № 96/2016: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/96/2016

130. Стратегія розвитку інформаційного суспільства в Україні (Україна), 15.03.2013, № 386-р. Актуально на 28.03.2021. URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text

131. Сунгуровський М. Методологічний підхід до формування системи національної безпеки України / М. Сунгуровський // Стратегічна панорама. – 2001. – № 3–4. – С. 101–119.

132. Суходоля О. М. Захист критичної інфраструктури: сучасні виклики та пріоритетні завдання сектору безпеки. Науковий часопис, 2017. Вип. 1-2 (13-14). С. 50-80.

133. Теленик С. С. Правова природа щорічних Послань Президента України. Прикарпатський юридичний вісник. 2017. № 1, т. 4. С. 243–249.

134. Теленик С.С. Державна система захисту критичної інфраструктури України: концептуальні засади адміністративно-правового регулювання / С. Теленик // Херсон: Видавничий дім "Гельветика", 2020. – 602 с.

135. Теленик С.С. Критична інфраструктура як об’єкт адміністративно-правового регулювання. Юридичний часопис Національної академії внутрішніх справ. 2018. № 1(15). С. 179–188.

136. Теленик С.С. Правовий зміст поняття «критична інфраструктура». Jurnalul juridic national: teorie şi practică. 2019. № 6(40). С. 34–38.

137. Ткаченко В. Д., Ручкін Є. Б. Поняття правового регулювання. Загальна теорія держави і права : підручник / за ред. проф. М. В. Цвіка, доц. В. Д. Ткаченка, проф. О. В. Петришина. Харків, 2002. С. 404.

138. Указ Президента України “Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року №96/2016 “Про Стратегію кібербезпеки України”

139. Фурашев В. М. Національна безпека України: шляхи забезпечення, роль і місце суспільства. Євроатлантичний курс : монографія / В. М. Фурашев, С. Ф. Джердж. – К. : Синопсис, 2009. – 176 с.

140. Хартія про особливе партнерство між Україною та Організацією Північно-Атлантичного договору : підписана 09 лип. 1997 р. Голос України. 1997. № 127 (1627). 11 липня.

141. Цыгичко В.Н. Обеспечение безопасности критических инфраструктур США (аналитический обзор) / В.Н. Цыгичко, Г.Л. Смолян, Д.С. Черешкин // Труды Института системного анализа РАН. – М. : Институт системного анализа РАН, 2006. – № 27. – С. 4−34.

142. Чирва В. С. Безпека життєдіяльності : навч. посіб. / В. С. Чирва, Л. В. Баб’як. – Одеса : Глобус, 2005. – 412 с.

143. Шемшученко Ю. С., Бобровник С. В. Правове регулювання. Юридична енциклопедія : в 6 т. / [редкол.: Ю. С. Шемшученко (голова. редкол.) та ін.]. Київ, 2003. Т. 5. П–С. С. 40–41.

144. Шипілова Л. М. Порівняльний аналіз ключових понять і категорій основ національної безпеки України : автореф. дис. … канд. політ. наук : 21.01.01. Київ, 2007. 20 с.

145. Шпильовий І. М. Державне регулювання у сфері природно-техногенної безпеки України: автореф. дис.… канд. держ. упр. : 25.00.02 / І. М. Шпильовий ; НАДУ при Президентові України, К., 2008. – 20 с.

146. Bonin, S., Doktor, C., & Habegger, B. (2009). Risk Analysis. Integrated Risk Management and Societal Security. Focal Report 2. Center for Security Studies. Retrieved from http://hdl.handle.net/20.500.11850/18960

147. Commission of the European Communities. Communication from the commission on a European Programme for Critical Infrastructure Protection.

Brussels, 12.12.2006. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

148. 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. (2008). European Council. Official Journal of the European Union, L 345, 75–80. Retrieved from https://publications.europa.eu/en/publication-detail/-/publication/ba51b03f-66f4-4807-bf7d-c66244414b10.

149. Critical Infrastructure Resilience Strategy: Australian Government. (2010). Retrieved from https://publications.europa.eu/en/publication-detail/-/publication/ba51b03f-66f4-4807-bf7d-c66244414b10.

150. 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.

151. Dimitris Gritzalis, Marianthi Theocharidou, George Stergiopoulos Critical Infrastructure Security and Resilience. Theories, Methods, Tools and Technologies. Springer Nature Switzerland AG 2019. 313 p.

152. Green Paper on a European Programme for Critical Infrastructure Protection: European Commission, 2006. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN

153. Moteff, J. (2004). Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a454038.pdf

154. Public Private Partnerships. Construction, Protection and Rehabilitation of Critical Infrastructure. Ed. by Robert M. Clark, Simon Hakim. Springer Nature Switzerland AG 2019. 302 p.

155. The national infrastructure: веб-сайт. URL: http://www.cpni.gov.uk

156. Training critical infrastructure protection. URL: https://www.google.com/search?q=training+critical+infrastructure+protection&oq

=training+critical+infrastructure+protection&aqs=chrome..69i57j0i22i30j69i60j69i61l2.3055j0j15&sourceid=chrome&ie=UTF-8.

157. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (PATRIOT ACT): Department of Justice or the USA. Retrieved from http://frwebgate.access.gpo.gov.

158. USA Patriot Act of 2001: веб-сайт. URL: https://www.gpo.gov/fdsys/pkg/BILLS107hr3162enr/pdf/BILLS107hr3162enr.pdf