МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет права, публічного управління та національної безпеки
Кафедра економічної теорії, інтелектуальної власності та публічного управління

Кваліфікаційна робота
на правах рукопису

НИКИТОВИЧ ІВАН ІГОРОВИЧ
(прізвище, ім'я, по батькові здобувача вищої освіти)

УДК 351: 65.012.8
(індекс)

КВАЛІФІКАЦІЙНА РОБОТА

УПРАВЛІННЯ БЕЗПЕКОЮ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

(тема роботи)

281 «Публічне управління та адміністрування»
(шифр і назва спеціальності)

Подається на здобуття освітнього ступеня бакалавр кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

І. І.НИКИТОВИЧ

Керівник роботи
ДОВЖЕНКО Валентина Анатоліївна
(прізвище, ім'я, по батькові)

кандидат економічних наук, доцент
(науковий ступінь, вчене звання)

Житомир – 2024

Висновок кафедри економічної теорії, інтелектуальної власності та публічного управління
за результатами попереднього захисту: **НИКИТОВИЧ Іван Ігорович** допущений до захисту

Протокол засідання кафедри економічної теорії, інтелектуальної власності та публічного управління № ____ від «____» травня 2024 р.

Завідувач кафедри економічної теорії, інтелектуальної власності та публічного управління
к.е.н., професор _____ Валентина ЯКОБЧУК
(науковий ступінь, вчене звання) (підпис) (власне ім'я та прізвище)

«___»травня 2024 р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти **НИКИТОВИЧ Іван Ігорович** захистив
(прізвище, ім'я, по батькові)

кваліфікаційну роботу з оцінкою:

сума балів за 100-бальною шкалою _____
за національною шкалою _____

Секретар ЕК
_____-_____ _____ Настасія ПУГАЧОВА
(науковий ступінь, вчене звання) (підпис) (власне ім'я та прізвище)

АНОТАЦІЯ

НИКИТОВИЧ І. І. Управління безпекою об’єктами критичної інфраструктури – Кваліфікаційна робота на правах рукопису. Кваліфікаційна робота на здобуття освітнього ступеня бакалавра за спеціальністю 281 «Публічне управління та адміністрування» – Поліський національний університет, Житомир, 2024.

Кваліфікаційна робота присвячена дослідженню системи управління безпекою об’єктів критичної інфраструктури з метою забезпечення їхньої надійної та безперебійної роботи. Критична інфраструктура включає в себе об'єкти та системи, які мають важливе значення для національної безпеки, економіки, охорони здоров'я та суспільного благополуччя.

Ключові слова: критична інфраструктура, управління безпекою, захист об’єктів, ризик-менеджмент, надзвичайні ситуації, кібербезпека, нормативно-правова база, технологічні рішення, інфраструктурні загрози, системи захисту

SUMMARY

NYKYTOVYCH I. Management of Security for Critical Infrastructure Objects – Qualification Work as a Manuscript. Qualification work for obtaining a Bachelor's degree in specialty 281 "Public Administration and Administration" – Polissia National University, Zhytomyr, 2024.

This qualification work is dedicated to the study of the security management system of critical infrastructure objects to ensure their reliable and uninterrupted operation. Critical infrastructure includes objects and systems that are of vital importance for national security, the economy, healthcare, and public welfare.

Keywords: Critical infrastructure, security management, object protection, risk management, emergency situations, cybersecurity, regulatory framework, technological solutions, infrastructure threats, protection systems.

ЗМІСТ

ВСТУП

Актуальність теми. Нині Україна має один із найсерйозніших безпекових викликів за часи свого становлення та розбудови незалежності. Країна зіштовхнулась з кібератаками на інформаційну інфраструктуру, а також руйнуваннями інфраструктурних об’єктів тепло-, енерго-, водопостачання та загрозою пошкодження об’єктів атомної промисловості внаслідок бомбардувань в ході війни Росії проти України. В цих умовах повинна забезпечуватися безпека держави, суспільства, різноманітних інституцій, а також звичайних громадян України. Зазначені чинники обумовлюють необхідність впровадження в Україні такого поняття як «захист критичної інфраструктури», та розробки дієвих інструментів реалізації політики безпеки.

Наукові дослідження окремих питань безпеки об’єктів критичної інфраструктури розкрито в роботах таких науковців, як: Д. С. Бірюков, Д. Г. Бобро, М. Б. Домарацький, Г. Ю. Зубко та ін. Проблеми зарубіжного досвіду захисту об’єктів критичної інфраструктури висвітлено у працях таких дослідників, як: І. В. Гора та О. В. Батюк, О. П. Єрменчук, Г. Ю. Зубко, Н. О. Кідалова, І. Манжул та ін. Щодо управління безпекою об’єктів критичної інфраструктури в Україні, дане питання розглядалося у роботах Б. В. Богдана, О. Верголяса, В. О. Євсєєва, О. П. Єрменчук, Г. Ю. Зубко, В. В. Косинського, В. В. Крикун, О. Мельничук, О. М. Суходолі, С. С. Теленика та ін. Водночас, залишається ряд невирішених проблем у даній сфері, що потребують подальших наукових досліджень.

Мета дослідження полягає в обґрунтуванні напрямів вирішення актуальних проблем у сфері управління безпекою об’єктів критичної інфраструктури.

Завдання дослідження:

- розкрити сутність поняття критичної інфраструктури, класифікацію об’єктів критичної інфраструктури;

- визначити організаційно-правові засади управління безпекою об’єктів критичної інфраструктури в Україні;

- ідентифікувати проблемні аспекти управління безпекою об’єктів критичної інфраструктури в Україні;

- запропонувати можливі напрями та шляхи вдосконалення управління безпекою об’єктів критичної інфраструктури в Україні.

Об’єктом дослідження є процес управління безпекою об’єктів критичної інфраструктури. *Предметом дослідження* є теоретико-організаційні аспекти управління безпекою об’єктів критичної інфраструктури

Методи дослідження. Для того, щоб вирішити поставлені завдання, використовувалися загальнонаукові та спеціально-наукові методи пізнання. Зокрема, застосовано діалектичні методи пізнання (абстрагування, виявлення співвідношення загального, особливого та одиничного, а також частини й цілого), метод системного аналізу, формально-логічний та формально-юридичний методи. Застосовувались методи класифікації та систематизації для узагальнення законодавчої, нормативної документації та наукової літератури за темою дослідження. Застосування історико-правового методу дозволило проаналізувати ґенезу становлення підходів щодо визначення поняття критичної інфраструктури та її об’єктів у науковій літературі та нормативно-правових актах. Визначення та характеристика класифікації об’єктів критичної інфраструктури, а також суб’єктів захисту безпеки об’єктів критичної інфраструктури в Україні проводилися із застосуванням формально-логічного методу і методу системно-структурного аналізу.

Аналіз зарубіжного досвіду управління безпекою об’єктів критичної інфраструктури з метою вдосконалення управління безпекою об’єктів критичної інфраструктури в Україні проведено із використанням порівняльно-правового методу. Крім того, використовувались методи аналізу, синтезу, індукції, дедукції, аналогії, єдності історичного та логічного, органічної єдності теорії та практики.

*Інформаційну базу дослідження с*клали Конституція України, нормативно-правові акти України (Закони, Укази Президента України, Постанови Кабінету Міністрів України тощо), міжнародне законодавство та законодавство зарубіжних країн, публікації науковців та інформаційні джерела (інтернет-ресурси) за темою даного дослідження.

Елемент наукової новизни дослідження полягає у тому, що дане дослідження є комплексним теоретико-правовим аналізом основ та підходів до управління безпекою об'єктів критичної інфраструктури, що проводився на основі нового вітчизняного законодавства у сфері управління безпекою об'єктів критичної інфраструктури та із порівняльним аналізом зарубіжного досвіду у даній сфері.

Практичне значення результатів дослідження. Результати дослідження, а також запропоновані в ньому рекомендації щодо вдосконалення управління безпекою об'єктів критичної інфраструктури в Україні, можуть бути використанні при розробці стратегії та державної політики у сфері формування безпеки об'єктів критичної інфраструктури в Україні, як складової національної безпеки.

Структура роботи обумовлена поставленою метою та завданнями. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел, що налічують 45 найменувань. Загальний обсяг роботи – 33 сторінки.

РОЗДІЛ 1
ЗАГАЛЬНА ХАРАКТЕРИСТИКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Поняття критичної інфраструктури як об'єкту державного управління

Поняття «інфраструктура» має латинське походження, звідки воно розповсюдилося у більшості європейських мов у розумінні «сукупності споруд, будівель, систем і служб, необхідних для функціонування галузей матеріального виробництва та забезпечення життєдіяльності суспільства». Міською інфраструктурою називають певну сукупність споруд, будівель і служб, які необхідні для функціонування міста. Її поділяють на кілька систем: комунальну (об'єкти водовідведення та водопостачання, теплопостачання, енергетичне споживання, газопостачання, зв'язок, гідротехнічні споруди), транспортну, соціальну та рекреаційну [11, с. 10]. Розрізняють також соціальну, виробничо-економічну, ринково-інституційну, інноваційну, транспортну та рекреаційну інфраструктуру [8, с. 65-66].

Відповідно до Академічного тлумачного словника української мови, під інфраструктурою розуміється певна структура, яка охоплює сукупність галузей і видів діяльності (виробничих та невиробничих), якою забезпечуються умови відтворення та надання послуг у різних сферах суспільного життя [16, с. 6; 6, с. 120]. Проте у наведеній дефініції є й дискусійні, подекуди навіть спірні моменти. Зокрема, багато експертів звертають увагу на те, що зведення інфраструктури до сфери послуг звужує діапазон функціонування даного поняття . Крім цього, наголошується на відсутність розуміння інформаційної інфраструктури .

Питання захисту критичних, тобто таких, які мали значний вплив на функціонування та розвиток країн, об'єктів інфраструктури постало разом із

виникненням перших джержавоподібних утворень. Насамперед, це стосувалося військової загрози

Критична інфраструктура містить значну кількість об’єктів. Об’єкти критичної інфраструктури визначено як стратегічно важливі підприємства та установи, які необхідні для забезпечення життєдіяльності суспільства та функціонування економіки країни. Їх незапланована зупинка, виведення з ладу чи повне руйнування здатні становити загрозу для національної безпеки, природного середовища, спричинити погіршення оборонної здатності, матеріальні та фінансові збитків чи навіть призвести до людських жертв.

Закон України «Про критичну інфраструктуру» визначає об’єкти критичної інфраструктури як «об’єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам» [10].

У літературі зустрічаються класифікації об’єктів критичної інфраструктури за певними ознаками.

Так, за ієрархічним рівнем управління (який використовують для окремої країни) виділяють: національні, регіональні, локальні об’єкти критичної інфраструктури.

За масштабом (за географією охоплення території внаслідок аварії або втрати елементу критичної інфраструктури) такі об’єкти поділяють на: глобальні, міжнародні, національні, регіональні, локальні.

За формою власності визначають: об’єкти національної критичної інфраструктури (державної власності); об’єкти регіональної та локальної критичної інфраструктури (державної, комунальної, приватної власності) [3, с.37].

Класифікація об’єктів критичної інфраструктури за тяжкістю можливих наслідків за показниками виглядає наступним чином:

- економічні наслідки: розмір прямих і непрямих економічних втрат (частини ВВП, частки ринку, кількості робочих місць, податкових надходжень

у бюджет, значні витрати на підсилення роботи аварійно-рятувальних служб та екстреної допомоги населенню).

- соціальні втрати: порушення безпеки життєдіяльності та здоров'я населення (кількість загиблих і постраждалих, кількість евакуйованого і переселеного населення, кількість населення, яке потерпає від порушення умов життєзабезпечення),

- безпека держави: втрата авторитету держави, порушення управління державою, зниження обороноздатності,

- екологічні наслідки: екологічні аварії та катастрофи, які чинять негативний вплив на навколишнє природне середовище [10].

За тривалістю часу, який потрібен для відновлення об'єктів критичної інфраструктури після негативного впливу на них: довготривале, середньотривале і швидкотривале відновлення [7].

За вразливістю об'єкта до впливу небезпечних чинників відповідно визначають: високу, середню і низьку ступінь вразливості [8, с. 96].

За термінами відновлювальних робіт: для національної критичної інфраструктури: - до шести годин, для регіональної критичної інфраструктури - до 12 годин, для локальної та об'єктної критичної інфраструктури - до 24-х годин [10, с. 427].

Об'єкти критичної інфраструктури в світі прийнято групувати за окремими секторами. Водночас кількість секторів і принципи групування є досить різними в кожній країні.

1.2. Суб'єкти захисту безпеки об'єктів критичної інфраструктури в Україні

Правове забезпечення безпеки критичної інфраструктури можна визначити як діяльність із забезпечення безпеки, захисту та охорони об'єктів критичної інфраструктури уповноваженими суб'єктами [14, с. 90-91].

До прийняття Закону України «Про критичну інфраструктуру» відповідальними за функціонування і захист системи критичної інфраструктури було визначено такі органи державної влади: Національна комісія з питань захисту критичної інфраструктури, Національна гвардія, Національна поліція, Служба безпеки України, Антитерористичний центр при Службі безпеки України, Генеральний штаб Збройних Сил України, Державна прикордонна служба, Державна служба із надзвичайних ситуацій, Державна інспекція ядерного регулювання України, Державна служба спеціального зв'язку та захисту інформації [17, с. 157].

Відповідно до ст. 14 Закону України «Про критичну інфраструктуру», до системи суб'єктів, уповноважених забезпечувати безпеку, здійснювати захист та оборону критичної інфраструктури, віднесено:

1) Кабінет Міністрів України,

2) Раду національної безпеки і оборони України,

3) Центральну виборчу комісію,

4) Національний банк України,

5) Національні комісії (з цінних паперів та фондового ринку, державного регулювання у сфері зв'язку та інформатизації, а також у сферах енергетики та комунальних послуг,

6) Адміністрацію Державної служби спеціального зв'язку та захисту інформації України,

7) Фонд державного майна України і інші центральні органи виконавчої влади зі спеціальним статусом,

8) уповноважений орган у сфері захисту критичної інфраструктури України – Держспецзв'язку,

9) Державну службу України з надзвичайних ситуацій,

10) секторальні та функціональні органи та інші міністерства і центральні органи виконавчої влади,

11) Службу безпеки України,

12) правоохоронні та розвідувальні органи, суб'єктів оперативно-розшукової та контррозвідувальної діяльності,

13) Збройні Сили України та інші військові формування,

14) місцеві органи виконавчої влади (військово-цивільні адміністрації),

15) органи місцевого самоврядування,

16) операторів критичної інфраструктури,

17) підприємства, установи та організації, що здійснюють діяльність у сфері забезпеченням безпеки та стійкості критичної інфраструктури [10].

Основним суб'єктом, що здійснює формування, а також реалізує державну політику у сфері захисту критичної інфраструктури, є Кабінет Міністрів України.

Крім того, дана політика реалізується відповідною діяльністю секторальних та функціональних органів, а також Уповноваженим органом у сфері захисту критичної інфраструктури України.

Відповідно до Закону України «Про критичну інфраструктуру», до секторальних органів у сфері захисту критичної інфраструктури віднесено:

- Національний банк України (визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України (на базі центру кіберзахисту НБУ),

- Службу безпеки України (відповідно до ст. 19 Закону України «Про національну безпеку України», Закону України «Про Службу безпеки України» [17], здійснює контррозвідувальний захист об'єктів критичної інфраструктури, зокрема в інформаційній сфері) [16]),

- Національну гвардію України (здійснює охорону об'єктів критичної інфраструктури, бере участь у ліквідації наслідків кризових ситуацій на об'єктах критичної інфраструктури, проводить контрдиверсійну діяльність щодо захисту критичної інфраструктури),

- Національну поліцію України (виконує обов'язок щодо планування заходів у сфері забезпечення стійкості та захисту об'єктів критичної інфраструктури, відновлення функціонування відповідних об'єктів;

припинення протиправних дій проти об’єктів критичної інфраструктури; підтримання або відновлення правопорядку в місцях розташування об’єктів критичної інфраструктури у разі виникнення кризових ситуацій; здійснення охорони об’єктів критичної інфраструктури на договірних засадах тощо),

- Збройні Сили України,

- Державну спеціальну службу транспорту [14, с. 357-358].

Крім того, відповідно до Постанови № 1109 до даного переліку, крім вищезазначених органі, слід додати: ДСНС (територіальні органи та підрозділи ДСНС України в межах своєї території та відповідно до своїх обов’язків оперативно повинні реагувати на виклики та ризики щодо захисту об’єктів критичної інфраструктури, здійснювати заходи із запобігання, виявлення та припинення терористичної діяльності на об’єктах ДСНС України, а також брати участь в ліквідації наслідків терористичних актів [17, с. 40]); МВС (Міністр внутрішніх справ, зокрема, координує роботу підрозділів ДСНС щодо питань захисту об’єктів критичної інфраструктури); Мінекономіки; Міненерго; Мінінфраструктури; Міноборони; Мінцифри; Мінфін; МОЗ; НСЗУ.

Усі зазначені секторальні органи підзвітні уповноваженому органу у сфері захисту критичної інфраструктури України. До повноважень функціональних органів у сфері захисту критичної інфраструктури, окрім зазначених вище, зокрема, віднесено:

- формування переліку об’єктів критичної інфраструктури, які віднесено до їх сфери управління;

- надання власникам та операторам інфраструктури консультацій щодо ризиків і загроз критичній інфраструктурі та заходів щодо їх нейтралізації;

- організацію та проведення оцінки загрози та ризиків критичній інфраструктурі у відповідних сферах;

- здійснення моніторингу рівня безпеки об’єктів критичної інфраструктури у відповідних сферах.

Постановою КМУ від 12.07.2022 № 787 «Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної

системи стійкості України» [34] було створено Уповноважений орган у сфері захисту критичної інфраструктури – Державну службу захисту критичної інфраструктури та забезпечення національної системи стійкості України (ДЗКІ). Уповноважений орган у сфері захисту критичної інфраструктури України відповідає за координацію діяльності суб'єктів національної системи захисту критичної інфраструктури у мирний час.

Після масивних ракетних атак РФ, спрямованих на об'єкти критичної інфраструктури України восени 2022 року, було прийнято Закон України «Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України» від 18.10.2022 р. [5], яким було внесено зміни до статусного Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» [7].

Відповідно до внесених змін Державна служба спеціального зв'язку та захисту інформації України наділена повноваженнями Уповноваженого органу у сфері захисту критичної інфраструктури України під час дії правового режиму воєнного стану та протягом 12 місяців після його припинення чи скасування [7].

Однією з найважливіших сфер, у межах якої функціонують об'єкти критичної інфраструктури, є життєзабезпечення населення. З огляду на таке, до суб'єктів захисту об'єктів критичної інфраструктури вітчизняним законодавцем віднесено органи місцевого самоврядування, які здійснюють такий захист на місцевому рівні [10, с .28]. Дана діяльність, відповідно до п. 23 ч. 1 ст. 26 Закону України «Про місцеве самоврядування» [11], є виключною компетенцією місцевих рад. Загалом діяльність органів місцевого самоврядування із захисту об'єктів критичної інфраструктури охоплює фінансове забезпечення об'єктів критичної інфраструктури, а також їх захист. Відповідно до ч. ч. 4, 5 ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України», органи місцевого самоврядування відповідають за процеси здійснення кіберзахисту об'єктів критичної інфраструктури.

Законом України «Про правовий режим воєнного стану», на територіях, де введено воєнний стан, повноваження щодо захисту критичної інфраструктури покладено на тимчасові державні органи – військові адміністрації, підзвітні обласним військовим або державним адміністраціям, Генеральному штабу Збройних Сил України та Кабінету Міністрів України (у межах їх повноважень у даній сфері, визначених законодавством).

Законом України «Про критичну інфраструктуру» операторами критичної інфраструктури визначено юридичних або фізичних осіб-підприємців, діяльність яких пов’язана із використанням та управлінням об’єкту критичної інфраструктури. До основних функціональних обов’язків операторів критичної інфраструктури віднесено, насамперед, забезпечення захисту об’єктів критичної інфраструктури (шляхом здійснення відповідних заходів та страхуванням таких об’єктів від можливих ризиків). При цьому, це стосується і об’єктів критичної інформаційної інфраструктури.

По-друге, оператори здійснюють свої повноваження у зазначеній сфері у співпраці із відповідними секторальними та функціональними органами. Така співпраця полягає в інформуванні операторами даних органів про інциденти, що сталися на об’єктах критичної інфраструктури, якими оператори керують.

Щодо забезпечення безпеки критичної інформаційної інфраструктури (кібербезпеки), відповідно до ч. 1 ст. 5 Закону України “Про основні засади кібербезпеки України”, повноваження із координації даної діяльності покладено на Президента України. Крім того, Президент України, як Голова РНБО України, здійснює дану діяльність у сфері кібербезпеки, як складової національної безпеки України.

Реалізацію із заходів кібербезпеки, відповідно до рішення РНБО України "Про невідкладні заходи з кібероборони держави” від 14 травня 2021 р. (введено в дію Указом Президента України від 26.08.2021 р. № 447) , здійснюють кібервійська, створення у системі Міністерства оборони України.

Слід також вказати на те, що система захисту критичної інфраструктури в Україні взаємодіє з іншими системами захисту у сфері національної безпеки

України (щодо боротьби з тероризмом, захисту інформаційних ресурсів в інформаційно-телекомунікаційних системах, протидії злочинності, забезпечення державної безпеки, цивільного захисту, а також системами організації повітряного руху України, енергобезпеки та ядерної безпеки, захисту персональних даних тощо).

Також, відповідно до ст.31 Закону України «Про критичну інфраструктуру», Україна співпрацює у сфері захисту критичної інфраструктури з іноземними державами, їх правоохоронними органами і спеціальними службами. Крім того, у зазначеній сфері Україна взаємодіє із міжнародними організаціями, діяльність яких пов’язана із протидією міжнародній злочинності та тероризму.

ВИСНОВКИ ДО РОЗДІЛУ 1

Отже, критична інфраструктура включає об'єкти та системи, що мають стратегічне значення для національної безпеки, економічної стабільності, охорони здоров'я та суспільного добробуту. Об’єкти критичної інфраструктури в світі прийнято групувати за секторами.

Суб’єкти безпекового середовища об’єктів критичної інфраструктури в Україні є органи державної влади різних рівнів. Основним суб’єктом, що формує та відповідає за реалізацію публічної політики у сфері захисту критичної інфраструктури, є Кабінет Міністрів України. Також певні функції у цій сфері виконують секторальні органи, що відносяться до сфери захисту критичної інфраструктури. Таку ж функцію здійснюють органи місцевого самоврядування. Система безпекового середовища критичної інфраструктури в Україні взаємодіє з іншими системами захисту у сфері національної безпеки України

РОЗДІЛ 2.
АНАЛІЗ ОРГАНІЗАЦІЙНО-ПРАВОВОГО МЕХАНІЗМУ ДЕРЖАВНОГО УПРАВЛІННЯ ЗАХИСТОМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

2.1. Правове регулювання та організаційні засади управління безпекою об’єктів критичної інфраструктури в Україні

Безпека (лат. Securitas – без турботи, страху) є однією з якісних ознак розвитку будь-якого суспільства [11, с. 96].

У минулому основним завданням безпеки було забезпечення захисту території держави від іноземного вторгнення чи політичного залякування [14, с.143]. Сучасні дослідники визначають безпеку як стан захищеності конкретного соціального об’єкта: держави, суспільства, особистості (людини і громадянина). При цьому захист усіх зазначених об’єктів сьогодні охоплюється категорією національної безпеки [24, с. 62].

Здебільшого у вітчизняній та зарубіжній літературі національна безпека розуміється як здатність особи, суспільства, і держави до захисту та їх захищеність від сукупності об'єктивно існуючи негативних факторів, які створюють реальну небезпеку національним інтересам країни [7, с. 36].

Аналіз фундаментальних постулатів Закону України «Про національну безпеку України» [12] дає підстави стверджувати, що національна безпеку визначає баланс трьох складових: життєво важливих національних інтересів, загроз і захисту. При цьому до життєво важливих національних інтересів держави М. Б. Домарецький відносить саме забезпечення захисту населення об’єктів критичної інфраструктури в умовах надзвичайних ситуацій, терористичних актів, війни [14,с.83].

З огляду на п. 4 ст. 3 Закону України «Про національну безпеку України» та Стратегії забезпечення державної безпеки (Указ Президента України від 16.02.2022 р. № 56/20), об’єкти критичної інфраструктури віднесено до об’єктів

державної безпеки [25], а виходячи з розуміння безпеки об’єкта критичної інфраструктури, що містяться у тексті Постанови Кабінету Міністрів України № 943 від 9 жовтня 2020 р. [33], критичну інфраструктуру та її об’єкти можна віднести до складової національної безпеки, яка потребує захисту з огляду на її важливе значення для сталого функціонування та неухильного прогресу країни.

До прийняття Закону України «Про критичну інфраструктуру» правове регулювання забезпечення безпеки здійснювалося такими нормативними актами, як Указ Президента України «Про Стратегію національної безпеки України» від 12.02.2007 р. № 105/2007 [31], Рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України» від 06.05.2015 р., Концепція створення державної системи захисту критичної інфраструктури (Розпорядження Кабінету Міністрів України № 1009-р від 06.12.2017 р.), Кодекс цивільного захисту України [3], Законами України «Про національну безпеку України», «Про основні засади забезпечення кібербезпеки України», «Про боротьбу з тероризмом» [4], «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» [18], «Про правовий режим надзвичайного стану» [16], «Про правовий режим воєнного стану» [15], Постановою КМУ «Деякі питання об’єктів критичної інфраструктури» від 09.10.2020 р. № 1109 та ін. Проте зазначені нормативні акти дозволяли врегулювати ситуації лише відносно окремих категорій об’єктів критичної інфраструктури [17, с. 32].

Важливим нормативним актом в сфері захисту об’єктів критичної інфраструктури є Стратегія національної безпеки України 2020 року [29], в якій прямо йде мова про створення державою ефективної системи безпеки та стійкості критичної інфраструктури.

На сучасному етапі законодавство про критичну інфраструктуру та її захист в Україні складають:

- Конституція України [1],
- Закон України «Про критичну інфраструктуру» від 16.11.2021 р. № 1882 IX,

- інші закони України,

- міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України,

- інші нормативно-правові акти у зазначеній сфері.

Вітчизняні учені захист критичної інфраструктури визначають як «комплекс заходів, реалізований у нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури. Цю позицію відстоює у своїх працях і С. С. Теленик [24, с. 66].

Дане визначення фактично збігається із розумінням захисту критичної інфраструктури, викладеним у Законі України «Про критичну інфраструктуру», у ст. 1 якого надаються визначення безпеки та захисту критичної інфраструктури, а також охорони її об'єктів. Так, безпека критичної інфраструктури у зазначеному нормативному акті визначається як забезпечення безперервної функціональності, цілісності, стійкості та відновлюваності критичної інфраструктури.

Закон України «Про критичну інфраструктуру» регламентує захист критичної інфраструктури у якості складової частини забезпечення національної безпеки України. Такий захист передбачає діяльність із своєчасного виявлення, запобігання і нейтралізації загроз безпеці об'єктів критичної інфраструктури, а також мінімізації та ліквідації наслідків, спричинених даними загрозами. Щодо охорони об'єктів критичної інфраструктури, нею визначено комплекс певних заходів захисту критичної інфраструктури, що здійснюється уповноваженими суб'єктами [10].

За сучасної ситуації повномасштабного збройного конфлікту в Україні, на нашу думку, даний Закон слід вважати ключовим нормативно-правовим актом. Цей документ становить основу в концепції публічної політики у сфері захисту критичної інфраструктури, як у мирний час, так і в умовах військового стану.

Крім того, захист та правовий режим об’єктів критичної інфраструктури в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, особливого періоду, сьогодні регулюються Законами України "Про правовий режим воєнного стану", "Про правовий режим надзвичайного стану", "Про функціонування єдиної транспортної системи України в особливий період"[19] та "Про оборону України" [13]. До складових національної безпеки відносять, зокрема, оборону та воєнну безпеку.

Загальновизнаним є підхід, за яким оборона розглядається в аспекті державної діяльності. При цьому саме оборона є одним з основних засобів забезпечення національної безпеки держави, особливо в умовах надзвичайного та воєнного стану.

Щодо воєнної безпеки, порівняно з обороною дане явище є більш складним, комплексним за своєю природою. Воно включає багато аспектів (реалізацію різних заходів у політичній, економічній та інших сферах суспільного життя) в умовах воєнного стану.

Воєнний стан в Україні введено у зв’язку з військовою агресією Російської Федерації відповідно до п. 20 ч. 1 ст. 106 Конституції України та Закону України «Про правовий режим воєнного стану» 24 лютого 2022 року [20].

Варто зазначити, що прояви російського військового вторгнення систематично порушують міжнародні нормативно-правові акти, у тому числі й у сфері захисту критичної інфраструктури. Так, частина об’єктів критичної інфраструктури в умовах війни знаходиться під захистом Додаткового протоколу до Женевських конвенцій від 12 серпня 1949 року. У документі відсутнє саме формулювання терміну «критична інфраструктура», однак зазначається, що «будь які цивільні об’єкти не повинні бути об’єктом нападу або репресалій» [2]. Відповідно, можна зробити висновок, що об’єкти критичної інфраструктури підпадають під дію даного документу, оскільки вони не відносяться до військових об’єктів.

Окремий пункт Указу Президента України від 26 травня 2020 р. № 203/2020 стосується питань функціонування системи захисту критичної інфраструктури. Наголошено на необхідності: формування принципів класифікації об'єктів критичної інфраструктури; створення системи координації та контролю функціонування системи захисту критичної інфраструктури; на завданнях, виконання яких позитивно вплине на підвищення рівня стійкості національної критичної інфраструктури до всього спектра загроз.

Організаційні засади управління безпекою об'єктів критичної інфраструктури в Україні полягають у:

- визначенні об'єктів як таких, що відносяться до критичної інфраструктури (відповідно до порядку, встановленого Кабінетом Міністрів України),

- внесенні даних об'єктів секторальними органами у сфері захисту критичної інфраструктури до Реєстру об'єктів критичної інфраструктури (формується та ведеться Уповноваженим органом у сфері захисту критичної інфраструктури України). Порядок ведення Реєстру, включення до нього об'єктів, доступу та надання інформації про об'єкти визначається Кабінетом Міністрів України [16],

- повідомленні про включення об'єкта до Реєстру секторальними органами у сфері захисту критичної інфраструктури оператора даного об'єкта з метою подальшої паспортизації ним такого об'єкта,

- процедурі паспортизації об'єктів критичної інфраструктури [16].

Паспорти об'єктів критичної інфраструктури готуються операторами, погоджуються секторальними або функціональними органами у сфері захисту критичної інфраструктури відповідно до Порядку, встановленого Національним банком України та Кабінетом Міністрів України [10].

У відповідності до ст. 7 Закону України «Про критичну інфраструктуру», державне управління національною системою захисту та формування безпеки об'єктів критичної інфраструктури відбувається на різних рівнях.

Так, на загальнодержавному рівні повноваженнями з управління національною системою захисту критичної інфраструктури наділено Кабінет Міністрів України, Національний банк України, Уповноважений орган у сфері захисту критичної інфраструктури України, центральні органи виконавчої влади, інші державні органи.

2.2. Ідентифікація проблем в системі публічного управління безпекою об’єктів критичної інфраструктури

В Україні вироблено досить розгалужену систему правового регулювання забезпечення захисту об’єктів критичної інфраструктури. Втім, варто наголосити на відсутності системного підходу щодо даного питання.

По-перше, слід зазначити, що дієва узгоджена державна політика у цій сфері тільки-но починає розроблятися.

Крім того, на нормативному рівні вироблено загальний механізм управління захистом та формування безпеки таких об’єктів, проте ще його не опрацьовано належним чином.

В Україні до сьогодні діє збалансована система управління техногенною безпекою об’єктів підвищеної небезпеки, розроблена ще у радянські час. Проте, такої системи управління щодо об’єктів критичної інфраструктури та аналізу загроз щодо таких об’єктів в умовах воєнного конфлікту немає [13, с. 37]. Певні проблеми мають місце і в законодавчій невизначеності форм взаємодії державних органів у даній сфері [12, с. 120]. Зокрема, це стосується державно-приватного партнерства, яке, з огляду на зарубіжний досвід, може вважатися одним з пріоритетних напрямів такої діяльності [27, с. 54]. Також не вироблено і єдиного підходу щодо координації заходів із захисту на рівні міністерств та інших центральних органів виконавчої влади .

Отже, Закон України “Про критичну інфраструктуру», не зважаючи на свій прогресивний характер, потребує подальшого вдосконалення.

Сучасний стан системи такої складової безпеки як інформаційна безпека України характеризується посиленням вже наявних загроз, проте досить часто з'являються нові виклики. Специфічні умови та динаміку інформаційної війни на сучасному етапі визначає поєднання та координація таких груп чинників: організаційні, технологічні, доктринальні, політичні і соціальні.

Від початку російсько-українського конфлікту в системі інституційного механізму інформаційної безпеки України було вжито певних реорганізаційних заходів зі зміцнення спроможності держави протистояти ворожим інформаційним впливам [13, с. 700]. Втім, сам процес реорганізації інституційного механізму не набув завершеного характеру.

Особливої уваги на сучасному етапі за умови повномасштабного вторгнення потребує забезпечення кібербезпеки як елемента протидії бойового застосування кібератак [13]. Основною проблемою у даній сфері є відсутність в Україні кваліфікованих та досвідчених фахівців з інформаційної безпеки та кібербезпеки, зокрема, - з причини браку практичних навичок.

Необхідність підготовки спеціалістів із захисту критичної інфраструктури добре усвідомлюється в розвинутих країнах світу. Владні органи зазвичай приділяють важливу увагу процесам навчання та підготовки фахівців у сфері формування безпекового середовища для критичної інфраструктури.

Так, наприклад у Франції питаннями планування безпекових заходів, навчання та розробки технологій безпеки, в тому числі стосовно сфери захисту критичної інфраструктури, займається підрозділ з державного захисту та безпеки (англ., State Protection and Security – PSE) при Генеральному секретаріаті з питань оборони та національної безпеки (фр., Secrétariat Général de la Défense et de la Sécurité Nationale, SGDSN) [36, 37].

В Іспанії питання навчання персоналу з питань безпеки критичної інфраструктури покладено на Національний криптологічний центр (CCN), який є важливим підрозділом для захисту критичної інфраструктури у складі Національного центру розвідки (ісп., Centro Nacional de Inteligencia, CNI), що

створений в 2002 році як національний розвідувальний та контррозвідувальний орган [36, 37].

ВИСНОВКИ ДО РОЗДІЛУ 2

Отже, в Україні існує комплексна нормативно-правова база, яка регулює питання захисту критичної інфраструктури. Основними документами, що визначають цей механізм, є закони України, постанови Кабінету Міністрів, а також нормативні акти профільних міністерств та відомств. Для реалізації державної політики у сфері захисту критичної інфраструктури функціонують різні інститути та органи влади, зокрема Міністерство внутрішніх справ, Служба безпеки України, Державна служба з надзвичайних ситуацій та інші.

Україна активно співпрацює з міжнародними організаціями та державами-партнерами у сфері захисту критичної інфраструктури. Це включає участь у міжнародних проектах, обмін досвідом та впровадження міжнародних стандартів.

Незважаючи на наявність законодавчої бази, існують певні вразливості та виклики у сфері захисту критичної інфраструктури. Це включає недостатню координацію між різними органами влади, обмеженість фінансових ресурсів та необхідність оновлення та вдосконалення правових норм з урахуванням сучасних загроз.

РОЗДІЛ 3.
ОБҐРУНТУВАННЯ ПРОПОЗИЦІЙ ЩОДО ВИРІШЕННЯ ПРОБЛЕМ УПРАВЛІННЯ БЕЗПЕКОЮ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

3.1. Зарубіжний досвід управління безпекою об'єктів критичної інфраструктури

Першою європейською країною, яка встановила проблему захисту критичної інфраструктури як основну проблему національної безпеки, стала Велика Британія. У 1999 р. у законодавстві даної держави було закріплено основні параметри критичної інфраструктури. Більш того, було визначено систему державних органів, відповідальних за захист об'єктів критичної інфраструктури. У подальшому таке законодавство було прийнято на рівні усіх країн-членів ЄС. А у жовтні 2004 р. Європейською комісією було розроблено загальну методологію для усіх держав-членів Союзу із захисту критичної інфраструктури. При чому наголошувалося на посиленні захисту тих об'єктів, загроза для яких може негативно вплинути на декілька країн одночасно за принципом транскордонного зв'язку. Зокрема, йшлося про технологічні об'єкти та об'єкти інформаційної інфраструктури .

Більшість країн-членів ЄС започаткували робочі групи для вирішення питань захисту критичної інфраструктури [37]. Водночас, слід зазначити, що у зарубіжних країнах існують розбіжності у підходах, за допомогою яких країни визначають критичну інфраструктуру держави.

Передусім це стосується "стартової точки" аналізу. Наприклад, деякі країни починають роботу з визначення основних послуг, необхідних для функціонування суспільства, і як наслідок, визначають інфраструктури, які забезпечують ці послуги. Інші спочатку визначають основні інфраструктури у кожному секторі, а потім встановлюють як припинення їхньої роботи вплине на суспільство. Дехто спочатку визначає основних суб'єктів у кожному

критичному секторі, а потім дає їм змогу визначити інфраструктуру, функціонування якої є визначальним для безперервного забезпечення послуг безпеки життєдіяльності.

Більшість країн надає провідну роль щодо виконання заходів захисту критичної інфраструктури державним установам у визначених галузях і утримуються від надання статусу оператора критичної інфраструктури приватним власникам. Майже 45% державних установ, зосереджених на діяльності щодо захисту критичної інфраструктури, підпорядковуються Міністерству внутрішніх справ або подібній установі сектору безпеки.

Так, у Німеччині це Федеральне міністерство внутрішніх справ. В Австрії - Федеральна канцелярія Австрії та Федеральне міністерство внутрішніх справ. У Франції головним органом координації питань захисту найважливіших складових критичної інфраструктури є Генеральний секретаріат з питань оборони і національної безпеки. У Польщі завдання координації заходів в сфері захисту критичної інфраструктури покладено на Урядовий центр безпеки, який є надміністерською організацією, підпорядкованою безпосередньо Прем'єр-Міністру. В Естонії це Державне агентство з питань системної інформації. Водночас у Норвегії центральна установа виконує ще й контрольну функцію щодо ефективності заходів захисту критичної інфраструктури у кожному окремому міністерстві [37].

Проте лише у двох країнах-членах ЄС є державні установи, які займаються винятково питаннями захисту критичної інфраструктури (Велика Британія – CPNI, Іспанія – CNPIC) [37].

Однією з провідних країн світу сьогодні у боротьбі з інформаційним загрозами залишається США. Розроблення державних нормативних актів у сфері забезпечення безпеки критичної інфраструктури тут було розпочато ще у 1998 р. У вересні 2001 р. було створено Міністерство внутрішньої безпеки [25], а 2003 р. - Єдину національну систему управління в умовах надзвичайних ситуацій. Паралельно Конгресом США було прийнято «Патріотичний акт». До

даного документу було включено десять законопроектів та резолюцій щодо міжнародних та внутрішніх юридичних аспектів боротьби з тероризмом [36].

Крім того, 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 [28, с. 10-11].

Що стосується відповідальності за захист критичної інфраструктури та координації відповідної діяльності на загальнодержавному рівні, то зарубіжна практика свідчить про можливість застосування різноманітних організаційних підходів. У більшості країн відповідальність за безпеку критичної інфраструктури лежить на одному або розподіляється між декількома державними відомствами. У Польщі, наприклад, це Центр державної безпеки (RCB) [36].

У США за безпеку критичної інфраструктури відповідає Міністерство внутрішньої безпеки до складу якого входять більш ніж 22 федеральних агентства, відомства і окремі структури. Подібний підхід застосовується у Швеції, де агентство цивільної оборони (MSB), яке підпорядковується Міністерству оборони Швеції, забезпечує організацію планування та відповідні заходи реагування на надзвичайні та кризові ситуації у країні, а також виконує координаційну функцію в контексті створення та впровадження на державному рівні ефективної системи захисту об’єктів критичної інфраструктури [37].

У Фінляндії взагалі немає єдиного органу, який відповідає за захист всіх секторів критичної інфраструктури. Відповідно до Стратегії кібербезпеки Фінляндії, більша частина її критичної інфраструктури знаходиться у приватній власності бізнесу. Тому основна відповідальність із захисту критичної інфраструктури та її об’єктів у даній країні покладається на приватні підприємства. Водночас, головним відповідальним за кібербезпеку критичної інфраструктури визначено державне агентство у сфері зв'язку - Національний центр кібербезпеки Фінляндії. Дана держава установа входить до складу Фінського органу нагляду за комунікаціями.

Крім того, діяльність з управління забезпечення безпеки та захисту критичної інфраструктури у Фінляндії здійснюється управліннями, агентствами та органами у різних стратегічних галузях (енергетичній, у т.ч., радіаційній та ядерній, банківській, соціального забезпечення та охорони здоров'я, транспортній), які визначено відповідальними суб’єктами державної політики з безпеки критичної інфраструктури на державному та регіональному рівнях.

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.

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

На основі вивчення досвіду провідних країн світу, а також опрацювання робіт вітчизняних фахівців щодо захисту критичної інфраструктури, можна виділити такі напрями для розбудови в Україні публічної системи формування безпекового середовища для критичної інфраструктури.

По-перше, вдосконалення системи дієвих організаційно-правових механізмів щодо реагування на загрози, небезпеки і ризики. Даний напрям передбачає, насамперед, наявність нормативно-правової бази з регулювання забезпечення захисту об’єктів критичної інфраструктури. Законодавство у даній сфері має містити чіткий перелік повноважень Уповноваженого органу з питань захисту критичної інфраструктури України щодо координації діяльності суб’єктів захисту критичної інфраструктури, здійснення контролю та нагляду за даною діяльністю, проведення моніторингу та експертної оцінки рівня критичності загроз об’єктів критичної інфраструктури, організації заходів із відновлення пошкоджених або зруйнованих об’єктів та попередження виникнення таких загроз.

Ефективна реалізація цього напряму передбачає наявність відповідних науково-дослідних установ. Основними питаннями цих установ має бути забезпечення науково-технічного супроводу функціонування системи аналізу про стан критичної інфраструктури. Крім того, такі установи мають бути уповноважені здійснювати експертизу з оцінки прогнозування наслідків впливів на стійкість об’єктів критичної інфраструктури [10, с. 57-58].

Слід зазначити, що деякі перспективи щодо зазначених аспектів вдосконалення системи ефективних організаційно-правових механізмів реагування на загрози, небезпеки і ризики окреслено у Стратегії забезпечення державної безпеки, затвердженої Указом Президента України від 16.02.22 р. № 56/20.

По-друге, створення комплексної системи захисту об’єктів критичної інфраструктури. Об’єкти критичної інфраструктури в умовах повномасштабного вторгнення стали найбільш вразливими для таких дій як диверсії, терористичні акти та несанкціоновані втручання.

Реалії такі, що країна-агресор руйнує об’єкти життєзабезпечення, тим самим тероризуючи морально-психологічний стан мирного населення Це посилює внутрішню дестабілізацію країни. Військово-терористична ситуація, що склалась в Україні становить небезпеку для всього європейського континенту. Це вимагає вжити заходів щодо формування спільних рішень і забезпечувати комплексний підхід до системи захисту України.

По-третє, створення системи забезпечення інформаційної безпеки та кібербезпеки. Ключовим елементом у боротьбі із кібертероризмом є законодавство. На сьогоднішній день існує чимала кількість міжнародно-правових ініціатив, міжнародних майданчиків, форумів для протидії кібертероризму. Дані інструменти торкаються великого спектру загроз, що виходять з інформаційного простору і, певною мірою, є обмежувальним фактором для поширення кіберзлочинності.

Однак, як показує практика, дії, що вживаються, не дають досягти належного результату. Це є наслідком того, що ініціативи здебільшого

орієнтовані на зміцнення внутрішнього законодавства для боротьби зі злочинами в інформаційному просторі.

Отже, можна зробити висновок, що в міжнародному співтоваристві наразі відсутні ефективні міжнародно-правові ініціативи щодо протидії кібертероризму, що ставить перед ним завдання не лише виробити єдині міжнародно-правові стандарти, а й забезпечити їх здійснення кожною державою. У відповідь на ці виклики державам слід зосередитися на розробці систем контролю над інформаційним потоком усередині мережевих ресурсів, при цьому не виходячи за правові рамки міжнародного та національного законодавства.

За останній час на національному рівні у державах було сформовано спецпідрозділи, які ставили за мету: ведення розвідки в комп'ютерних мережах, захист власних таких мереж, блокування роботи структур супротивника.

З огляду на даний досвід, пропонується створити координаційний центр діяльності державних органів України у протидії інформаційним впливам. Такий центр, на нашу думку, може бути створений на базі Служби зовнішньої розвідки України. До його функцій слід також віднести контроль за всіма компонентами національного інформаційного простору та проведення моніторингу у даній сфері..

У країнах, які мають високий рівень інформатизації, питання захисту критичної інфраструктури від кіберзагроз входять до складу загальнодержавної системи кібернетичної безпеки. Крім того, належна увага у зарубіжних країнах приділяється підготовці фахівців у зазначеній галузі.

З огляду на зарубіжний досвід, з метою вдосконалення управління безпекою об'єктів критичної інфраструктури в Україні запропоновано вжити наступні заходи:

- створити ефективні організаційно-правові механізми реагування на загрози, небезпеки і ризики,

- створити комплексну систему захисту об'єктів критичної інфраструктури,

- створити систему забезпечення інформаційної безпеки та кібербезпеки,

- удосконалити технічний захист об’єктів критичної інформаційної інфраструктури,

- створити систему професійної підготовки фахівців у сфері забезпечення і захисту об’єктів критичної інфраструктури,

- посилити взаємодію із іншими країнами та міжнародними інституціями у сфера захисту об’єктів критичної інфраструктури.

Усі недоліки щодо організації механізму управління системою забезпечення та захисту об’єктів критичної інфраструктури мають бути усунено шляхом внесення відповідних змін до профільного нормативно-правового акту – Закону України «Про критичну інфраструктуру».

ВИСНОВКИ ДО РОЗДІЛУ 3

З урахуванням зарубіжного досвіду було запропоновано наступні напрями вдосконалення безрпекового середовища для об’єктів критичної інфраструктури в Україні:

- створення ефективних організаційно-правових механізмів реагування на загрози, небезпеки і ризики та комплексної системи захисту об’єктів критичної інфраструктури, у т.ч., у сфері інформаційної безпеки та кібербезпеки,

- удосконалення технічного захисту об’єктів критичної інформаційної інфраструктури,

- створення системи професійної підготовки фахівців у сфері забезпечення і захисту об’єктів критичної інфраструктури,

- посилення взаємодії із іншими країнами та міжнародними інституціями у сфера захисту об’єктів критичної інфраструктури,

- вдосконалення нормативно-правової бази у сфері формування безпекового середовища об’єктів критичної інфраструктури.

ВИСНОВКИ

Дане дослідження проводилося з метою вивчення актуальних проблем управління безпекою об’єктів критичної інфраструктури та з’ясування можливих шляхів їх вирішення в Україні. Результатом проведеного дослідження стали наступні висновки та пропозиції.

Встановлено, що загальновизнаного поняття «критична інфраструктура» не існує, воно визначається на національному рівні, відповідно різняться підходи щодо визначення об’єктів критичної інфраструктури, їх класифікації, державної політики щодо управління їх забезпеченням та захистом тощо.

Проте для усіх країн характерним є розуміння критичної інфраструктури як стратегічно важливі підприємства та установи, які необхідні для забезпечення життєдіяльності суспільства та функціонування економіки країни, незапланована зупинка, виведення з ладу чи повне руйнування яких здатні становити загрозу для національної безпеки, природного середовища, спричинити погіршення оборонної здатності, матеріальні та фінансові збитків чи навіть призвести до людських жертв.

Захист об’єктів критичної інфраструктури полягає у подоланні наслідків загроз та їх запобіганні щодо визначених об’єктів з метою забезпечення сталого функціонування та неухильного прогресу країни. Суб’єкти захисту безпеки об’єктів критичної інфраструктури в Україні включають органи державної влади всіх рівнів та органи місцевого самоврядування, крім того є ще секторальні органи у сфері захисту критичної інфраструктури.

Встановлено, що в Україні існує комплексна нормативно-правова база, яка регулює питання захисту критичної інфраструктури. Проте, незважаючи на наявність законодавчої бази, існують певні вразливості та виклики у сфері захисту критичної інфраструктури. Це включає недостатню координацію між різними органами влади, обмеженість фінансових ресурсів та необхідність оновлення та вдосконалення правових норм з урахуванням сучасних загроз.

Удосконалення управління безпекою об’єктів критичної інфраструктури в Україні потребує реалізації таких заходів:

- створити ефективні організаційно-правові механізми реагування на загрози, небезпеки і ризики,

- створити комплексну систему захисту об’єктів критичної інфраструктури та систему забезпечення інформаційної безпеки та кібербезпеки,

- удосконалити технічний захист об’єктів критичної інформаційної інфраструктури,

- створити систему професійної підготовки фахівців у сфері забезпечення і захисту об’єктів критичної інфраструктури,

- посилити взаємодію із іншими країнами та міжнародними інституціями у сфері формування безпекового середовища для об’єктів критичної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України від 28.06.1996 р. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

2. Додатковий протокол до Женевських конвенцій від 12.08.1949 р. URL: https://zakon.rada.gov.ua/laws/show/995_199 (дата звернення: 10.03.2024)

3. Кодекс цивільного захисту України від 02.10.2012 р. №5403-VI URL: https://zakon.rada.gov.ua/laws/show/5403-17 (дата звернення: 10.03.2024)

4. Про боротьбу з тероризмом: Закон України від 20.03.2003 р. №638-IУ URL: https://zakon.rada.gov.ua/laws/show/638-15 (дата звернення: 10.03.2024)

5. Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України: Закон України від 18.10.2022 р. №2684-IX URL: https://zakon.rada.gov.ua/laws/show/2684-20 (дата звернення: 10.03.2024)

6. Про громадські об’єднання: Закон України від 22.03.2012 р. №4572-VI URL: https://zakon.rada.gov.ua/laws/show/4572-17 (дата звернення: 10.03.2024)

7. Про Державну службу спеціального зв’язку та захисту інформації України: Закон України від 23.02.2006 р. №3475-IУ URL: https://zakon.rada.gov.ua/laws/show/3475-15 (дата звернення: 10.03.2024)

8. Про державну таємницю: Закон України від 21.01.1994 р. №3855-XII URL: https://zakon.rada.gov.ua/laws/show/3855-12 (дата звернення: 10.03.2024)

9. Про доступ до публічної інформації: Закон України від 13.01.2011 р. №2939-VI URL: https://zakon.rada.gov.ua/laws/show/2939-17 (дата звернення: 10.03.2024)

10. Про критичну інфраструктуру: Закон України від 16.11.2021 р. № 1882 URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 10.03.2024)

11. Про місцеве самоврядування в Україні: Закон України від 21.05.1997 р. № 280/97-ВР URL: https://zakon.rada.gov.ua/laws/show/280/97-вр (дата звернення: 10.03.2024)

12.Про національну безпеку України: Закон України від 21.06.2018 р. №2469-VIII URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 10.03.2024)

13.Про оборону України: Закон України від 06.12.1991 р. №1932-XII URL: https://zakon.rada.gov.ua/laws/show/1932-12 (дата звернення: 10.03.2024)

14.Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. №2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 10.03.2024)

15.Про правовий режим воєнного стану: Закон України від 12.05.2015 р. №389-VIII URL: https://zakon.rada.gov.ua/laws/show/389-19 (дата звернення: 10.03.2024)

16.Про правовий режим надзвичайного стану: Закон України від 16.03.2000 р. № 1550-III URL: https://zakon.rada.gov.ua/laws/show/1550-14 (дата звернення: 10.03.2024)

17.Про Службу безпеки України: Закон України від р. №2229-XII URL: https://zakon.rada.gov.ua/laws/show/2229-12 (дата звернення: 10.03.2024)

18.Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання: Закон України від 19.10.2000р. №2064-III URL: https://zakon.rada.gov.ua/laws/show/2064-14 (дата звернення: 10.03.2024)

19.Про функціонування єдиної транспортної системи України в особливий період: Закон України від 20.10.1998р. №194-XIУ URL: https://zakon.rada.gov.ua/laws/show/194-14 (дата звернення: 10.03.2024)

20.Про введення воєнного стану: Указ Президента України від 24.02. 2022 р. № 64/2022 URL: https://zakon.rada.gov.ua/laws/show/64/2022

21.Про Річну національну програму під егідою Комісії Україна – НАТО на 2020 рік: Указ Президента України від 26.05. 2020 р. № 203/2020 URL: https://zakon.rada.gov.ua/laws/show/203/2020 (дата звернення: 10.03.2024)

22.Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. “Про загрози кібербезпеці держави та невідкладні заходи з їх

нейтралізації”: Указ Президента України від 13.02. 2017 р. № 32/2017 URL: https://www.president.gov.ua/documents/322017-21282 (дата звернення: 10.03.2024)

23.Про рішення Ради національної безпеки і оборони України від 16 лютого 2017 р. “Про невідкладні заходи з нейтралізації загроз енергетичній безпеці України та посилення захисту критичної інфраструктури” : Указ Президента України від 16.02. 2017 р. № 37/2017 URL: https://www.president.gov.ua/documents/372017-21302 (дата звернення: 10.03.2024)

24.Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року «Про нову редакцію Стратегії національної безпеки України»: Указ Президента України від 08.06.2012 р. №389 URL: https://zakon.rada.gov.ua/laws/show/389/2012 (дата звернення: 10.03.2024)

25.Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки»: Указ Президента України від 16.02.2022 р. № 56/20 URL:https://www.president.gov.ua/documents/562022-41377 (дата звернення: 10.03.2024)

26.Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. “Про Стратегію кібербезпеки України”: Указ Президента України від 15.03. 2016 р. № 96/2016 URL: https://www.president.gov.ua/documents/962016-19836 (дата звернення: 10.03.2024)

27.Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.2021 р. №447 URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 10.03.2024)

28.Про рішення Ради національної безпеки та оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26.05. 2015 р. № 287/2015 URL:

https://www.president.gov.ua/documents/2872015-19070 (дата звернення: 10.03.2024)

29.Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.2020 р. № 392/2020 URL: https://www.president.gov.ua/documents/3922020-35037 (дата звернення: 10.03.2024)

30.Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. “Про удосконалення заходів забезпечення захисту об’єктів критичної інфраструктури”: Указ Президента України від 16.01.2017 р. № 8/2017 URL: https://www.president.gov.ua/documents/82017-21058 (дата звернення: 10.03.2024)

31.Про Рекомендації парламентських слухань з питання розвитку інформаційного суспільства: Постанова Верховної Ради України від 01.12.2005 р. №3175-IV URL: https://zakon.rada.gov.ua/laws/show/3175-15 (дата звернення: 10.03.2024)

32.Деякі питання об’єктів критичної інформаційної інфраструктури: постанова Кабінету Міністрів України від 09.10.2020 р. № 943 URL: https://zakon.rada.gov.ua/laws/show/943-2020-п (дата звернення: 10.03.2024)

33.Деякі питання об’єктів критичної інфраструктури: постанова Кабінету Міністрів України від 09.10.2020 р. № 1109 URL: https://zakon.rada.gov.ua/laws/show/1109-2020-п (дата звернення: 10.03.2024)

34.Арсенович Л. А. Деякі питання запровадження системи підготовки фахівців у сфері захисту критичної інфраструктури. *Таврійський науковий вісник. Серія: Публічне управління та адміністрування.* 2023. №5. С. 3-14.

35.Бірюков Д. С. Загрози критичній інфраструктурі та їх вплив на стан національної безпеки: Аналітична записка. URL: file:///C:/Users/Student/Desktop/nivanb_2015_3-4_14.pdf (дата звернення: 10.03.2024).

36.Войціховський А. В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «ПРАВО».* 2020. Випуск 29. С.281-288.

37.Гора І.В., Батюк О.В. Окремі питання захисту об'єктів критичної інфраструктури: зарубіжний досвід. *Соціально-правові студії*. 2021. Випуск 1 (11). С. 132-139.

38.Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналіт. доп. / за ред. О. М. Суходолі. Київ: НІСД, 2020. 28 с.

39.Домарацький М. Б. Забезпечення безпеки та підвищення ефективності захисту критично важливих об'єктів на державному рівні. *Публічне управління і адміністрування в Україні*. 2019. Вип. 14. С. 82–85.

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

41.Єрменчук О. П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монографія. Дніпро: ДДУ ВС, 2018. 180 с.

42.Захист критичної інфраструктури в умовах надзвичайних ситуацій: монографія / С.І. Азаров, В.Л. Сидоренко, С.А. Єременко, А.В. Пруський, А.М. Демків; за заг. ред. П.Б. Волянського. Київ, 2021. 375 с.

43.Зубко Г. Ю. Поняття та зміст стратегічних об'єктів інфраструктури. *Visegrad Journal on Human Rights*. 2020. № 2 (Vol. 1). С. 104–115.

44.Зубко Г.Ю. Державна інфраструктурна політика: досвід балтійських країн. *Право та державне управління*.2019. № 2 (35) том 1. С.258-265.

45.Іванюта С.П. Пріоритети формування реєстру об'єктів критичної інфраструктури та порядку їх обліку. *Стратегічні пріоритети*. 2018. №3-4(48). С. 26-35.