НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

ДОМАРАЦЬКИЙ Михайло Богданович

УДК 351.862.4

ДИСЕРТАЦІЯ

ДЕРЖАВНЕ УПРАВЛІННЯ ЗАБЕЗПЕЧЕННЯМ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

25.00.05 – державне управління у сфері державної безпеки
та охорони громадського порядку

Подається на здобуття наукового ступеня кандидата наук
з державного управління

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ М. Б. Домарацький

Науковий керівник: ШВЕДУН Вікторія Олександрівна,
доктор наук з державного управління, професор

Харків – 2020

АНОТАЦІЯ

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.

Дисертаційну роботу присвячено обґрунтуванню й розробці теоретичних засад і науково-практичних рекомендацій щодо вдосконалення державного управління забезпеченням безпеки критичної інфраструктури в Україні.

Надано сутнісну характеристику критичної інфраструктури як об'єкту державного управління, описано механізми державного управління захистом об'єктів критичної інфраструктури, охарактеризовано державну систему забезпечення безпеки і захисту критичної інфраструктури.

Проаналізовано досвід зарубіжних країн стосовно державного управління критичною інфраструктурою, виокремлено специфіку державного управління критичною інфраструктурою в Україні, здійснено оцінку вітчизняного нормативного й адміністративного забезпечення державного управління критичною інфраструктурою.

Удосконалено державні механізми забезпечення безпеки та підвищення ефективності захисту критичної інфраструктури, виокремлено напрями розвитку системи державного управління захистом критичної інфраструктури, запропоновано підходи до вдосконалення державної політики захисту критичної інфраструктури в Україні.

Обґрунтовано, що для практичної реалізації заходів державного управління стосовно стратегічних ризиків для критичної інфраструктури повинні застосовуватися: системно-правовий, політичний, інформаційний,

економічний й організаційно-адміністративний механізми у межах комплексного механізму державного управління критичною інфраструктурою.

Запропоновано шляхи вдосконалення державної політики захисту критичної інфраструктури в Україні. Розроблено комплекс заходів, що забезпечують реалізацію основних механізмів й етапів впровадження державної політики у сфері забезпечення безпеки автоматизованих систем управління критичної інфраструктури.

Ключові слова: державне управління, захист критичної інфраструктури, критично важливі об'єкти, державна система безпеки, стратегічні ризики для критичної інфраструктури.

ANNOTATION

Domaratskyy M. B. «Public administration of critical infrastructure security in Ukraine».– Manuscript.

Dissertation on competition of Candidate of Sciences degree in Public Administration by specialty 25.00.05 – public administration in the sphere of state security and protection of public order.– National University of Civil Defense of Ukraine, Kharkiv, 2020.

The thesis is devoted to justification and development of theoretical foundations and scientific and practical recommendations for improving of the public administration of critical infrastructure in Ukraine.

The essential characteristic of critical infrastructure as an object of public administration is presented, the mechanisms of public administration of protection of critical infrastructure facilities are described, and state system of ensuring of security and protection of critical infrastructure is described.

The experience of foreign countries on public administration of critical infrastructure is analyzed, the specifics of public administration of critical

infrastructure in Ukraine are revealed, the assessment of domestic normative and administrative support of public administration of critical infrastructure is carried out.

The state mechanisms on ensuring security and improving of effectiveness of protection of critical infrastructure are improved, the directions of development of the system of public administration of critical infrastructure protection are identified, and the approaches to improvement of state policy of protection of critical infrastructure in Ukraine are proposed.

It is justified that the system and legal, political, information, economic and organizational and administrative mechanisms within the framework of the integrated mechanism of public administration of critical infrastructure should be applied for the practical implementation of public administration measures concerning strategic risks for critical infrastructure.

The ways to improve the state policy of protection of critical infrastructure in Ukraine are proposed. A set of measures to ensure implementation of the main mechanisms and stages of realization of the state policy in the field of security of automated management systems of critical infrastructure are developed.

Keywords: public administration, critical infrastructure protection, critical facilities, state security system, strategic risks for critical infrastructure.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, які відображають основні наукові результати дисертації

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

2. Домарацький М. Б. Методика державного категорування критично важливих об’єктів / М. Б. Домарацький // Держава та регіони. – 2019. − № 4(68). – С. 278 – 281. – (Серія «Державне управління»).

3. Домарацький М. Б. Особливості формування та функціонування державної системи моніторингу стану об’єктів критичної інфраструктури / М. Б. Домарацький // Право та державне управління. – 2019. − № 4. – С. 170–174.

4. 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. – (Серія «Державне управління»).

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

Праці, які додатково відображають наукові результати дисертації

6. Домарацький М.Б. Аналіз загроз у процесі категоріювання об’єктів критичної інформаційної інфраструктури на державному рівні / М. Б. Домарацький // Інноваційне підприємництво, менеджмент, фінанси: стан, аналіз тенденцій та науково-економічний розвиток : матеріали міжнародної науково-практичної конференції. – Львів: ЛЕФ, 2019. – Ч. 2. – С. 104–105.

7. Домарацький М. Б. Впровадження державних заходів щодо антикризової діяльності відносно захисту регіональної критичної інфраструктури / М. Б. Домарацький // Інноваційний розвиток і підвищення рівня спроможності об'єднаних територіальних громад: матеріали науково-практичної конференції за міжнародною. − Дніпро : ДРІДУ НАДУ, 2019. – С. 74–75.

8. 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.

9. Домарацький М. Б. Актуальні проблеми державного управління захистом критичної інфраструктури в Україні / М. Б. Домарацький // IV Всеукраїнська науково-практична конференція «Публічне управління та адміністрування у процесах економічних реформ»: збірник тез. –Херсон : Херсонський державний аграрно-економічний університет, 2020. – С. 159–161.

10. Домарацький М. Б. Особливості імплементації міжнародного досвіду забезпечення безпеки критичної інфраструктури в українську практику державного управління / М. Б. Домарацький // Державне управління у сфері цивільного захисту: наука, освіта, практика: матеріали міжнародної науково-практичної інтернет-конференції. – Х. : НУЦЗУ, 2020. – С. 54–56.

11. Домарацький М. Б. Реформування процесів державного управління критичною інфраструктурою / М. Б. Домарацький // Інформаційні технології: наука, техніка, технологія, здоров’я: тези доповідей XXVII науково-практичної конференції MicroCAD-2020. – Ч. IV. – Х. : НТУ «ХПІ», 2020. – С. 74–75.

Публікації в інших виданнях

12. Домарацкий М. Б. Научные основы государственного управления критической инфраструктурой в Украине [Электронный ресурс] / М. Б. Домарацкий // East Journal of Security Studies. – 2018. – Вып. 1(3). – Режим доступа : http://repositsc.nuczu.edu.ua/bitstream/123456789/10664/1/domaratskyejss.pdf

ЗМІСТ

ВСТУП

Актуальність теми. В сучасних умовах існує необхідність переосмислити спектр та характер загроз, що проявляються як у відношенні до окремих держав, так і для світової спільноти в цілому. Ускладнення технологічного потенціалу цивілізації, збільшення чисельності населення та складність його урбанізації призвели до збільшення ризику виникнення різних надзвичайних ситуацій, особливо на критично важливих об’єктах. У зв'язку з цим все більшого значення набувають питання, пов'язані з подоланням різних кризових явищ та забезпеченням особистої, соціальної та національної безпеки в надзвичайних ситуаціях.

В даний час здатність держави та суспільства своєчасно розпізнавати передумови криз та катастроф, які можуть негативно вплинути на критичну інфраструктуру та ефективно боротися з ними, стала одним із ключових завдань національної безпеки.

Така ситуація спричинена тим, що наслідки аварій, катастроф та стихійних лих стають все більш масовими та становлять небезпеку для населення та сталого функціонування економіки. Аналіз надзвичайних ситуацій різних масштабів та наслідків демонструє, що загрозу національній безпеці можуть становити як окремі надзвичайні ситуацій на державному та регіональному рівнях так і щорічні надзвичайні ситуації на територіальному, місцевому та локальному рівнях. Крім того, кризові явища, з якими стискається наше суспільство, показують, що необхідно кардинально змінити систему захисту населення та критично важливі об'єкти у надзвичайних ситуаціях, розробити та впровадити ефективні механізми її функціонування.

Необхідно також прийняти до уваги, що питання змісту управлінських функцій, організаційної структури, основ функціонування і напрямів розвитку системи державного управління забезпеченням безпеки критичної

інфраструктури зумовлюють необхідність вдосконалення державної політики у сфері забезпечення безпеки населення і територій при надзвичайних ситуаціях у мирний і воєнний час у взаємозв'язку з теоретичними проблемами державного будівництва.

В останні роки в нашій країні було суттєво розвинено процеси створення та розвитку державних механізмів захисту населення та територій від надзвичайних ситуацій будь-яких форм і масштабів. Зокрема, у Стратегії національної безпеки України окреслено пріоритети державної політики національної безпеки України до 2020 року. Загалом, можна сказати, що в Україні сформована та діє дуже ефективна та соціально затребувана система захисту населення та територій від надзвичайних ситуацій. У той же час масштабні зміни в різних сферах життєдіяльності держави та збільшення кількості й масштабів терористичних актів призвели до необхідності формування ефективної національної політики щодо захисту критично важливих об’єктів у разі виникнення та поширення надзвичайних ситуацій. Враховуючи наведене вище, необхідно вдосконалити процеси забезпечення державної безпеки критичної інфраструктури в сучасних умовах.

Значний внесок у дослідження проблем державного управління зробили такі науковці, як: Г. В. Атаманчук, В. Д. Бакуменко, І. І. Бодрова, О. В. Бойко-Бойчук, В. М. Вакуленко, А. О. Дєгтяр, С. М. Домбровська, В. К. Євдокименко, М. А. Латинін, В. М. Мороз, В. М. Нижник, Р. М. Рудніцька, В. В. Токовенко, О. О. Труш, А. О. Чечель, та інші.

Аналіз наукових джерел із проблематики державного управління у сфері національної безпеки, у тому числі − захисту населення і територій − свідчить, тут належить вагомий теоретичний доробок як українським, так і зарубіжним ученим. Зокрема, зазначеним питанням присвячено наукові праці таких авторів: Ю. А. Абрамов, С. О. Андреєв, В. А. Андронов, С. В. Бєлай, А. В. Бєлоусов, М. В. Болотських, Б. Е. Братко, П. Б. Волянський, А. Б. Качинський,

В. В. Коврегін, В. А. Ліпкан, О. А. Мельниченко, Д. О. Полковниченко, В. О. Пономаренко, А. В. Ромін, В. П. Садковий, В. Ю. Стрельцов, Г. П. Ситник, М. В. Сунгуровський та ін.

Водночас деяким питанням цієї важливої з практичної точки зору та складної в теоретичному плані проблеми не приділено достатньої уваги. Ще недостатньо опрацьованими залишаються питання вироблення дієвих напрямів розвитку державного управління критично важливими об'єктами. Це й зумовлює актуальність обраної теми дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційну роботу виконано у навчально-науково-виробничому центрі Національного університету цивільного захисту України відповідно до тематики науково-дослідної робот «Розробка наукових основ державного управління у сфері безпеки ринку соціально-економічних послуг України з точки зору цивільного захисту» (державний реєстраційний номер 0115U002035). Роль здобувача полягає в обґрунтуванні методичних підходів і напрямів удосконалення державної політики захисту критичної інфраструктури в Україні. Крім того, дисертаційна робота виконувалася згідно тематики науково-дослідної роботи «Розробка механізмів державного управління соціально-економічною сферою та її галузями в контексті забезпечення безпеки українського суспільства» (ДР № 0118U001007), у межах якої автором вдосконалено систему управління критичною інфраструктурою в Україні.

Мета й завдання дослідження. Мета дисертаційної роботи полягає в обґрунтуванні теоретичних засад та розробці практичних рекомендацій щодо вдосконалення державного управління забезпеченням безпеки критично важливих об'єктів.

Необхідність досягнення поставленої мети зумовила визначення та вирішення таких завдань:

- розкрити сутність державного управління забезпеченням безпеки об'єктів критичної інфраструктури;

- визначити особливості формування державної системи захисту критичної інфраструктури;

- проаналізувати досвід зарубіжних країн стосовно державного управління забезпеченням безпеки критичної інфраструктури;

- окреслити специфіку державного управління забезпеченням безпеки критичної інфраструктури в Україні;

- здійснити оцінку вітчизняного нормативного й адміністративного забезпечення державного управління критичною інфраструктурою;

- вдосконалити державні механізми забезпечення безпеки та підвищення ефективності захисту критичної інфраструктури;

- виокремити напрями розвитку системи державного управління забезпеченням захисту критичної інфраструктури;

- запропонувати шляхи вдосконалення державної політики захисту критичної інфраструктури в Україні.

Об’єкт дослідження – державне управління безпекою інфраструктури життєзабезпечення населення і територій.

Предмет дослідження – державне управління забезпеченням безпеки критичної інфраструктури в Україні.

Методи дослідження. Теоретичною та методичною основою дослідження виступають закономірності й принципи державного управління у сфері цивільного захисту. Для вирішення поставлених у роботі завдань було використано такі наукові методи:

- аналіз і синтез, індукція та дедукція – для деталізації предмета дослідження;

- узагальнення та порівняння – для дослідження закономірностей державного управління забезпеченням безпеки критичної інфраструктури в Україні та інших країнах;

- системний підхід – для обґрунтування дефініції комплексного механізму державного управління стратегічними ризиками критичної інфраструктури;

- ретроспективний аналіз – для оцінки кількості надзвичайних ситуацій на критично важливих об’єктах України;

- структурний підхід – для визначення взаємозв’язків між елементами державної системи захисту критичної інфраструктури;

- логіко-дескриптивний аналіз – для визначення напрямів трансформації державної системи моніторингу стану критичної інфраструктури;

Інформаційну базу дисертаційного дослідження складають чинні вітчизняні та закордонні законодавчі та підзаконні нормативно-правові акти щодо питань державного управління, зокрема, у сфері захисту населення і територій від надзвичайних ситуацій, наукові напрацювання вітчизняних і зарубіжних учених, періодичні видання, статистичні й аналітичні матеріали, особисті дослідження автора.

Наукова новизна одержаних результатів полягає в обґрунтуванні та розробленні теоретичних засад і науково-практичних рекомендацій щодо формування та впровадження комплексу заходів, спрямованих на вдосконалення державного управління забезпеченням безпеки критичної інфраструктури.

Уперше:

- розроблено принципово новий підхід до вдосконалення державної системи захисту критичної інфраструктури, яка являє собою інтегрований комплекс реальних елементів, видів діяльності і процесів з цільовою поведінкою, логічно і функціонально упорядкованих, та спрямованих на

забезпечення безпеки об'єктів критичної інфраструктури в певний час і у даному просторі, а також об'єднує в собі підсистеми цивільного захисту, фізичного захисту, кібернетичного захисту та антитерористичного захисту з метою досягнення синергетичного ефекту у процесах захисту об’єктів критичної інфраструктури від викликів і загроз популяційного, диференційованого й інтегрального походження;

- запропоновано напрями трансформації державної системи моніторингу стану критичної інфраструктури через створення центрів системного моніторингу й оперативного управління, комплексів одержання інформації про узагальнені параметри стану захищеності об'єктів критичної інфраструктури, а також систем і засобів телекомунікацій, збору, передачі даних та оповіщення на загальнодержавному, міжрегіональному, регіональному, муніципальному й об'єктовому рівнях, що уможливлює формування єдиного інформаційного простору системи моніторингу критичної інфраструктури на основі уніфікації і сумісності інформаційних, програмних і апаратних засобів;

удосконалено:

- методичний підхід до формування комплексного механізму державного управління стратегічними ризиками критичної інфраструктури, який, на відміну від існуючих, передбачає поєднання системно-правового, політичного, інформаційного, економічного й організаційно-адміністративного механізмів, та передбачає практичну реалізацію комплексу заходів з управління стратегічними ризиками для критичної інфраструктури з опорою на всю державну владну вертикаль;

- теоретичний підхід до державної протидії стратегічним ризикам і загрозам для критичної інфраструктури, який, на відміну від існуючих, передбачає пріоритетну реалізацію системного комплексу організаційних, технічних, фінансових та інших заходів попереджувального та реагувального характеру, які виробляються на основі експертно-аналітичних методів

вирішення ряду взаємопов'язаних завдань щодо ідентифікації, оцінки та ранжування часткових та інтегральних стратегічних загроз критичній інфраструктурі на загальнодержавному та регіональному рівнях за наявності політичного, правового, інституційного, адміністративного, економічного, науково-технічного та техніко-технологічного забезпечення;

- практичний підхід до формування державної політики у сфері забезпечення безпеки автоматизованих систем управління критичною інфраструктурою через інтеграцію в єдині комплекси автоматизованих систем управління критично важливими об’єктами й інших інформаційних систем, що використовуються в управлінні виробничими і транспортними структурами, а також адміністративними і фінансовими ресурсами, що в сукупності уможливлює створення єдиної державної системи виявлення і попередження комп'ютерних атак на критичну інформаційну інфраструктуру та оцінку рівня реальної захищеності її елементів;

дістали подальшого розвитку:

- послідовність етапів забезпечення функціональності системи раннього попередження прояву кризових ситуацій в якості аналітичного процесу, який спирається на ідентифікацію областей і секторів критичної інфраструктури на національному, регіональному та локальному рівні, а також ідентифікацію релевантних ризиків для секторів критичної інфраструктури з точки зору збереження їх безпеки, функціональності, економічної та суспільної стабільності з урахуванням специфіки критично важливих об’єктів державної та приватної сфер;

- напрями трансформації державної політики захисту критичної інфраструктури в Україні, яка передбачає наявність таких складових: політика «легких мішеней», політика національної безпеки, антитерористична політика, політика кібербезпеки, спрямованих на забезпечення комплексного захисту критичної інфраструктури, включаючи оцінку рівня реальної захищеності

елементів критичної інфраструктури шляхом консолідації зусиль органів державної влади й інститутів громадянського суспільства за допомогою комплексного використання правових, організаційних, технічних, соціально-економічних, спеціальних та інших заходів підтримки необхідного рівня безпеки;

- понятійний апарат науки «Державне управління» шляхом уточнення сутності категорій *«державний захист критичної інфраструктури»,* який являє собою сукупність організаційних і технічних заходів, орієнтованих на забезпечення захисту секторів критичної інфраструктури від різнохарактерних загроз як у разі появи надзвичайних чи кризових ситуацій, так і від наслідків ненавмисних дій, які могли б завдати шкоди для критичної інфраструктури через організуючий і регулюючий вплив системи державних органів; *«захищеність критично важливих об'єктів»*, під яким слід розуміти стан, при якому у відношенні до об'єктів критичної інфраструктури державою забезпечуються умови для запобігання виникнення потенційної небезпеки і подолання або зниження до мінімального рівня негативних наслідків кризових ситуацій природного і техногенного характеру, а також ситуацій, викликаних проявами тероризму.

Практичне значення одержаних результатів полягає в тому, що теоретичні та методичні положення дисертаційної роботи доведено до рівня конкретних рекомендацій і пропозицій, які можуть використовуватись у науково-дослідній діяльності – як підґрунтя для подальшої розробки концептуальних засад розвитку критичної інфраструктури в Україні; у процесі державного управління функціонуванням критично важливих об’єктів – як основа для вдосконалення державної політики України захисту критичної інфраструктури; у межах функціонування органів самоврядування – щодо вдосконалення державної системи захисту критичної інфраструктури; у процесі розробки нормативно-правового інструментарію – під час формування

понятійно-категоріального апарату та нормативних засад державного управління забезпеченням безпеки критичної інфраструктури.

Запропонований автором практичний підхід до формування державної політики у сфері забезпечення безпеки автоматизованих систем управління критичною інфраструктурою був використаний у процесі функціонування Департаменту інфраструктури Волинської обласної державної адміністрації (довідка про впровадження від 14.05.2019 р. № 294/01-17/2-19). Результати досліджень автора стосовно державної протидії стратегічним ризикам і загрозам для критичної інфраструктури були використані в практичній діяльності Управління Західного офісу Держаудитслужби у Волинській області (довідка про впровадження від 14.05.2019 р. № 13-03-09-14/1592-2020).

Крім того, теоретичні положення та наукові результати дослідження роботи використано в роботі Національного університету цивільного захисту України (акт б/н від 21.11.2019).

Особистий внесок здобувача. Дисертаційна робота є самостійною науково-дослідною роботою автора, яка містить теоретичні обґрунтування, практичні рекомендації, висновки та пропозиції, що були отримані автором особисто, та в сукупності вирішують важливе наукове завдання щодо розробки та впровадження комплексу заходів щодо підвищення рівня державної безпеки критичної інфраструктури.

Апробація результатів дослідження. Основні положення дисертації доповідалися на Міжнародній науково-практичній конференції для студентів, аспірантів та молодих учених «Фінансова система та економічна безпека: стан, проблеми, ефективність» (м. Київ, 23 листопада 2019 р.), Міжнародній науково-практичній конференції «Інноваційне підприємництво, менеджмент, фінанси: стан, аналіз тенденцій та науково-економічний розвиток» (Львів, 23 листопада 2019 року), науково-практичній конференції за міжнародною участю «інноваційний розвиток і підвищення рівня спроможності об'єднаних

територіальних громад» (м. Дніпро, 30 жовтня – 29 листопада 2019 р.), Міжнародній науково-практичній Інтернет-конференції «Державне управління у сфері цивільного захисту: наука, освіта, практика» (м. Харків, 18−19 березня 2020 р.), Всеукраїнській науково-практичній конференції «Публічне управління та адміністрування у процесах економічних реформ» (м. Херсон, 25 березня 2020 р.) та XXVIII науково-практичній конференції MicroCAD-2020 (м. Харків, жовтень, 2020 р.).

Публікації. Основні положення та результати дослідження за темою дисертації відображено у 12 наукових працях, у тому числі 5 статей опубліковано в спеціалізованих фахових виданнях України, 1 стаття – у закордонному виданні відповідно до напряму дослідження, 6 – тези доповідей на конференціях. Загальний обсяг публікацій становить 3,4 авт. арк.

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, висновків, списку використаних джерел і додатків. Повний обсяг дисертації становить 259 сторінок, з них 224 сторінки основного тексту. Робота містить 6 рисунків, 10 таблиць та 3 додатки (на чотирьох сторінках). Список використаних джерел містить 251 найменування (на 35 сторінках).

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДЕРЖАВНОГО УПРАВЛІННЯ ЗАБЕЗПЕЧЕННЯМ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Сутнісна характеристика критичної інфраструктури як об'єкту державного управління

Основним пріоритетом людей в усі періоди їхнього життя завжди є прагнення забезпечити існування, зберегти життя та здоров'я, уникати агресії, досягати комфортних умов життя та захищати довкілля. Більшість з цих пріоритетів безпосередньо належать до галузі безпеки. Безпека − найважливіша частина якості життя та найважливіша мета існування.

Роль безпеки визначається наявністю в природної та соціальній сферах існування людства численних постійних і різноманітних небезпек. Саме наявність в цьому світі небезпек, що загрожують всім і кожному, обумовлює необхідність докладати зусилля для забезпечення особистої, громадської, державної та будь-якої іншої безпеки. У найзагальнішому вигляді небезпека − це потенційна можливість викликати шкоду, принести нещастя. Небезпека також може бути представлена як можливий результат дії тих чи інших негативних факторів на ті чи інші об'єкти [16; 93].

Небезпекою, так само, можна назвати стан того чи іншого середовища (природного, господарського, політичного, соціального, техногенного, психофізіологічного тощо), якому притаманна небезпека через наявність різких змін, що завдають шкоди. Іноді небезпеку трактують як можливість втрати істотних властивостей або цілісності через незадоволення будь-яких потреб.

Усвідомлюючи поняття небезпеки, необхідно пам'ятати, що тут мається на увазі лише потенційна можливість нещастя, а не саме нещастя. Це нагадування необхідно тому, що на практиці іноді плутають небезпеку з її реалізацією. Час від часу небезпеки реалізуються і стають фактом життя,

перетворюючись з потенційного стану в різного виду реальні негативні події − стихійні лиха, аварії тощо. Виникають ураження, збитки, інші негативні наслідки цих подій. В результаті на будь-яких ділянках, місцевостях, територіях можуть скластися надзвичайні ситуації різного масштабу.

Теорія та практика національної безпеки та їх окремих типів ґрунтуються на аналізі тріади таких елементів: життєво важливі інтереси-загрози (небезпека) - захист (забезпечення безпеки).

Важливі життєві інтереси включають захист життя та здоров'я людини, а також захист власності людини від надзвичайних ситуацій у мирний час та воєнний час та терористичних актів [16; 56].

У цьому випадку до життєвих інтересів суспільства слід віднести запобігання надзвичайним ситуаціям та інших екстремальних ситуацій, спричинених аваріями, катастрофами, природними та іншими катастрофами, терористичними актами та при веденні військових дій або небезпеками, спричиненими цими діями.

До життєво важливих інтересів держави слід віднести:

- забезпечити ефективний захист населення та критично важливих об'єктів на території Україні при надзвичайних ситуаціях і терористичних актах;

- забезпечити захист та виживання населення у воєнний час;

- збереження об'єктів, істотно необхідних для стійкого функціонування економіки та виживання населення.

Забезпечення безпеки передбачає систему певних заходів і дій, здійснюваних на державному, регіональному, територіальному й інших рівнях, які забезпечували б встановлення і підтримання стану захисту населення та територій [16; 94; 125].

Основними завданнями державного управління стосовно забезпечення безпеки населення та критично важливих об'єктів є: створення комплексу правових, організаційних, технологічних, інженерно-технічних та інших заходів

залежно від можливих загроз призначених на попередження аварій, катастроф на небезпечних об’єктах, а також підготовка для підтримки необхідних сил і засобів.

У дисертації населення означає громадян України, іноземних громадян та осіб без громадянства, які перебувають на території України. До критично важливих об'єктів України в дисертації належать об'єкти, порушення функціонування яких призводить до:

- втрати управління;

- руйнування інфраструктури;

- незворотних негативних наслідків або істотного погіршення безпеки і життєдіяльності населення [56; 93].

У цьому випадку концепція "забезпечення безпеки населення та захисту критичних об'єктів у надзвичайних ситуаціях та терористичних актах означатиме набір взаємопов'язаних програмних цілей та ресурсів, спрямованих на запобігання чи скорочення:

- втрат серед населення;

- загроз життю та здоров'ю населення;

- пошкодження виробничих та соціальних об'єктів, навколишнього середовища від надзвичайних ситуацій природного та техногенного характеру, терористичних актів, а також від впливу сучасних засобів ураження.

Одним із основних рушійних мотивів розвитку людського суспільства є усвідомлена необхідність піклуватися про продовження людського роду. При цьому суспільство прагне забезпечити певний рівень безпеки, прийнятний для всіх його членів, але який може відрізнятися від рівня безпеки, відповідного індивідуальним перевагам деяких членів суспільства. Істотно відрізняються також індивідуальні здібності людей оцінювати небезпеку і усвідомлювати обґрунтованість пропонованих суспільством критеріїв, нормативів і заходів по забезпеченню безпеки [6; 125].

Оскільки цивілізоване суспільство свідомо витрачає на цілі забезпечення безпеки дедалі більшу частину своїх ресурсів, бажано досягнення згоди серед його членів для оптимального розподілу цих хоча і великих, але все-таки обмежених коштів. Проблема створення науково-методологічної основи для раціонального управління безпекою території виникає тільки в контексті наявних у суспільства ресурсів для досягнення цілей безпеки.

Сучасне розуміння національної безпеки та, особливо, регіональної безпеки відображає тісний зв'язок та взаємозалежність безпеки особистості, суспільства та держави на всіх рівнях − від регіонального до конкретно місцевого. Правове регулювання питань національної безпеки України здійснюється достатньою кількістю законів, указів Президента України та постанов Уряду України, а також багатьох інших підзаконних актів. Але, незважаючи на наявні великі кількісні масштаби, законодавча база в галузі національної безпеки носить здебільшого фрагментарний характер, перш за все стосовно до територіального рівня [88, с. 11−15].

У той же час явна недооцінка діяльності забезпечення національної безпеки на регіональному та місцевому рівнях свідчить про надзвичайно низький рівень теоретичної та практичної компетентності органів державної влади. Складається враження, що інтереси людей можуть реалізовуватися і захищатися тільки на загальнодержавному рівні. Але це зовсім не так. Люди живуть в конкретній місцевості, в конкретному регіоні і вимагають задоволення своїх матеріальних і духовних потреб, а також захисту своїх інтересів не тільки на загальнодержавному рівні, а й в регіонах [94; 125].

Заперечення регіональних інтересів найвиразніше відбито в характеристиці національних економічних інтересів. Подібне ставлення до таких актуальних регіональних проблем свідчить про збереження традиційного для України ставлення до людини з боку держави і не сприяє просуванню країни демократичним шляхом розвитку.

Односпрямованість процесу формування інтересів регіонів пояснюється загальним низьким рівнем пізнання сутності інтересів і їх ролі в суспільному житті. Поки ж в публікаціях по цій проблемі лише передбачається, що всередині суспільства на рівні особистості і спільнот є інтереси, відмінні від державних.

Економічні інтереси регіональних спільнот здебільшого розглядаються лише крізь призму державних інтересів. Але державні інтереси і регіональні інтереси в галузі економіки не завжди збігаються [29, с. 15−17].

На практиці регіональна економічна політика виявилася зведена до міжбюджетних відносин, хоча регулярно ставиться завдання підтримувати ініціативи регіонів стосовно територіального розвитку.

Економічні інтереси населення регіонів багато в чому визначаються нерівномірним розвитком територій. Існуюча типологія регіонів України мало пов'язана з ринковим станом. Формування ефективної економіки і вирівнювання процесів розвитку територій відповідають економічним інтересам територіальних спільнот і служать основою для консолідації населення під ідеєю загальнонаціонального інтересу.

Національні інтереси України в політичній стабільності в значній мірі пов'язані з інтересами особистості і регіональної спільності.

Базовими принципами політичної стабільності є такі:

- розвинене місцеве самоврядування;
- демократичні вибори;
- законність і безпека громадян;
- дієва незалежна судова система.

Разом з тим, реальна практика свідчить, що політичні процеси в суспільстві перехідного періоду розвиваються часом драматично, а політична система в вигляді державних структур функціонує недостатньо ефективно. Очевидно, що в політичних процесах повинні велику роль відігравати недержавні суспільно політичні структури низової ланки, а також територіальні

і національні спільноти. Підміна політичних інтересів громадян і особистостей інтересами політичних еліт гальмує прогресивні зміни в суспільстві, становлення громадянського миру та злагоди, заважає формуванню громадянського суспільства.

У структурі інтересів регіональних спільнот особливе місце займають інтереси в соціальній сфері. Гармонійна соціальна структура − це гарантія громадянського миру та злагоди в суспільстві. Від профілю соціальної структури залежать мотивація праці, моральність. Таким чином, соціальна справедливість створює атмосферу взаєморозуміння.

Власне людина та соціалізація особистості визначаються станом соціуму, а також ступенем задоволення соціальних інтересів людей. Разом з тим, соціальні інтереси формуються безпосередньо в первинних соціальних групах, спільнотах і лише потім стають предметом вивчення і реалізації державних, громадських, політичних структур [229, с. 152−173].

Українське суспільство історично склалося на гетерогенній основі. Велика територія країни, безліч народів, культурних традицій, різних релігійних конфесій, неоднаковий психічний склад, особливості трудових, побутових, культурних тощо факторів багато в чому визначають інтереси регіональних спільнот.

Відповідно різний зміст і специфічні особливості регіональних інтересів на території країни позначаються на характері діяльності щодо їх захисту, тобто на характері діяльності щодо забезпечення безпеки регіону. В результаті стабільність положення і безпека регіонів визначають і рівень національної безпеки в цілому.

Дана обставина свідчить про необхідність розгляду стану національної безпеки, і, в першу чергу, − внутрішньої безпеки не тільки за сферами життєдіяльності, а й в територіальному розрізі. Тому велику теоретичну і

практичну значимість представляє оцінка ролі і місця регіональної безпеки в загальній системі внутрішньої безпеки країни.

При вивченні проблем регіональної безпеки найважливіше методологічне значення має вирішення питання − що розуміти під категорією "регіон". Слід зазначити, що в нашій країні до цих пір не вироблено єдиного, загальноприйнятого або якось узаконеного чіткого і однозначного визначення цього поняття [110, с. 102−115].

Регіон відрізняється:

- своєрідністю природних умов;
- спеціалізацією виробництва, що склалася;
- певним рівнем розвитку продуктивних сил;
- виробничою інфраструктурою;
- специфікою соціальної структури;
- способом життя населення.

Якщо регіональна економіка вивчає проблеми раціонального розміщення продуктивних сил, що визначається природними і трудовими ресурсами, то соціальний підхід передбачає обґрунтування шляхів і форм забезпечення порівняно рівних соціальних умов життя населення в різних регіонах країни, розвитку духовної культури населення в рамках історичних традицій тощо. Тому регіон − це самодостатній соціальний організм, що знаходиться в єдності з середовищем, та володіє фізико-географічними, культурно-цивілізаційними, еколого-економічними, етноісторичними, політико-адміністративними і правовими властивостями, та виступає засобом формування і функціонування держави.

Регіони, як і в цілому держава, прив'язані до географічного середовища і мають політико-адміністративний зміст, який пов'язаний з:

- типом і формою державності;
- регіональним заломленням взаємин з іншими державами;

- характером кордонів;

- функціонуванням партій, громадських рухів, засобів масової інформації.

У деяких публікаціях зазначається, що регіон − це не просто географічний простір або сукупність людей, що в ньому живуть. Необхідність виділення регіонів обумовлена, зокрема, адміністративними вимогами розвитку інфраструктури (наприклад, водопостачання, телефонний зв'язок), причому створені з урахуванням цих вимог регіональні одиниці можуть перетинатися і піддаватися постійним змінам. Однак політичного значення регіони набувають лише в тому випадку, якщо більшість жителів регіонів вважає їх існування необхідним, і суспільство в цілому робить з цього необхідні висновки.

Таким чином, регіональну безпеку слід розуміти як захист інтересів регіонів від внутрішніх і зовнішніх загроз. Зовнішніми загрозами при цьому є ті загрози, джерела яких розташовуються за межами даного регіону.

Цей факт ще більше підкреслює, що регіональна безпека повинна забезпечуватися силами та засобами даного регіону у тісній співпраці та за підтримки відповідних сил та засобів держави та інших регіонів. А для цього потрібна відповідна правова база та механізм її реалізації [29, с. 60−61].

Критичні об'єкти - об'єкти, порушення чи припинення функціонування яких призводить до втрати управління економікою України, її регіонів чи муніципалітетів, а також до значного зниження безпеки життєдіяльності населення, яке проживає в цих районах протягом тривалого.

Категоризацію критично важливих об'єктів слід проводити незалежно від належності відомства та типу об'єкта. Метою категоріювання є пред'явлення кількісних і якісних вимог до системи фізичного захисту. Ці вимоги пред'являються залежно від рівня втрат і присвоєної у відповідності з ним категорією об'єкта. Категорія об'єкта повинна визначатися на основі оцінки потенційної небезпеки об'єкта, при цьому повинна враховуватися ймовірність наступних видів та масштабів втрат [65, с. 278−280].

До видів втрат відносяться наступні:

- політичні (визначаються зниженням авторитету для всіх рівнів влади та загальною нестабільністю, що виникає в результаті цього);

- людські (виражаються в загрозі життю і здоров'ю людей);

- фінансові (виражаються в безпосередній втрати матеріальних цінностей в результаті надзвичайної ситуації);

- економічні (враховують витрати на переселення людей із зони надзвичайної ситуації, а також подальші виплати на компенсацію завданих збитків);

- культурні (полягають у втрати художніх цінностей, пам'яток архітектури та історії, конфіденційної інформації та передових технологій);

- екологічні (враховують шкоду, заподіяну природним ресурсам).

Крім того, повинні визначатися втрати для наступних шести масштабів:

- локального (збиток проявляється в межах території об'єкта);

- місцевого (збиток проявляється в межах населеного пункту, в якому розташований об'єкт);

- територіального (збиток проявляється в межах регіону України);

- регіонального (збиток проявляється в межах двох регіонів України);

- державного (збиток проявляється в межах більш ніж регіонів України);

- міждержавного (збиток виходить за межі України).

У випадках категоріювання об'єктів критичної інфраструктури потрібно створити комісію з категоріювання, і першою дією комісії є складання переліку процесів організації:

- управлінських;

- технологічних;

- виробничих;

- фінансово-економічних тощо, в яких використовуються об'єкти інфраструктури. Формально правила категоріювання передбачають включення

до переліку взагалі всіх процесів, але в реальності процеси, пов'язані виключно з ручною або механізованою працею потім все одно будуть виключені з розгляду [68, с. 91−92].

Далі, для кожного процесу необхідно визначити, чи може його порушення чи припинення спричинити негативні соціальні, політичні, економічні, екологічні наслідки, а також наслідки для забезпечення оборони країни, державної безпеки та правопорядку. Самі правила не визначають того, які саме наслідки повинні розглядатися.

Процеси, порушення яких може привести до таких наслідків, називаються критичними, а решта з подальшого розгляду виключаються. Слід зазначити, що можливість негативних наслідків, які роблять процес критичним, не завжди очевидна. На перший погляд, процеси бухгалтерського обліку та взаєморозрахунків з контрагентами не можуть істотно впливати на виробничу діяльність, і в більшості організацій це саме так. Але, наприклад, на деяких підприємствах припинення бухгалтерських операцій може призвести до затримки оплати матеріалів і, як наслідок, припинення поставок, зупинку виробництва і зриву термінів виконання державного оборонного замовлення − наслідку, який саме для цього підприємства робить процеси бухгалтерського обліку критичними.

Далі для кожного критичного процесу визначаються об'єкти інфраструктури, що використовуються в процесі − вони і стануть об'єктами критичної інфраструктури, які комісія повинна категоризувати. Критичні процеси, які не використовують об'єкти критичної інфраструктури, з подальшого розгляду виключаються. Усі визначені таким чином об'єкти критичної інфраструктури включені до єдиного списку, який слід надіслати державним органам [17; 22].

Далі для кожного об'єкта критичної інфраструктури слід оцінити відповідні негативні наслідки нападу на цей об’єкт та масштаб таких наслідків.

Це вже творча робота, аналогічна аналізу загроз, яка повинна проводитися при створенні системи захисту. Складність полягає в тому, що:

- кожен об'єкт може використовуватися в декількох критичних процесах;

- один і той же об'єкт можна атакувати різними способами, і це буде проводити до різних наслідків для різних процесів.

В результаті аналізу необхідно оцінити для кожного об'єкта критичної інфраструктури за кожним показником категоризації максимально можливу шкалу негативних наслідків, що відповідають даному показнику. Нарешті, на основі цієї оцінки потрібно для кожного показника категоріювання визначити, якій категорії значущості відповідає даний об'єкт критичної інфраструктури за даним показником.

В результаті об'єкту присвоюється максимальна з категорій і складається акт категоріювання [65; 68].

Відомості про результати категоріювання включаються у спеціальну форму.

Для категоризації критичних об'єктів за групами пропонується ввести як критерій характер та масштаб можливих втрат у випадку реалізації основних загроз безпеці об'єкта.

Таким чином, державне управління суспільними відносинами у галузі захисту критичних об'єктів - це вплив державної влади на суспільні відносини через систему правових засобів захисту, до яких, зокрема, належать верховенство права, правовідносини, правозастосовчі акти.

Державне управління суспільними відносинами у сфері захисту критичних об'єктів - це реалізація національного правового управління, об'єктом якого є внутрішні суспільні відносини.

Слід зазначити, що врегулювання групи суспільних відносин здійснюється не лише правовими засобами, але й іншими, насамперед політичними та моральними.

Об'єктом державного управління можуть бути лише ті відносини, які можуть об'єктивно регулюватися законом, тобто мають нормативний характер і знаходяться у сфері соціального простору, в якій право здатне чинити прогресивне перетворюючий вплив на суспільне життя. Крім того, врегулювання цих відносин має бути доцільним, ефективним.

Система всіх правових засобів, методів та способів, за допомогою яких здійснюється державне управління суспільними відносинами у галузі охорони критичних об'єктів, формує нормативно-правовий механізм державного регулювання у сфері охорони критичної інфраструктури [23; 110].

Слід зазначити, що серед категорій критичних об'єктів, що підлягають державному управлінню, планується виділити наступне:

- об'єкти, що реалізують важливі функції державного управління;
- об'єкти безпеки життєдіяльності населення, транспортне призначення;
- потенційно небезпечні об'єкти;
- об'єкти оборонного призначення;
- об'єкти з постійним або періодичним масовим зібранням людей;
- об'єкти історії та культури.

Зокрема, функціональне призначення об'єктів, які реалізують важливі функції державного управління, полягає в наступному:

- державне управління загалом;
- управління конкретною територією;
- управління окремою групою державних органів.

Серед основних загроз для закладів, які реалізують важливі функції державного управління, слід відзначити надзвичайні ситуації. Слід зазначити, що характер можливих втрат внаслідок реалізації ключових загроз передбачає:

- втрата контролю над територією;
- паніку;
- людські жертви;

- матеріальні збитки.

Щодо об’єктів життєзабезпечення населення, транспортних цілей, то їх функції включають наступне:

- забезпечення населення та організацій запасами води, газу, тепла та енергопостачанням;

- забезпечення транспортних перевезень (тунелі, мости, метро).

Надзвичайні ситуації являються ключовою загрозою для об'єктів життєзабезпечення населення та транспортного призначення. Щодо можливих наслідків виникнення та поширення надзвичайних ситуацій на цих об'єктах , ми повинні зосередитись на наступних питаннях:

- заподіяння шкоди здоров'ю людини, матеріальних збитків;

- відсутність транспортних шляхів сполучення.

Потенційно небезпечні об'єкти передбачають:

- виробництво, зберігання, транспортування і переробка ядерних та хімічних речовин;

- наявність гідротехнічних споруд.

Ключові загрози в цьому випадку - надзвичайні ситуації та розкрадання небезпечних речовин, внаслідок чого можливо наступне:

- шкода здоров'ю та життю персоналу підприємства, а також населенню за межами території об'єкта;

- катастрофічний вплив на навколишнє середовище.

Об'єкти оборонного призначення забезпечують оборонні можливості країни. Серед основних загроз їх функціонуванню слід також виділити надзвичайні ситуації, внаслідок виникнення та поширення яких може знизитись рівень обороноздатності держави [9; 241].

Об'єкти з постійним або періодичним масовим збиранням людей передбачають:

- вираження політичних поглядів;

- мітинги;

- демонстрації;

- масові народні свята.

Стабільному функціонуванню цих об'єктів також загрожують надзвичайні ситуації, які можуть призвести до паніки та завдати шкоди життю та здоров’ю людини.

Призначенням об'єктів історії та культури є:

- просвітництво населення;

- збереження пам’ятників історії та культури.

Загрозами у цьому випадку являються надзвичайні ситуації, а також розкрадання культурно-історичних цінностей. Одним із наслідків, які слід зазначити, є те, що відвідування цих місць може завдати шкоди здоров’ю та життю людини, а також втрати пам’ятників історії та культури.

Особливості аналізу загроз при категоріюванні об'єктів критичної інфраструктури полягають в тому, що суб'єкти категоріювання часто плутають ці два поняття:

- аналіз загроз, який проводиться при створенні системи безпеки значимого об'єкта критичної інфраструктури;

- оцінка негативних наслідків інциденту з об'єктом критичної інфраструктури, яка проводиться при категоріюванні [68; 125].

У першому випадку вирішується завдання вибору заходів захисту і способів їх реалізації. Щоб вибрати адекватну реалізацію заходів захисту (наприклад, чи доцільно для захисту від мережевих атак застосовувати міжмережевий екран прикладного рівня або досить обійтися сигнатурною системою виявлення вторгнень), потрібно оцінити всі можливі способи проведення атак - і для цього пропонується використовувати Банк даних загроз і вразливостей.

Для оцінки негативних наслідків порушення роботи об'єкта критичної інфраструктури цей рівень деталізації являється марним, в деяких випадках - неможливим, а головне - не потрібним.

Описаний процес доцільно розглянути на прикладі теплопостачання. На стадії категоріювання в загальних рисах відомий технологічний процес теплопостачання:

- водогрійні котли нагрівають воду;

- насоси нагнітають холодну воду в котли, а гарячу − в труби теплотраси;

- подача води в окремі ділянки труби регулюється засувками, тиск води контролюється датчикам, перевищення допустимих показників призводить до дію аварійний захист [17; 22; 65].

Всі перераховані компоненти управляються автоматизовано. На стадії категоріювання слід прийняти в якості аксіоми, що якщо не забезпечувати захист системи від дій зловмисника, то він може впливати на елементи системи управління. Виходячи з цього, необхідно оцінити потенційно можливі сценарії дій зловмисника, маючи на меті заподіяння максимального збитку. Наприклад, порушник потенційно може відключити аварійний захист, перекрити засувку на виході водогрійного котла і збільшити до максимуму потужність насоса, що нагнітає воду в котел. Результатом потенційно може стати пошкодження котла, як наслідок − порушення теплопостачання підключених до котельні споживачів. Для оцінки можливості такого сценарію не потрібно оцінювати, чи можливо впровадження шкідливого коду або даних в програмне забезпечення системи управління котельнею чи інші загрози, перераховані в банку даних. Досить того, що система управління дозволяє людині, яка отримала до них доступ, виконати подібні дії, і це підтверджує фахівець зі служби головного інженера організації. При оцінці негативних наслідків суб'єкти критичної інфраструктури часто намагаються врахувати заходи захисту, що вживаються, наприклад:

- у системі управління реалізований комплекс заходів захисту, що виключає несанкціоновані дії зловмисника;

- у котельні встановлено два котли, які в штатному режимі працюють з половинним навантаженням.

У подібному підході присутні відразу три методичних помилки. По-перше, порушений причинно-наслідковий зв'язок: спершу оцінюються загрози, і тільки потім вибираються відповідні їм заходи захисту. Повне резервування котлів тому і виконується, що вихід з ладу одного з них привів би до порушення теплопостачання споживачів.

По-друге, у разі категоріювання об'єктів критичної інфраструктури загрози визначають категорію значущості, а категорію значимості - склад основних заходів захисту, які мають бути здійснені на об'єкті критичної інфраструктури.

На стадії категоріювання ще не визначена категорія значущості об'єкта, а, відповідно, не визначено, які заходи захисту є необхідними. Тому на цій стадії у суб'єкта немає ніяких підстав стверджувати, що вжиті ним заходи захисту достатні [68; 82; 145].

По-третє, правила категоріювання вимагають при оцінці наслідків враховувати також і взаємозв'язок об'єктів, включаючи можливість комбінованої атаки на них. Якщо порушник здатний провести атаку на один котел, то він здатний точно так же провести атаку і на другий котел, а значить, при категоріювання системи управління доведеться враховувати можливість виведення з ладу всіх котлів.

Будь-які фізичні, хімічні процеси, об'єкти техногенної діяльності, природні об'єкти, системи контролю параметрів навколишнього середовища є елементами складної системи, що представляють взаємопов'язані елементи на виділеній території.:

- взаємозв'язок всіх елементів;

- єдність із зовнішнім середовищем;

- система може бути елементом іншої системи вищого порядку (наприклад, більш великої території);

- серед об'єктів технічної діяльності існують об'єкти різного класу небезпеки;

- одним з елементів системи є населений пункт.

Основним завданням забезпечення безпеки об'єктів критичної інфраструктури є швидке отримання інформації про загрозу та її використання для здійснення адекватних заходів безпеки. При цьому велике значення мають питання обладнання та технології побудови автоматизованих систем забезпечення безпеки життєдіяльності міст, ситуаційних та кризових центрів, організація відео спостереження територій, обладнання найбільш відповідальних елементів інфраструктури за допомогою екстреного виклику оперативних підрозділів тощо [56; 125; 145].

Питання концептуального плану визначають вибір правильного підходу до вирішення проблем запобігання загрозам для об'єктів критичній інфраструктури, вимоги до функціональних властивостей систем безпеки та ідеології їх побудови повинні бути дуже цікавими для суб’єктів, що займаються питаннями безпеки. Перш ніж вирішувати питання, як захищати, необхідно визначитися з тим, що захищати, від чого і до якої міри. Саме в такій послідовності вирішуються завдання побудови систем безпеки об'єктів критичної інфраструктури.

Розглядаючи всю сукупність загроз, їх можна умовно розділити на дві групи:

- загрози для критично важливого об'єкту;

- загрози від критично важливого об'єкту.

Зокрема, перша група об'єднує типові внутрішні загрози (локальні пошкодження систем життєзабезпечення, злочинність, крадіжки,

правопорушення, вчинені на побутовій основі, нещасні випадки тощо) [138; 241].

На запобігання цих загроз спрямована повсякденна діяльність правоохоронних органів і внутрішніх структур безпеки об'єктів.

Друга група поєднує загрози, які становлять небезпеку життєдіяльності населення, навколишніх населених пунктів, які є джерелом найбільш критичних об'єктів.

Виникнення різних надзвичайних ситуацій у цих об'єктах та територіях через природні та техногенні явища чи несанкціоновані дії порушників може призвести до серйозних порушень у життєдіяльності населення.

Між обома групами загроз існує певний взаємозв'язок, однак саме загрози безпеки життєдіяльності, як найбільш складні та мало вивчені, підлягатимуть подальшому розгляду. При цьому основна увага буде приділена загрозам, реалізованим несанкціонованими діями порушників.

Загрози для критично важливих об'єктів можна розділити на наступні групи:

- загрози критично для важливих об'єктів міста, оснащених системами безпеки;

- загрози об'єктам і територіям, що не оснащені системами безпеки.

З точки зору здійснення перша категорія загроз володіє наступними характерними особливостями:

- можливість реалізації як в робочий, так і в неробочий час;

- можливість змови з персоналом об'єкта, що істотно спрощує проведення акції;

- можливість проведення акції порівняно невеликим числом виконавців без залучення терористів-смертників;

- можливість вибору для проведення акції об'єкта, який володіє найбільшою вразливістю, що дозволяє виконати максимальну кількість дій приховано;

- наявність достатнього часу для підготовки акції;

- досить серйозні для життєдіяльності населення наслідки.

До особливостей другої категорії загроз слід віднести:

- доцільність проведення акції тільки в разі масового скупчення на критично важливому об'єкті людей;

- спрямованість акції або на заподіяння шкоди життю і здоров'ю людей (пожежа, вибух, дія небезпечних речовин), або на психічний вплив (захоплення в заручники);

- високий політичний і психологічний резонанс на міському, регіональному та загальнодержавному рівнях при реалізації загроз;

- потреба в залученні до реалізації загроз смертників;

- обмеженість у часі для підготовки і проведення акції.

У порівнянні з загрозами першої групи, загрози безпеки життєдіяльності міста відрізняють здійсненність при наявності у виконавців професійних навичок, озброєння і оснащення, а також на необхідності ґрунтовної підготовки акції (збір інформації про об'єкт, наймання виконавців, поетапна доставка необхідних предметів в безпосередню близькість до місця акції тощо) [125; 138].

Традиційно до складу первинних функцій систем безпеки об'єктів входять:

- виявлення загрози;

- затримка загрози;

- реагування.

Забезпечення безпеки критично важливих об'єктів ускладнюється наступними факторами:

- безперешкодність пересування населення і транспорту всередині і / або поблизу життєво важливих об'єктів (за винятком особливих випадків);

- критично важливі об'єкти знаходяться в різних формах власності;

- існуючі критично важливі об'єкти потребують різних рівнів безпеки;

- наявність на критично важливому об'єкті власної системи (служби) безпеки, при цьому можлива відсутність узгодженості між діями власної служби безпеки і спеціалізованих органів по ліквідації надзвичайних ситуацій;

- розподіл функцій забезпечення безпеки в межах одного населеного пункту між позавідомчими, відомчими і приватними охоронними структурами;

- єдині для всіх об'єктів і територій системи життєзабезпечення (електропостачання, теплопостачання, водопостачання і каналізація, громадський транспорт, міська телефонна мережа, вуличне освітлення тощо);

- порушення їх функціонування може призвести до можливості виникнення надзвичайної ситуації на критично важливому об'єкті.

Наявність засобів масової інформації є позитивним фактором забезпечення безпеки на критично важливих об'єктах. Однак у деяких випадках засоби масової інформації можуть ненавмисно спровокувати надзвичайні ситуації - насамперед через непрофесіоналізм людей, які працюють у ЗМІ та недотримання закону про секретність. Безперечно, наявність загальних систем реагування на надзвичайні ситуації (ситуаційно-кризові центри, системи громадського попередження тощо) відіграє позитивну роль у забезпеченні безпеки на критично важливих об'єктах [16; 138].

Зазначені чинники дещо видозмінюють можливості реалізації первинних функцій безпеки, що необхідно враховувати при виробленні підходів до вирішення завдань безпеки в місті. Зокрема, їх попередній аналіз показує, що з точки зору міської інфраструктури найскладнішими та найважливішими завданнями є запобігання та виявлення загроз життю на територіях та об'єктах, не обладнаних власними системами безпеки.

Основне навантаження в рішенні цих завдань лежить на міських силових структурах і їх підрозділах. Вагомим фактором підвищення ефективності їх роботи, крім оперативної інформації, є безпосередній моніторинг безпеки об’єктів та територій міста, детектування тривожних ситуацій з передачею інформації оперативним підрозділам, а також контроль ввезення і переміщення в межах міста небезпечних для життєдіяльності речовин (ядерних і радіоактивних матеріалів, хімічних речовин, біологічних засобів тощо). Чимале значення має приділятися інформації, що одержується від населення [90; 172].

З урахуванням усіх очевидних технічних рішень, що реалізують ці функції, попередньо повинні бути визначені інформаційні ознаки, що вказують на виникнення надзвичайної ситуації, оптимізовані обсяги та послідовність переданих фрагментів інформації та встановлення їх споживачів. Вирішення цього завдання має здійснюватися на основі відповідної інформаційної моделі.

Ефективність вирішення завдання припинення загрози в значній мірі визначається умовами її первинного виявлення. У міському середовищі виявлення загрози, спрямованої проти потенційно небезпечних і критично важливих об'єктів, здійснюється засобами виявлення їх власних систем безпеки (при наявності таких), що розміщуються на кордонах об'єктів. Умова, за якої виявлена загроза буде припинена, буде залежати від двох чинників: часу стримування загрози елементами системи безпеки об'єкта та часу прибуття оперативного підрозділу міста до місця акції. Вважаючи, що другий фактор є фіксованим для конкретного об'єкта в силу його віддаленості від оперативного підрозділу, можна визначити, яким має бути мінімально допустимий час стримування загрози службою безпеки об'єкта. Таким чином, загальні технічні вимоги, що визначають структуру та склад служби безпеки залежно від відомчої належності об'єкта, доповнюються функціональною вимогою (час стримування загрози), яка встановлюється конкретними міськими умовами.

Ефективність припинення загрози, спрямованої проти об'єктів або територій, які не мають власних служб безпеки, буде визначатися переважно можливостями міських засобів виявлення і близькістю знаходження до місця акції сил оперативних підрозділів.

Фактор раптовості, властивий початку прояви загрози в міських умовах, висуває в якості одного з основних завдань ідентифікацію передкризової (попередньої виникненню загрози) ситуації, що дозволить силам реагування впровадити необхідні попереджувальні дії. Ознаками такої ситуації можуть бути:

- неадекватна поведінка людей в місцях масового скупчення;

- безконтрольно залишені предмети;

- досягнення параметрів систем життєзабезпечення значень, близьких до критичних.

Визначення сукупності цих ознак для кожного відповідального елемента інфраструктури міста, за якими може бути здійснена автоматична генерація гіпотез передкризової ситуації, є одним із завдань, що передують вибору і реалізації технічних рішень.

Таким чином, адекватність та достатність проектних рішень, спрямованих на забезпечення безпеки життєдіяльності міста, досягаються попередніми обґрунтуванням вимог до функціональних властивостей систем та засобів безпеки, які, у свою чергу, визначаються на основі аналізу загроз потенційно небезпечним і критично важливим об'єктам міста та інших відповідальних елементів його інфраструктури [56; 125; 138].

1.2. Механізми державного управління захистом об'єктів критичної інфраструктури

У найзагальнішому і приблизному вигляді можна вважати, що в сучасний період перед державним і муніципальним управлінням об'єктивно стоять такі цілі.

1. Формування нових інститутів державної влади регіонів України та оптимізація діяльності існуючої системи виконавчої влади (адміністративна реформа).

2. Розгортання та зміцнення соціальних інститутів, які забезпечують стійку демократію суспільства та держави.

3. Створення та впровадження в життя соціальних та адміністративно-правових регуляторних органів, які гарантують конституційний набір прав, свобод та обов'язків громадян України

4. Формування та практична реалізація державної політики, спрямованої на забезпечення громадської безпеки та захисту критичної інфраструктури

5. Забезпечення внутрішньої та зовнішньої безпеки регіонів України та сприятливих мирних умов для їх життєдіяльності

6. Досягнення гармонійного, збалансованого і взаємопов'язаного розвитку регіонів у взаємодії з державою на основі поглиблення процесів формування і функціонування загальноукраїнського ринку.

Проблему встановлення цілей у державному управлінні можна розглядати не стільки як відкритість та вираження конкретних цілей, спрямованих на реалізацію держави скільки в побудові "дерева цілей", в яких стратегічні, оперативні та тактичні цілі, кінцеві та проміжні, державні та приватні, віддалені та тісно узгоджені, пов'язані та становлять певну логічну цілісність. [10, с. 100−185].

Важливо також з'єднати "дерево цілей" з необхідними й адекватними їм засобами, ресурсами, методами і формами їх реалізації, бо, як відомо з історії, досить часто несправедливі засоби, методи і форми спотворювали в результаті найблагороднішi цілі.

Цілепокладання в державному управлінні об'єктивно пов'язано зі стратегічними національними інтересами і України. Національна стратегія об'єднує суспільство і державу, класи і особистість, нації і регіони, концентрує енергію руху. Вироблення такої об'єднуючої національної стратегії для України − це актуальне завдання, реалізація якого закладе міцний фундамент для її зовнішньої і внутрішньої політики.

Питання про зміст та структуру функцій державного управління у сфері громадської безпеки та захисту критично важливих об'єктів пов’язане з визначенням місця та ролі регіону у певній сфері життєдіяльності. Саме місце і роль регіону припускають його зміст і форму, а потім функції управління й інші прояви [78; 79].

У даній роботі функції державного та муніципального управління розуміються як об'єктивно визначені типи влади, цілепокладання, впорядкування та регулювання впливу системи державних органів на певні процеси в суспільстві, природі тощо. Ці дії відображаються певним чином на об'єктах, в тому числі на свідомості, поведінці і діяльності людей.

Сьогодні всі питання державного управління зосереджені як ніколи на проблемі забезпечення національної безпеки України. Управління безпекою в різних сферах життєдіяльності особистості, суспільства і держави, а також пошук ефективних шляхів вирішення поставлених перед суспільством проблем проникають в інтереси всіх груп населення, партій, вчених і практиків [88; 241].

Очевидно, що серед найгостріших економічних, продовольчих, енергетичних, соціальних, політичних та інших проблем, які наша країна має вирішити у XXI столітті, особливо на етапі переходу до прогресу сталого

розвитку, самі по собі проблеми природної та техногенної безпеки не є провідними. Але не можна не враховувати, що вони мають значний вплив на стан економічної, екологічної та соціальної безпеки [34; 47].

"Набір" функцій державного управління залежить, з одного боку, від стану та структури керованих процесів − сукупності керованих об'єктів, а з іншого − від місця та ролі держави у сферах життєдіяльності.

Держава пов'язана з суспільством, її діяльність невільно визначається потребами й інтересами суспільного розвитку. Дану взаємозалежність особливо важливо підкреслити, оскільки у багатьох політичних заявах та виступах засобів масової інформації постійно висувається теза про те, що держава не повинна впливати на суспільство, не повинно заважати його свободі, а також відкрити простір творчості. Однак вивільнення суспільства, його окремих відносин, процесів, явищ від цілепокладаючих, організуючих і регулюючих впливів держави передбачає, що замість них працюватимуть самоврядувальні механізми (економічні, соціальні, культурні, інформаційні тощо), що підтримують досягнутий рівень організованості та урегульованості, інакше в суспільстві виникає стан некерованості, свавілля, анархії і хаосу.

В сучасних умовах проявляються суперечливі суспільні потреби зменшення і зростання ролі держави. Зокрема, перша полягає в скороченні директивного управління та зменшенні державного сектора економіки і державного втручання в господарський процес.

Друга полягає у:

- розширенні функцій держави;

- створенні ринкової інфраструктури;

- формуванні нових законодавчо-нормативних процедур господарських відносин і нових відносин власності.

Отже, необхідно відмовитися від механістичних підходів до ролі і місця держави в суспільстві в умовах трансформаційного періоду, а доцільно враховувати складний баланс суперечливих потреб і тенденцій.

Розглядаючи функції державного управління у галузі громадської безпеки та захисту критичної інфраструктури в цій роботі, слід спиратися на аналіз усієї сукупності факторів, що впливають на сучасний період на державні відносини, а також те, що суспільство наразі не готове взяти на себе функції, що виконуються державними установами. Протистояти впливу надзвичайних ситуацій на сталий розвиток України в сучасних умовах можна лише відповідною соціальною організацією суспільства, поклавши відповідну стратегічну роль на державу [46; 53; 161].

У світовій практиці і теорії, що стосується державного управління, менеджменту й інших видів управління, до загальних функцій управління цілком обґрунтовано відносять:

- планування;
- організацію;
- регулювання;
- роботу з персоналом;
- контроль.

Це особливо важливо при оптимізації функцій органів виконавчої влади регіонів України в рамках адміністративної реформи. Відмова від функцій планування та контролю в державному управлінні, де вкрай необхідний перспективний (стратегічний) погляд, навряд чи виправданий, оскільки соціальні процеси, що підлягають державному управлінню, охоплюють десятки мільйонів людей.

На управлінській практиці позначається ігнорування і недооцінка функції організації, що стосується, зокрема, взаємодії різноманітних організаційних структур: замість свідомої організації (як статичної, так і динамічної),

зроблений упор на стихійну самоорганізацію. Однак весь світовий досвід суперечить таким принципам, і практично скрізь організаційний резерв є найважливішим для вирішення проблем суспільного розвитку.

Відповідно, потрібен більш серйозний підхід до реалізації функції регулювання як на законодавчому рівні (створення правил поведінки), так і на виконавчому, що забезпечує практичне дотримання встановлених правил, норм та інших регуляторів. Це дозволило б уникнути існуючих перекосів у сфері забезпечення громадської та особистої безпеки.

Державне управління на рівні регіону України в теоретичному плані достатньо не вивчено. В цьому випадку для формування раціональних структур управління надзвичайно важливо збагнути глибину і складність реальних проблем України в період, коли в країні проводяться адміністративні реформи, а також потрібно зрозуміти закономірності цього періоду і врахувати їх при реформуванні систем управління. При цьому необхідний зважений погляд на стан суспільства, його можливості та перспективи, ресурси, резерви, потенціал і джерела розвитку.

Реформування системи громадської безпеки та захисту об'єктів критичної інфраструктури в надзвичайних ситуаціях та терористичних актах неможливе без здійснення специфіки функцій управління, зокрема, тих, які притаманні саме державі і повинні реалізовуватися за допомогою управлінських функцій спеціальних державних органів [15; 22; 145].

Наукова методологія вимагає розгляду особливостей державного і муніципального управління в Україні щонайменше в чотирьох площинах:

- з точки зору наявності існуючих в країні орієнтацій на вікові традиції, зокрема, політичну культуру населення та правлячі групи (претенденти на владу), які більшою чи меншою мірою визначають реалізацію цієї проблеми. Не обов'язково, щоб ці традиції визначали процес державного управління. Однак

немає сумніву, що заперечення їх у нинішній ситуації в кінцевому рахунку створює тупикову ситуацію.;

- прийняття до уваги сьогоднішнього соціально-політичного й економічного становища. Аналіз цього фактора необхідний, оскільки він дозволяє, з одного боку, вибудовувати розробку рішень поставленої проблеми на реальній основі, з іншого − це дає можливість врахувати минуле, характерне лише для сьогоднішнього моменту, а також зосередитися на дійсно ключових проблемах оптимізації механізмів та структур державного управління;

- прийняття до уваги глобального аспекту завдань державного управління, що вирішуються в Україні. Світовий досвід дає не тільки і не так багато знань про можливі рішення конкретних завдань управління. Глобальний контекст дозволяє будувати запропоновані рішення таким чином, щоб передбачити світові тенденції, зберегти українську самобутність та використовувати справді оптимальні варіанти рішень проблем державного управління:

- використання загальнонаукового принципу подвійної герменевтики, тобто подвійної інтерпретації вирішення поточного дослідного завдання: строго наукового аналізу проблем державного управління, обліку фундаментальних аспектів проблеми, новітніх наукових напрацювань тощо.

Захищеність об'єктів критичної інфраструктури − це стан, при якому у відношенні до об'єктів критичної інфраструктури забезпечуються умови для запобігання виникнення потенційної небезпеки та подолання (зведення до мінімального рівня) негативних наслідків кризових ситуацій природного та техногенного характеру, а також ситуацій, викликаних проявами тероризму [22; 80; 219].

При оцінці захищеності критично важливого об'єкта враховується:

- обсяг впровадження інженерно-технічних заходів для підвищення безпеки;

- наявність і стан діагностичної апаратури і автоматичних систем контролю і регулювання параметрів стану небезпечних елементів об'єкта;

- забезпеченість захисту персоналу об'єкта та населення, що проживає в зоні впливу об'єкта, як джерела надзвичайної ситуації;

- підготовленість об'єкта до роботи в умовах надзвичайних ситуацій;

- повнота проведення заходів щодо запобігання та пом’якшення наслідків надзвичайних ситуацій;

- готовність систем управління до роботи в умовах надзвичайних ситуацій;

- фізична захищеність об'єкта від терористичних актів.

Виконання заходів щодо захисту об'єктів критичної інфраструктури дозволить виконати завдання:

- визначення показників ступеня ризику надзвичайних ситуацій для персоналу небезпечного об'єкта та населення, проживає поблизу;

- визначення можливості виникнення надзвичайних ситуацій;

- оцінки можливих наслідків надзвичайних ситуацій;

- оцінки можливого впливу надзвичайних ситуацій, що сталися на сусідніх небезпечних об'єктах;

- оцінки стану робіт з попередження надзвичайних ситуацій та готовності до ліквідації надзвичайних ситуацій на небезпечному об'єкті;

- розробка заходів щодо зменшення ризику та пом'якшення наслідків надзвичайних ситуацій на небезпечному об'єкті.

Існує необхідність проводити моніторинг небезпечних хімічних та біологічних речовин на території України, а також розробляти пропозиції щодо впровадження першочергових заходів небезпечних хімічних та біологічних об’єктів, територій їх розміщення при здійсненні заходів [130; 172].

- по розробці моделі управління та взаємодії, а також алгоритмів прийняття управлінських рішень на об’єктному, місцевому, регіональному та загальнодержавному рівнях;

- створення базової регіональної системи забезпечення хімічної і біологічної безпеки.

Моніторинг, по суті, полягає в спостереженні за станом та розвитком цих структур, явищ та процесів, а також попередженні надзвичайних ситуацій. Мета моніторингу - інформаційне забезпечення підготовки та прийняття управлінських рішень щодо зміни у правильному напрямку стану системи, явища чи процесу. По-друге, метою моніторингу є вироблення аналітичної інформації, необхідної для проведення досліджень в тій предметній області, де організовується моніторинг. У сфері техногенної, природної й екологічної безпеки, з урахуванням сформованих в Україні поглядів на координуючу роль і розподіл відповідальності в цій сфері між певними державними структурами, доцільна організація трьох основних видів моніторингу:

- моніторингу техногенних небезпек і впливів;

- моніторингу небезпечних явищ і процесів;

- екологічного моніторингу.

Перші два види моніторингу організовуються за координуючій ролі Державної служби України з надзвичайних ситуацій (далі – ДСНС України) в складі Єдиної державної системи цивільного захисту [169; 206].

Екологічний моніторинг, як один з основних перерахованих вище видів моніторингу, має більш широке цільове призначення. Він втілюється в Єдину державну систему цивільного захисту, що забезпечує всі зацікавлені міністерства і відомства, зокрема і Державну службу України з надзвичайних ситуацій, необхідною екологічною інформацією [104; 130].

Включення до єдиної системи сил і засобів великого числа відомств обумовлює наявність широких можливостей у цій системи стосовно рішення

задач комплексного моніторингу. Всі згадані системи, як і десятки інших систем спостереження, контролю, покликаних вирішувати ті чи інші приватні завдання, складають той базис, на якому можуть бути побудовані системи моніторингу техногенних небезпек і впливів небезпечних природних явищ та процесів, а також екологічного моніторингу. Зокрема, система моніторингу техногенних небезпек і впливів об'єднує в своїй структурі на принципах жорстких управлінських зв'язків та інформаційної підтримки комплекс джерел інформації, який дозволив би здійснювати:

-спостереження, оцінку та контроль за станом небезпечних в техногенному відношенні об'єктів, ідентифікації загроз, а також прогноз розвитку ситуації з урахуванням можливих сценаріїв виникнення аварій, катастроф та надзвичайних ситуацій на об'єктах критичної інфраструктури;

- оцінку та прогноз характеру та масштабів наслідків техногенного впливу на об'єкти критичної інфраструктури;

- спостереження, оцінку та прогноз стану навколишнього середовища;

- інформаційну та інтелектуальну підтримку підготовки та прийняття управлінських рішень у сфері забезпечення техногенної безпеки населення та територій, відповідно, об'єктів критичної інфраструктури [34; 145; 214].

Аналогічним чином система моніторингу небезпечних природних явищ та процесів повинна включати комплекс джерел інформації, що забезпечує виконання завдань щодо:

-спостереження, оцінки та прогнозу стану навколишнього середовища, своєчасному виявленню симптомів (ознак), що вказують на виникнення небезпечних природних явищ, процесів, а також прогноз їх розвитку та переростання у надзвичайні ситуації, зокрема, на об'єктах критичної інфраструктури;

- спостереження, оцінки та прогнозу стану характеру та ступеня ураження, що завдається об'єктам критичної інфраструктури;

- інформаційної та інтелектуальної підтримки підготовки та прийняття управлінських рішень у сфері забезпечення природної безпеки.

Система екологічного моніторингу покликана здійснювати:

- спостереження, оцінку та прогноз стану навколишнього середовища за програмами геофізичного, біологічного моніторингів та моніторингу джерел антропогенного впливу;

- інформаційно-інтелектуальну підтримку підготовки та прийняття управлінських рішень, а також проведення наукових досліджень у сфері екологічної безпеки.

Аналіз розглянутих видів моніторингу показує їх глибокий зв’язок із цільовими функціями, особливо щодо спостереження, оцінки та прогнозування стану навколишнього середовища. Разом з тим не можна не бачити і явні особливості, і деякі відмінності в цих цільових функціях. Вони обумовлені характером завдань, які повинні вирішуватися структурами управління, в інтересах яких здійснюється той чи інший вид моніторингу [145; 164].

Цільова функція моніторингу техногенних небезпек і впливів як спостереження, а також оцінки та прогнозування стану навколишнього середовища повинна здійснюватися лише в частині, що стосується впливу цього стану на життєзабезпечення населення і, відповідно, на об'єкти критичної інфраструктури. Крім того, дані про стан довкілля в рамках цього моніторингу необхідні для виявлення тенденцій розвитку ситуації та ознак небезпеки та перетворення її у надзвичайну ситуацію. Аналогічні судження можна зробити і щодо цільових функцій моніторингу, оцінці та прогнозування стану довкілля в процесі моніторингу небезпечних природних явищ та ознак небезпеки їх переростання в надзвичайну ситуацію. Однак розглянута цільова функція значно розширюється в напрямку прогнозування та оцінки динаміки розвитку стану навколишнього середовища та виявлення ознак виникнення небезпечних природних явищ та процесів. Найбільш широко представлена цільова функція

моніторингу, оцінки та прогнозування стану довкілля в екологічному моніторингу.

Таким чином, екологічний моніторинг відноситься до числа заходів, спрямованих, зрештою, на інформаційну підтримку вирішення основних завдань щодо забезпечення екологічної безпеки. Тому мета проведення екологічного моніторингу в загальному випадку може бути сформульована як ідентифікація та оцінка екологічних небезпек, а також інформаційна підтримка процесу підготовки та прийняття управлінських рішень щодо:

- охорони природи та здоров'я людини;

- регулювання та відновлення якості довкілля;

- нормалізації екологічної обстановки в екстремальних випадках.

У зв'язку з тим, що моніторинг навколишнього середовища включає спостереження, оцінку та прогнозування антропогенних змін абіотичної складової біосфери та відповідну реакцію біологічних систем на ці зміни, в її організації та здійсненні є принцип інтегрованого поєднання різних типів моніторинг навколишнього середовища. Як відомо, в залежності від реакції основних складових біосфери на антропогенний вплив, розрізняють геофізичний і біологічний моніторинги.

Зокрема, геофізичний моніторинг включає елементи спостереження, оцінки, прогнозу стану та змін геофізичного середовища (сукупність фізичних процесів та властивостей певної земельної ділянки), тобто зміни абіотичного компонента біосфери, як в мікро-, так і макромасштабі, включаючи забруднення навколишнього середовища різними інгредієнтами (радіоактивними, шкідливими хімічними речовинами тощо), а також реакції великих систем - погоди та клімату [69; 72].

Основним завданням біологічного моніторингу є визначення:

- стан біотичної складової біосфери, її відгуку, реакції на антропогенний вплив;

- функції стану та відхилення цієї функції від нормального природного стану на різних рівнях: молекулярному, клітинному, популяційному, а також рівні спільноти.

При організації та здійсненні біологічного моніторингу передбачається спостереження, оцінка та прогноз стану здоров'я людини, а також стану найважливіших популяцій як з точки зору існування тієї чи іншої екосистеми, так і з точки зору високої господарської цінності (наприклад, цінні сорти риб). Крім того, ведеться спостереження та оцінюється стан найбільш чутливих до того чи іншого виду антропогенного впливу популяцій рослин і тварин, а також популяцій-індикаторів [72; 142; 172].

Екологічний моніторинг, по суті, включає в себе в повному обсязі два розглянутих вище види моніторингу в їх взаємозв'язку. В екологічний моніторинг, відповідно до його функціональних завдань, про які вже згадувалося, входить також моніторинг джерел і чинників антропогенних впливів:

- джерел і чинників впливу на навколишнє середовище забруднень шкідливими хімічними, радіоактивними речовинами і біологічними компонентами;

- джерел і чинників впливу: шумів, джерел електромагнітних випромінювань та інших фізичних полів, що чинять шкідливий вплив на навколишнє середовище.

Моніторинг критично важливих об’єктів інфраструктури здійснюється постійно або з встановленою періодичністю контролю (спостереження, вимірювання, фіксації) та аналізу узагальнених параметрів стану охорони об'єктів критичної інфраструктури та впливати на них, щоб підготувати необхідні рішення для запобігання та усунення негативних наслідків кризових ситуацій природного та техногенного характеру [130, с. 102−120].

Цілями створення системи моніторингу є послідовне зниження до мінімального рівня ризику впливу на об'єкти критичної інфраструктури факторів терористичного, техногенного та природного характеру та мінімізація шкоди від кризових ситуацій для населення країни та навколишнього середовища [22; 86; 145].

Завданням системи моніторингу є надання інформаційної підтримки для розробки та впровадження заходів щодо своєчасного прогнозуванню, виявлення та запобігання загрозам та кризовим ситуаціям щодо об'єктів критичної інфраструктури.

Об'єктом моніторингу є стан захищеності об'єктів критичної інфраструктури. Система моніторингу повинна забезпечувати виконання наступних функцій: збір, обробка, аналіз, зберігання та передача інформації про:

- розташування узагальнених параметрів стану охорони критично важливих об’єктів інфраструктури;

- маршрути транспортування вантажів та інші необхідні данні;

- інформаційне забезпечення робіт, що виконуються з метою підготовки та реалізації заходів щодо забезпечення безпечного функціонування об'єктів критичної інфраструктури, запобігання та локалізації кризових ситуацій, а також ліквідації їх наслідків;

- підготовка інтегрованих оцінок (моделей) кризових ситуацій щодо критично важливим об'єктів інфраструктури та оцінка їх можливих наслідків;

-прогнозування загроз критичним об’єктам інфраструктури та динаміки змін стану їх захисту під впливом природних, техногенних та інших факторів;

- ведення інформаційних баз даних для забезпечення підтримки прийняття та реалізації управлінських рішень щодо захисту об'єктів критичної інфраструктури;

- забезпечення в установленому порядку інформаційних ресурсів системи моніторингу, забезпечення захисту цих ресурсів від несанкціонованого впливу;

- формування єдиного інформаційного простору системи моніторингу на основі уніфікації та сумісності інформаційних, програмних та апаратних забезпечень;

- інформаційне забезпечення реалізації міжнародних договорів та угод у сфері моніторингу об'єктів критичної інфраструктури.

Система моніторингу забезпечує національний, міжрегіональний, регіональний, міський та місцевий рівні. При цьому кожен рівень повинен бути включений до складу системи моніторингу:

- центри системного моніторингу та оперативного управління (далі − центри моніторингу);

- системи, комплекси та засоби отримання інформації про узагальнені параметри стану охорони критично важливих об’єктів інфраструктури;

- системи та засоби телекомунікацій, збору, передачі даних та оповіщення.

Основними структурними елементами системи моніторингу, які забезпечують вирішення покладеної на неї задачі, повинні бути центри моніторингу органів державної влади та місцевого самоврядування України..

При вирішенні завдання, покладеного на систему моніторингу, слід передбачити можливість інформаційної взаємодії центрів моніторингу різного рівня з іншими державними та недержавними інформаційними системами загального та спеціального призначення України, а також з міжнародними інформаційними системами [69; 70].

При створенні та використанні системи моніторингу слід дотримуватися наступних основних принципів:

- забезпечення відповідності завданню, яке вирішує система моніторингу, а також його структурі та характеристикам рівня загрози щодо об'єктів критичній інфраструктурі;

- структура та завдання органів державної влади та місцевого самоврядування України, в сферу діяльності яких входять питання забезпечення захищеності об'єктів критичної інфраструктури та охорони довкілля;

- організаційна, інформаційна та функціональна єдність системи моніторингу, основу якої складають:

1) єдина система класифікації та кодифікації загроз об'єктам критичної інфраструктури;

2) показники та критерії оцінки стану захищеності об'єктів критичної інфраструктури;

3) базові (типові) протоколи, алгоритми (програми) збору, обробки та обміну інформацією, підготовки та автоматизованої підтримки прийняття та реалізації управлінських рішень на основі даних моніторингу стану критично важливих інфраструктурних об'єктів;

4) єдина геоінформаційна система;

- ієрархічність побудови системи моніторингу, можливість централізованого та санкціонованого децентралізованого використання ресурсів системи моніторингу критичних об’єктів інфраструктури;

- раціональна функціональна сумісність центрів моніторингу критичної інфраструктури об'єктів різного рівня;

- уніфікація програмних, інформаційних та технічних засобів, забезпечення сумісності елементів системи моніторингу об'єктів критичної інфраструктури, можливості її модульного розширення та модернізації;

- можливість структурного та функціонального розвитку, оптимізації складу користувачів системи моніторингу критичної інфраструктури об'єктів та спектра відповідних наданих послуг;

- багатофункціональність, яка забезпечує одночасне вирішення завдань в інтересах національної безпеки та соціально-економічного розвитку країни;

- наступність, заснована на інтеграції та вдосконаленні інших систем моніторингу критичної інфраструктури об'єктів;

- гарантований захист інформації від несанкціонованого доступу, включаючи обмежений доступ до інформації про критичні об’єкти інфраструктури, що циркулюють у системі моніторингу;

- запобігання залежності системи моніторингу від зарубіжних технологій.

Основними завданнями механізмів державного регулювання захистом об'єктів критичної інфраструктури як складових механізмів державного управління у сфері цивільного захисту є наступне:

-здійснення в межах своєї компетенції державної політики у сфері цивільного захисту, захисту населення та територій від надзвичайних ситуацій, забезпечення пожежної безпеки та безпеки людей на водних об'єктах;

- здійснення функцій контролю у сфері цивільного захисту, захисту населення та територій від надзвичайних ситуацій, забезпечення пожежної безпеки та безпеки людей на водних об'єктах;

- здійснення в межах своєї компетенції заходів з організації та проведення цивільного захисту, захисту населення та територій від надзвичайних ситуацій та пожеж, забезпечення безпеки людей на водних об'єктах, а також екстреного реагування на надзвичайні ситуації на національному рівні [93; 145; 148].

При цьому кожен із суб'єктів зазначених механізмів:

- організовує прогнозування надзвичайних ситуацій в рамках системи моніторингу та прогнозування надзвичайних ситуацій, роботу з попередження та ліквідації надзвичайних ситуацій національного рівня, порятунку та життєзабезпечення людей у надзвичайних ситуаціях, забезпечує підтримку ліквідації надзвичайних ситуацій регіонального та міжмуніципального характеру, а також своєчасне прийняття управлінських рішень при переході цих надзвичайних ситуацій на національний рівень;

- організовує в установленому порядку роботу з запобігання пожежам, а також контроль за організацією гасіння пожеж на об'єктах, критично важливих для національної безпеки країни, інших особливо важливих пожежонебезпечних об'єктах, особливо цінних об'єктах культурної спадщини України, при проведенні заходів загальнодержавного рівня з масовим скупченням людей, перелік яких затверджується Урядом України [8; 86; 164];

- організовує в установленому порядку пошук та рятування людей на водних об'єктах;

- організовує в установленому порядку разом із зацікавленими органами виконавчої влади регіонів України формування та доставку вантажів гуманітарної допомоги населенню, що постраждало внаслідок надзвичайних ситуацій, у тому числі населенню зарубіжних країн;

- організовує облік атестованих аварійно-рятувальних служб, пожежників, пожежно-рятувальних, пошуково-рятувальних та аварійно - рятувальних формувань, а також громадських об'єднань, які мають статутні завдання з проведення аварійно-рятувальних робіт та гасіння пожеж;

- організовує фінансове забезпечення головних управлінь ДСНС України та підпорядкованих підрозділів, підготовку та затвердження кошторисів доходів і видатків по бюджетних та позабюджетних коштах, а також оперативного, бухгалтерського та статистичного обліку фінансово-господарської та іншої діяльності, ревізійну роботу;

- організовує взаємодію сил і засобів, що беруть участь у аварійно-рятувальних операціях у надзвичайних ситуаціях та гасінні пожеж;

- організовує проведення атестації аварійно-рятувальних служб, пожежно-рятувальних, аварійно-рятувальних формувань та рятувальників органів державної виконавчої влади, органів виконавчої влади регіонів України, органів місцевого самоврядування та організацій;

- здійснює контроль за створенням та забезпеченням готовності сил та засобів цивільного захисту в регіонах України, муніципальних утвореннях та організаціях;

- здійснює поточне та перспективне планування мобілізаційного розгортання сил та засобів цивільного захисту;

- здійснює контроль за створенням, збереженням та використанням страхового фонду документації на об'єкти підвищеного ризику та об'єкти систем життєзабезпечення населення;

- здійснює в межах своєї компетенції в установленому порядку заходи щодо запобігання, виявлення та припинення терористичної діяльності на об'єктах, підвідомчих ДСНС України, а також ліквідації наслідків терористичних актів;

- бере участь у межах своєї компетенції в інформуванні населення через засоби масової інформації та інші канали про прогнозовані та виникаючі надзвичайні ситуації та пожежі, заходи щодо забезпечення безпеки населення та територій, та методи захисту, а також здійснює пропаганду у сфері цивільного захисту, захисту населення та територій від надзвичайних ситуацій, забезпечення пожежної безпеки та безпеки людей на водних об'єктах;

- бере участь в управлінні єдиної державної системи цивільного захисту в межах своєї компетенції;

- бере участь у підготовці пропозицій щодо надання державної допомоги населенню та територіям, які постраждали від надзвичайних ситуацій регіонального, національного та транскордонного характеру; бере участь у координації діяльності всіх видів протипожежного захисту [91; 157; 248].

Таким чином, для реалізації завдань, покладених на суб'єктів забезпечення охорони об'єктів критичної інфраструктури, вони наділені такими основними повноваженнями:

- готувати проекти нормативно-правових актів та інших документів з питань цивільного захисту, захисту населення та територій від надзвичайних ситуацій, забезпечення пожежної безпеки, безпеки людей на водних об'єктах;

- здійснювати в установленому порядку контроль за організацією наглядової діяльності головними управліннями ДСНС України за дотриманням встановлених вимог у сфері цивільного захисту, захист населення та територій від надзвичайних ситуацій, забезпечення пожежної безпеки та безпеки людей на водних об'єктах органами місцевого самоврядування, організаціями, а також посадовими особами, громадянами України, іноземними громадянами та особами без громадянства;

- реалізують в установленому порядку функції з управління закріпленим державним майном;

- здійснює повноваження розпорядника коштів державного бюджету щодо головних управлінь ДСНС України та підпорядкованих підрозділів відповідно до законодавчих та інших нормативних правових актів України;

- створює координаційні і дорадчі органи (комісії, групи) на представницькій основі, а також інші колегіальні органи для обговорення актуальних питань діяльності ДСНС України та ін. [104; 216].

1.3. Державна система забезпечення безпеки і захисту критичної інфраструктури

Враховуючи загрози, спричинені стихійними лихами, технічними аваріями чи людськими прорахунками, тероризмом чи злочинними діями, заходи щодо основного захисту дуже складних економічних та соціальних елементів інфраструктури видаються абсолютно необхідними. Зокрема, у випадку елементів інфраструктури, які мають особливе значення для держави та суспільства, невдача чи недієздатність яких призведе до тривалих перебоїв у

постачанні, серйозних порушень громадської безпеки чи інших драматичних наслідків [156; 157].

Що стосується цих елементів так званої критичної інфраструктури, необхідно передбачити та розробити заходи щодо мінімізації та усуненню шкоди, але, перш за все, профілактичні заходи, які можуть запобігти серйозним аваріям спочатку або хоча б мінімізувати їх наслідки.

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). У той же 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 [91; 241].

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 [114; 241].

Зокрема, ризик − це ймовірнісна міра небезпеки або сукупності небезпек, встановлена для певного об'єкта критичної інфраструктури у вигляді можливих

втрат за заданий час або усвідомлена небезпека (загроза) настання в будь-якій системі негативної події з певними в часі і просторі наслідками.

Число різновидів ризику досить велике, але в зв'язку з надзвичайними ситуаціями розглядаються так звані "чисті ризики", які передбачають тільки небажаний (негативний) ефект. До них можна віднести ризики можливих втрат: популяційний, диференційований, індивідуальний, інтегральний (сумарний, сукупний), природний, фізичний, екологічний, економічний, соціальний (колективний, груповий) і ін.

Крім того, для умов надзвичайних ситуацій необхідне отримання оцінок індивідуального і соціального ризиків. У деяких окремих випадках, наприклад для небезпечних технологічних процесів, виконують оцінку регламентованих параметрів небезпек.

Індивідуальний ризик (розподіл ризику) − це ймовірність (частота) виникнення небезпечних факторів при надзвичайних ситуаціях в певному місці простору [35; 148].

Соціальний ризик (характерний для масштабу небезпеки) - залежність від ймовірності травмування певної кількості людей від загальної кількості людей, постраждалих від факторів впливу в надзвичайній ситуації. Ураження небезпекою об'єкта критичної інфраструктури, що оцінюється різними показниками і характеризується тісним зв'язком різних небезпек з об'єктами − реципієнтами небезпек − відображає категорійні поняття ризику.

Відповідно, прогнозування наслідків надзвичайних ситуацій для об'єктів критичної інфраструктури здійснюється в кілька етапів.

На I етапі встановлюють параметри впливів − значущих вражаючих факторів, що викликають основні руйнування й ураження, з характеристиками, що зазвичай приймаються з використанням існуючих методик.

На II 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 III 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 [23; 79; 169].

Параметри вражаючих факторів 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 є довіра співпраці між державою та інфраструктурними організаціями: в той час, коли держава залишається гарантом внутрішньої безпеки, а також виступає посередником в рамках інформаційно-комунікаційних процесів, інфраструктурні організації мають достатньо детальну інформацію про відповідних елементів інфраструктури, відповідно, лише вони здатні вжити ефективних конкретних заходів захисту.

Розробники основних заходів захисту повинні зосередитись, з одного боку, на відповідних положеннях закону, з іншого - на загальновизнаних принципах бізнесу далекоглядного управління ризиками та стратегічного

планування господарської діяльності підприємства, спрямована на досягнення успіху та послідовності, наприклад, у рамках так званого управління для забезпечення безперервності бізнесу.

Так щодо органів правління ряду інфраструктурних організацій присутні зобов'язання щодо прийняття належних заходів і створення системи контролю, наприклад, системи ризик-менеджменту, що дозволяють на ранній стадії помітити тенденції і факти, що представляють собою загрозу для подальшого існування суспільства [99; 133; 195].

До таких тенденцій та фактів, поряд із ризикованими операціями та порушеннями положень нормативно-правових актів, відносяться також загрози стихійних лих чи терактів, які можуть суттєво вплинути на подальше існування підприємства.

Відповідно, керівники за оцінкою достатності капіталу і прийнятими стандартами кредитування останнім часом стали приділяти посилену увагу питанням аналізу і оцінці підприємницьких ризиків.

Інший орієнтир щодо визначення критичних заходів щодо захисту інфраструктури випливає з відповідальності інфраструктурних організацій захищати свої об'єкти від потенційних загроз та прийняття необхідних заходів. Ці обов'язки інфраструктурних організацій частково закріплені законодавчо (загальні обов'язки інфраструктурних організацій або ж, відповідно, специфічні обов'язки). Однак частково вони є складовою загальноприйнятих підприємницьких принципів виходячи з того, що вони викладені, наприклад, в принципах належного врядування та керівництва підприємством [23; 82].

З точки зору безпеки, важливий внесок у захист критично важливих елементів інфраструктури, зокрема, заходів щодо припинення несанкціонованих дій з боку сторонніх осіб. Необхідно забезпечити рівень захисту об’єктів від порушень, спричинених навмисно, а також внаслідок стихійних явищ чи аварій,

які, по можливості, виключали б виникнення серйозної небезпеки, наприклад, внаслідок вибуху чи шляхом поширення небезпечних речовин.

Слід також уникати перебоїв у постачанні продукції та наданні послуг, якщо існує серйозний ризик для змісту вищезазначеного визначення критичної інфраструктури.

Відповідно, головним завданням розробки концепції основних заходів захисту 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. Таким чином, концепція основних заходів захисту повинна враховувати стандартизовані будівельні, організаційні, кадрові та технічні заходи безпеки. [93; 95; 156].

Хоча небезпека для навколишнього середовища також може становити серйозну загрозу, в цій концепції лише екологічні наслідки не слід розглядати окремо. Однак і в цій сфері можливе застосування аналогічного підходу. Також залишаються без уваги злочинні посягання на підприємства, що завдають шкоди, перш за все, їх конкурентоспроможності, такі як, наприклад, промислове шпигунство.

Вчені та практикуючі в різних сферах діяльності погоджуються з тим, що 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 [52; 72].

Крім того, 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. Зміст поняття "регіональна безпека" та його внутрішня структура дозволяють

сформувати уявлення про раціональну структуру системи громадської безпеки та захисту критично важливих об'єктів України в надзвичайних ситуаціях та терористичних актах.

Слід мати на увазі, що раціональність досягається за рахунок використання особливостей функціонування її компонентів - ланок державного механізму.

Методологічні аспекти функціонування окремих компонентів регіональної системи безпеки є найважливішою частиною методології національної безпеки.

Аналіз наукової думки та практики щодо формування та функціонування системи національної безпеки дозволяє зробити висновок, що в цій галузі слід використовувати положення та висновки як теорії прийняття рішень, так і теорії організації державних органів [88; 219].

Теорія прийняття рішень в державній політиці характеризується дослідженням як мінімум шести змінних:

- дійові особи процесу державного управління (організації та громадяни), їх цінності та сприйняття;

- ситуації (звичайні, кризові й їх комбінації);

- організаційна система (фіксований набір функцій та відносин основних установ, що беруть участь у прийнятті рішень);

- процес прийняття рішення (хронологічний потік подій та дій, що ведуть до вирішення проблеми);

- громадські особи, які приймають рішення (вивчаючи специфіку взаємовідносин між особами, які приймають рішення;

- власне рішення (вибір одного з декількох варіантів). У той же час політика національної безпеки є результатом ланцюга дій в рамках організаційної структури, тобто результатом певного процесу..

Процес прийняття та реалізації рішень складається з серії дій в рамках організаційних структур, які в сукупності формують курс державного управління.

Етапами цього процесу можуть бути:

- ідентифікація проблеми;

- планування її вирішення;

- прийняття рішення;

- реалізація політики;

- оцінка результату.

Як структуру, так і процес прийняття та реалізації рішень у сфері забезпечення національної безпеки визначає Конституція України та державні закони [88; 91].

При цьому теорія організації державних органів надає важливого значення такій характеристиці, як сутність організації або організаційна сутність. Відповідно до думки А. Г. Атаманчука, сутність організації − це точка зору самої організації, що виражається домінуючою в ній групою, на те, якими мають бути завдання і можливості організації.

Сутність організації визначальним чином впливає на формування інтересів цієї організації. Важливими при цьому вважаються наступні аспекти:

- організація вважає за краще таку політику або стратегію, які, на думку домінуючої в ній групи, зроблять організацію ще більш важливою;

- організації прагнуть отримати в своє розпорядження матеріальні й інші засоби, які розглядаються як необхідні для їх існування. Звідси тенденція до отримання максимального автономії організації;

- організації чинять опір при спробах позбавити їх функцій, які розглядаються як частина їх сутності;

- організація намагається вивести за свої рамки функцію, яка знову з'явилася, так як новий персонал з новими знаннями, вміннями і інтересами може спробувати змінити сутність організації.

Таким чином, конфлікти навколо завдань і функцій є постійним явищем на вищому рівні управління.

Формування системи безпеки при надзвичайних ситуаціях, з точки зору як теоретичної, так і практичної, - це багатогранний, об'ємний процес, який включає цілий комплекс взаємозалежних заходів. Відповідно, у цьому процесі необхідно виділити організаційні та функціональні компонент.

Зокрема, організаційна складова процесу формування згаданої системи включає в себе встановлення і вдосконалення організаційної структури. Це статичний (структурний) "зріз" системи, покликаний забезпечити взаємодії елементів системи, а також стійкість, визначеність і послідовність.

Створення системи постійних спеціально уповноважених органів управління у сфері захисту населення та територій від надзвичайних ситуацій на всіх рівнях організації державної влади та місцевого самоврядування, їхніх завдань та функцій слід виділити як пріоритетну сферу [174; 204].

Функціональна складова процесу формування системи забезпечення безпеки при надзвичайних ситуаціях, або її динамічний (функціональний) "зріз" пов'язана з реальною практичною взаємодією, в результаті якої виникає сукупний результат всієї управлінської діяльності у сфері захисту від надзвичайних ситуацій. Зазначена складова формування системи вимагає постійної уваги, коригування, стимулювання та контролю, оскільки у функціонуванні системи не виникає автоматизму, раз і назавжди заданої визначеності. Це пов'язано, перш за все, об'єктом управління, який розвивається і постійно видозмінюється. Тому без сильного зовнішнього організуючого впливу система буде постійно дисфункціонувати.

У зв'язку з цим найважливішою складовою методології побудови системи забезпечення безпеки населення і захисту критично важливих об'єктів України в надзвичайних ситуаціях та терористичних актах є обґрунтування концепції управління цією системою. [35; 129; 197].

Ґрунтуючись на положеннях загальної теорії управління складними системами, управління безпекою при надзвичайних ситуаціях слід розглядати в рамках певної соціально-економічної системи, що об'єднує:

- стабільні внутрішні зв'язки населення;

- об'єкти економіки, інфраструктури, території;

- управлінські структури.

У процесі державного управління об'єктами критичної інфраструктури слід виділяти два рівні, дві ієрархічно пов'язані складові, кожна з яких характеризується певним змістом.

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 [23; 145].

Другий рівень процесу державного управління критично важливими інфраструктурними об'єктами стосується організаційно-технічних систем. Основними елементами системи управління на цьому рівні є:

- 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.

Фактори формування системи тісно пов'язані з процесом вироблення основних напрямів регіональної політики у сфері забезпечення безпеки

населення та захисту критично важливих об'єктів України в надзвичайних ситуаціях та терористичних актах. Орієнтовна структура цього процесу представлена на рис. Дана схема свідчить, що вироблення регіональної політики − це широкомасштабний і багаторівневий процес. Тут необхідний облік величезного числа факторів і явищ [29; 94].

Природно, що чим вище становище організації в державній ієрархії, тим більший спектр чинників вона повинна враховувати.

На рівні вищого керівництва регіону на основі аналізу загроз життєво важливим інтересам в економічній, соціальній, екологічній та природно-техногенній сферах, а також оцінки наявних для усунення цих загроз людських, фінансових, інформаційних, сировинних, енергетичних та інших ресурсів виробляються основні напрями забезпечення національної безпеки в цій галузі.

Таким чином, формування системи забезпечення безпеки населення та захисту критично важливих об'єктів України при надзвичайних ситуаціях та терористичних актах підпорядковане дії великого і тісно пов'язаного між собою кола закономірностей. Їх доцільно об'єднати в дві великі групи, що відображають соціально-економічний і організаційний характер будівництва системи [12; 72].

Зокрема, група закономірностей 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. Найважливішими з них є такі:

- 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;

- єдність інтересів усіх груп населення щодо захисту від надзвичайних ситуацій [94; 213].

Інша група закономірностей має організаційний характер і виражає внутрішні компоненти, які притаманні лише цій системі, і є особливостями її формування порівняно з іншими державними системами (наприклад, системою соціального забезпечення, системою охорони здоров'я) та характеризує взаємозв'язок між складовими елементами системи, внутрішньою логікою формування кожного з них. При цьому основними закономірностями формування системи організаційного характеру є такі:

- 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;

- відповідність організації, складу сил та засобів, фінансових та матеріальних ресурсів ступеня небезпеки та наслідкам аварій, катастроф та стихійних лих, а також небезпеки терористичних актів.

Закономірності формування системи реалізуються на практиці через відповідні принципи. При цьому доцільно розглядати суспільно-економічні та організаційні засади у цьому контексті. Всі вони знаходяться в діалектичній єдності, доповнюються і уточнюються в міру розвитку української державності, науково-технічного прогресу, зміни в характері і ступені загроз безпеці України.

Творче застосування цих принципів на практиці забезпечується науковим підходом до використання в конкретних умовах закономірностей формування системи.

Перша група − суспільно-економічні принципи. Ця група враховує реалії, що склалися поточного моменту, такі як:

- державна перебудова України;

- хід економічних реформ;

- загальний характер заходів щодо захисту населення та територій від надзвичайних ситуацій.

Одним із провідних соціально-економічних принципів є єдність заходів щодо забезпечення безпеки населення та захисту критично важливих об'єктів України у надзвичайних ситуаціях та терористичних актах та заходів щодо забезпечення регіональної безпеки. Значущими принципами у цьому контексті є принципи:

- забезпечення єдності державного будівництва та формування системи;

- загального характеру заходів щодо захисту населення та територій від надзвичайних ситуацій.

Друга група − організаційні принципи формування системи забезпечення безпеки населення та захисту критично важливих об'єктів України в надзвичайних ситуаціях та терористичних актах − відображають закономірність її функціонування та розвитку як особливого виду державної діяльності, а також вимоги до її організації [94; 143; 179].

Найважливішими принципами цієї групи є такі:

- виправданості практичної діяльності;

- оптимізації захисту;

- інтегральної оцінки небезпеки;

- стійкості екосистем;

- раціональності (економічної доцільності);

- правової забезпеченості;

- поділу відповідальності.

Крім того, система на рівні регіонів України та органів місцевого самоврядування повинна будуватися на єдиних принципах, згідно з якими всі регіони України та органи місцевого самоврядування повинні мати рівні повноваження.

Таким чином, сформульовані основні концептуальні принципи, які дозволяють розробити конкретні заходи з метою формування реалістичного та доступного для практичного використання регіональної політики у цій галузі забезпечення безпеки населення та територій у надзвичайних ситуаціях природного та техногенного характеру, а також при терористичних актах [29; 145].

Забезпечення регіональної безпеки, насамперед безпеки населення та захист критично важливих об'єктів України − це цілеспрямована діяльність державних і громадських установ, а також громадян щодо виявлення, запобігати загрозам безпеці та протидіяти їм в якості обов'язкової та неодмінної умови захисту інтересів регіонів України. Основними напрямами забезпечення регіональної безпеки за конкретних сферами життєдіяльності при цьому є такі.

В економічній сфері:

- забезпечення стійкого зростання економічного потенціалу України та рівня соціального захисту населення;

- обмеження концентрації виробництва в певних промислових зонах;

- перехід трудомістких, енерго- та ресурсоємних галузей до передових і високотехнологічним галузей діяльності з урахуванням світового досвіду;

- організація підтримки товаровиробників;

- проведення приватизації і акціонування з урахуванням інтересів регіону та населення;

- забезпечення конкурентоспроможності підприємств, сприяння процесам їх реформування;

- сприяння фінансовому забезпеченню програм розвитку промислових підприємств;

- зміцнення виробничих та економічних зв'язків з регіонами України та країнами ближнього зарубіжжя;

- подальший розвиток транспортних магістралей.

У соціальній сфері:

- стабілізація та підвищення рівня життя населення, забезпечення її соціального захисту;

- охорона здоров'я населення;

- розвиток системи професійної підготовки та перепідготовки, організація громадських робіт з метою максимальної зайнятості трудових ресурсів;

- реалізація заходів щодо покращення санітарно-епідеміологічної обстановки в регіоні;

- оптимізація співвідношення державної, муніципальної та приватної власності при створенні поточних запасів та організації торгівлі продовольством та предметами першої необхідності;

- виконання комплексної програми заходів соціального захисту для жителей регіону.

В екологічній сфері:

- вдосконалення адміністративно-економічних методів управління навколишнім середовищем, екологічного законодавства та екологічних стандартів;

- зниження техногенного впливу на навколишнє природне середовище та здоров'я населення;

- широка участь громадськості у прийнятті та реалізації рішень, що впливають на стан довкілля;

- розробка системи моніторингу стану навколишнього середовища та контролю над джерелами забруднення;

- вдосконалення еколого-освітньої діяльності та системи безперервної екологічної освіти для формування дбайливого ставлення до природи у громадян [145].

В оборонній сфері:

- підтримка цивільної оборони на рівні, що забезпечує ефективний захист населення, матеріальних та культурних цінностей від загроз воєнного характеру;

- забезпечення мобілізаційної підготовки.

Основною формою ухилення від процедур громадського обговорення стало приховування суспільно значущих відомостей про критично важливі об'єкти. При цьому відсутні відомості про:

- об'єкт, його технічні характеристики, терміни будівництва;

- відповідальних (контактних) осіб;

- процедури або порядок ознайомлення з проектом

а також, не ведеться реєстрація й облік висловлених думок.

Дану діяльність пропонується розвивати шляхом застосування системного підходу, який містить такі складові:

- економічна;

- адміністративно-кримінальна (штрафи, судові розгляди);

- соціально-психологічна.

Для успішного вирішення проблеми вважається доцільним:

- сприяти впровадженню стану показників у систему оцінювання ефективності діяльності регіональних органів виконавчої влади;

- поступово запровадити систему технічних регламентів та привести її у відповідність із міжнародними стандартами;

- надавати офіційну інформацію про те, що надзвичайні ситуації не знають політичних кордонів, вимагають довгострокової перспективної роботи і потребують участі громадянського суспільства, активної позиції людей.

В даний час функції щодо забезпечення безпеки і контролю розосереджені серед низки міністерств і відомств. Єдиним органом щодо забезпечення безпеки і контролю, в тому числі і критично важливих об'єктів має стати Державна служба України з надзвичайних ситуацій. В даний час на ДСНС України покладено ведення реєстру критично важливих об'єктів. Основними структурними елементами системи моніторингу, які забезпечують вирішення покладеної на неї задачі, повинні бути центри моніторингу державних органів виконавчої влади та місцевого самоврядування [138; 172].

Організації, що експлуатують потенційно небезпечні об'єкти, підлягають обов'язковій оцінці готовності до запобігання та ліквідації надзвичайних ситуацій (надалі − оцінка готовності об'єктів).

Оцінка готовності об'єктів повинна проводитися з урахуванням класу небезпеки об'єкта. У цьому випадку оцінку готовності об’єкта слід проводити не рідше одного разу на п’ять років у формі самостійного заходу або із включенням у плани регулярних та позачергових перевірок організацій з питань запобігання надзвичайним ситуаціям. Для проведення оцінки допускається залучення спеціалізованих науково-дослідних, проектних та інших організацій, які мають відповідні ліцензії.

В Україні здійснюється паспортизація територій та небезпечних об'єктів. Паспортизація, звичайно, стала основою для обліку та контролю над територією та особливо небезпечними об’єктами для запобігання та ліквідації надзвичайних ситуацій. Однак типовий паспорт безпеки небезпечного об'єкта і території повинен враховувати таку категорію як критично важливі об'єкти.

Технічні регламенти встановлюють обов'язкові вимоги до об'єктів технічного регулювання (продукція, включаючи будівлі та споруди, виробничі

процеси, експлуатація, зберігання, транспортування, продаж та утилізація). Необхідно розробити єдину національну нормативну базу з проблем для оцінки ризику критично важливих об'єктів. Цій меті слугуватиме категоріювання критично важливих об'єктів. Відповідно, перелік об’єктів, на які поширюється вимога заповнити цей паспорт, буде розширено [9; 68].

У той же час необхідно відзначити таку обставину - критично важливі об'єкти потребують насамперед запобігання надзвичайним ситуаціям. І заходи фізичного захисту від зовнішніх і внутрішніх впливів виходять на перший план. Розглядаючи проблему забезпечення безпеки критично важливих об'єктів, слід пам’ятати про два напрямки:

- захист об’єктів від зовнішніх впливів з метою запобігання їх знищення та аварійних ситуацій;;

- захист людей та навколишнього середовища від негативних факторів, які утворюються у випадку, якщо аварія все-таки сталася.

Загалом основні принципи функціонування державної системи забезпечення безпеки та захисту критичної інфраструктури такі:

- 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. [138; 145].

Висновки до першого розділу

1. Встановлено, що об’єктами критичної інфраструктури є об'єкти, порушення чи припинення функціонування яких призводить до втрати управління економікою України, її регіонів чи муніципалітетів, а також до значного зниження безпеки життєдіяльності населення, яке проживає в цих районах тривалий час.

2. Обґрунтовано, що в процесі державного управління громадськістю критичну інфраструктуру слід розділити на два рівні, кожен з яких характеризується певним змістом.

Зокрема, перший рівень включає управлінську діяльність аналітичного, науково-прогностичного й організаційного характеру. Її результатом, насамперед, є визначення стратегій управління зовнішніми впливами, а також організація механізму їх реалізації з урахуванням соціальних, економічних та інших факторів.

Другий рівень процесу громадського управління критично важливими інфраструктурними об'єктами стосується організаційно-технічних систем. Базовими елементами системи управління на цьому рівні є такі:

- функціональний контур та інформаційні технології;

- методи та засоби підготовки та прийняття управлінських рішень;

- методичний апарат аналізу та оцінки ризиків з урахуванням соціальних, економічних та інших аспектів.

3. Визначено, що головним завданням забезпечення безпеки об'єктів критичної інфраструктури є швидке отримання інформації про загрозу та її використання для здійснення адекватних заходів безпеки. У той же час велике значення мають питання обладнання та технології побудови автоматизованих систем забезпечення безпеки життєдіяльності міст, ситуаційних та кризових центрів, організації відеоспостереження територій, обладнання найбільш відповідальних елементів інфраструктури за допомогою екстреного виклику оперативних підрозділів тощо.

4. Зазначається, що формування системи забезпечення безпеки населення та захисту критично важливих об'єктів України при надзвичайних ситуаціях та терористичних актах підпорядковане дії великого і тісно пов'язаного між собою кола закономірностей. Доцільно поєднувати їх у дві великі групи, що відображають соціально-економічний та організаційний характер будівництва системи.

Зокрема, група законів соціально-економічного характеру відображає взаємозв'язок формування системи громадської безпеки та захисту критично

важливих об'єктів України в надзвичайних ситуаціях та терористичних актів із зовнішніми та внутрішніми умовами розвитку суспільства та держави.

Інша група закономірностей має організаційний характер і виражає ті внутрішні компоненти, які притаманні лише цій системі, і є особливостями її формування порівняно з іншими державними системами та характеризує взаємозв'язок між складовими елементами системи та внутрішньою логікою формування кожної з них.

5. Показано, що прогнозування наслідків надзвичайних ситуацій для об'єктів критичної інфраструктури здійснюється в кілька етапів.

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. Використовуючи цей методологічний підхід, оцінюються наслідки майже всіх природних катастроф та техногенних аварій для прийняття рішень щодо організації екстреної евакуації населення з районів надзвичайних ситуацій та його життєзабезпечення у безпечних районах, а також залучення сил та засобів Державної служби України до надзвичайних ситуацій різного рівня для ліквідації надзвичайної ситуації.

Матеріали даного розділу оприлюднені в наступних публікаціях автора: [60; 61; 69].

РОЗДІЛ 2. АНАЛІЗ СУЧАСНОГО СТАНУ ТА ТЕНДЕНЦІЙ РОЗВИТКУ ДЕРЖАВНОГО УПРАВЛІННЯ ЗАБЕЗПЕЧЕННЯМ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1. Досвід зарубіжних країн стосовно державного управління забезпеченням безпеки критичної інфраструктури

У контексті обраної теми дисертаційного дослідження необхідно дослідити зарубіжний досвід діяльності органів державної влади щодо захисту критичної інфраструктури, зокрема, в умовах кризи [21; 184].

.У зв'язку з цим заслуговує на увагу досвід створення системи антикризового управління в США, особливо її територіальної складової. Серія терористичних актів, що мали місце в різних країнах, об'єктивно вимагали від керівництва США перегляду підходів до організації антикризового управління. У зв'язку з цим заява Адміністрації США від 1 березня 2003 року про створення Єдиної національної системи управління в умовах надзвичайних ситуацій та відповідний комплекс організаційних заходів були дуже серйозною підготовчою роботою в цьому напрямку.

В останньому десятиріччі XX століття увага Президента та адміністрації США була націлена на вдосконалення концепції запобігання актам тероризму з використанням хімічних і біологічних агентів. Так, зокрема, у проведеному в 1997 році ЦРУ і Міністерством енергетики США дослідженні стверджувалося, що час для скоординованих дій в загальнонаціональному масштабі щодо протидії цьому виду екстремістських акцій давно настав. Керівник комісії по підготовці цього документа колишній директор ЦРУ Дж. Вулсі, зокрема, заявив, що країні потрібна детально розроблена система протидії тероризму, що використовує в своїх цілях компоненти зброї масового ураження.

Здійснена у квітні 1995 року в метро міста Нью-Йорк в навчальних цілях імітація газової атаки за типом відомого інциденту в Японії («газова атака» в Токійському метро) продемонструвала практичну безпорадність і неготовність державних служб до екстреного реагування на існуючу загрозу.

Серед недоліків, виявлених під час навчань для відбиття терористичних атак із застосуванням хімічних та біологічних агентів, були відмічені наступні:

- відсутність чіткої координації між організаціями, які беруть участь у боротьбі з технологічним тероризмом, роз'єднаність зусиль, боротьба між різними агенціями за фінансування та верховенство в національній системі заходів. Для подолання цього, на думку американських експертів, потрібен був єдиний державний центр з широкими повноваженнями:

- 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;

- правила карантину виявилися застарілими для застосування в умовах масштабної кризової ситуації у великих містах;

- відсутність практичного досвіду поводження з ізольованими людьми, які зазнали впливу вражаючих факторів;

- неефективність існуючих профілактичних заходів щодо запобігання виникнення та нейтралізації паніки серед населення [126, с. 192−195].

В інтересах усунення зазначених недоліків Президентом США в травні 1998 року були підписані дві керівні Директиви PDD 62 «Боротьба з тероризмом» і PDD 63 «Захист критичних інфраструктур». Зокрема, як зазначається у першій директиві:

- у разі застосування терористами хімічних і біологічних агентів спеціальні підрозділи США повинні мати можливість швидко і точно визначити патоген або токсикант, що використовується;

- персонал служб протидії актів технологічного тероризму повинен мати відповідні знання і оснащення для кваліфікованих, безпечних та ефективних дій;

- слід мати необхідний асортимент та кількість вакцин, детоксикантів та інших медикаментів для лікування уражених і запобігання епідемічних ситуацій від біологічної та хімічної атаки, для чого намічалося створити безпрецедентний запас витратних матеріалів, заснований на списку найбільш вірогідних патогенів і хімічних отруйних речовин;

- враховуючи, що біотехнологія надає найширші можливості для зниження наслідків терористичних актів, здійснити дослідження і розробку медикаментів, вакцин, діагностикумів нового покоління [15; 21; 129].

Ці дані показали, що захист населення та критичної інфраструктури від терористичних актів, здійснених силами та засобами спецслужб та правоохоронних органів, не відіграли головної ролі в загальному комплексі заходів, спрямованих на підвищення їх безпеки. У США це було актуально:

- попередження незаконного втручання в роботу критичної інфраструктури;

- пом'якшення можливих негативних наслідків;

- загальне підвищення їх життєздатності та стійкості функціонування критичної інфраструктури в різних надзвичайних та кризових ситуаціях.

Події 11 жовтня 2001 р., які показали низьку готовність служб порятунку та органів управління до таких надзвичайних ситуацій, змусили Адміністрацію США переглянути свої підходи до організації системи управління кризовими ситуаціями, а також змістити акценти в бік на створення системи сил і засобів

на всіх рівнях державного управління, необхідних для запобігання кризових ситуацій різного характеру.

Вже 21 вересня 2001 року, виступаючи перед конгресом, президент Буш оголосив про необхідність створення нового федерального відомства − Міністерства внутрішньої безпеки, − яке координувало б роботу багатьох органів, що займаються питаннями безпеки. Створення Міністерства знаменує собою саму велику реорганізацію федерального уряду з 1940-х років. Більше 20 федеральних відомств у перспективі будуть повністю або частково об'єднані в єдиному міністерстві з безпрецедентно великою штатною чисельністю близько 170 тис. службовців.

З точки зору організації робіт було запропоновано визначати:

- за видами контртерористичної діяльності: охорона кордонів − 26%, «зовнішні ініціативи» міністерства оборони − 18%, захист від біотероризму − 16%, авіаційна безпека −13%;

- за урядовими відомствами: міністерство оборони − 22%, міністерство транспорту − 20%, міністерство юстиції − 19%.

Одночасно пропонувалося зменшити асигнування на охорону навколишнього середовища, вищу освіту, гранти для людей з низькими та середніми доходами, професійну підготовку [131; 200; 232].

Асигнування на внутрішню безпеку США представляються досить великими, складаючи 10% від загального військового бюджету (379,3 млрд. дол.), що на 15% перевищує середні військові витрати у часи холодної війни, тоді як збройні сили з тих пір зменшилися на третину.

Конгресом США вжиті безпрецедентні для США юридичні заходи щодо зміцнення внутрішньої безпеки. Одразу після вчинення терористичних актів та до кінця 2001 року Конгрес прийняв десять законопроектів та резолюцій щодо міжнародних та внутрішніх юридичних аспектів боротьби з тероризмом.

Крім того, на розгляді палат конгресу в даний час перебувало близько двохсот відповідних документів.

У жовтні 2001 року президент Буш затвердив закон, що отримав назву «Патріотичний акт», майже одноголосно підтриманий обома палатами конгресу. Акт містить низку заходів, що розширюють повноваження поліції і федеральних правоохоронних агентств, а також посилюють банківське й імміграційне законодавство. Закон розширює права спецслужб з прослуховування телефонних розмов і перлюстрації електронної пошти. Поліція і ФБР отримали право на обшук будинків, гаражів, офісів або автомобілів, в тому числі з собаками і міношукачами, в будь-який час доби.

Закон розширює визначення тероризму. Згідно з ним залучати до судової відповідальності можна не тільки за вчинення терористичних актів, а й за приховування або фінансування терористів.

Кардинальний перерозподіл завдань та функцій у системі федеральних органів виконавчої влади США у галузі забезпечення внутрішньої безпеки країни, очевидно, зумовив необхідність підготовки національного плану реагування на надзвичайні ситуації, в яких повинні відображати основні заходи всіх органів державного та військового управління на території США та щодо підготовки до дій у кризових ситуаціях.

Все це спрямовано на підвищення готовності федеральних та місцевих органів влади, а також приватного сектору реагувати на широкий спектр різних загроз критичній інфраструктурі. Слід очікувати помітну активізацію роботи над формуванням єдиної національної системи антикризового управління у зв’язку зі зростаючою терористичною загрозою та проблемами, пов’язаними з реконструкцією післявоєнного Іраку [15; 239].

В той же час говорити про ефективність єдиної національної системи управління в умовах кризових ситуацій, яка створюється зараз рано, як попередня діяльність федеральних відомств США свідчила про значну ступінь

децентралізації організації кризового управління, а також превалювання економічних механізмів над організаційною у розглянутій сфер.

Характерною особливістю законодавства США є надання права губернаторам штатів вводити особливий режим при виникненні надзвичайної або іншій кризовій ситуації.

Згідно із законами штату, які різні в кожному зі штатів США, 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).

Звичайно, реагування часто починається до офіційного оголошення і без декларації про надзвичайну ситуацію (надзвичайний стан). Як правило, губернатори користуються цим правом тільки якщо їм потрібні особливі екстрені повноваження або вони хочуть запросити президентську декларацію про надзвичайну ситуацію. Хоча закони в різних штатах варіюють, декларація про надзвичайну ситуацію (надзвичайний стан) зазвичай надає губернатору наступні надзвичайні права [184; 239].

Необхідність використання Національної гвардії, посилення правового захисту та отримання додаткового фінансування - три основні причини, щоб губернатор оголосив надзвичайну ситуацію (надзвичайний стан).

У той же час, екстрені повноваження можуть виявитися сумнівною привілеєм. Хоча вони дають губернатору необхідну владу, її застосування може викликати критику. Наприклад, у губернатора можуть виникнути проблеми політичного характеру, якщо населення пізніше буде сприймати його дії як перевищення влади. Більш того, якщо губернатор прямо санкціонує евакуацію із зони лиха, місцеві чиновники можуть критикувати його дії як узурпацію повноважень.

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 [184, 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.

Заслуговує на увагу досвід організації управління охороною населення та об'єктів економіки на територіальному та місцевому рівнях в умовах надзвичайних ситуацій та в інших країнах.

Так, починаючи з 90-років правова і організаційна діяльність держав Західної Європи (Великобританія, Франція, Швеція) у розглянутій сфері здійснювалась за двома основними напрямами.

Перший - це прийняття нових законів та створення нових керівних органів чи підрозділів у існуючих структурах державного управління (наприклад, Міністерство оборони, Міністерство внутрішніх справ).

Інший шлях полягає в узгодженні, приведення у відповідність до існуючих нормативних актів та посилення координації роботи державних, приватних та громадських організацій у напрямку запобігання та ліквідації надзвичайних ситуацій [102; 145].

Таким чином, цивільна оборона Великобританії структурно входила до Міністерства внутрішніх справ та вирішувала обмежене коло питань, пов'язаних з усуненням наслідків повітряних нападів противника. Тому новий закон про

цивільну оборону Великобританії, прийнятий у 2003 році, натомість того, що діяв з 1948 року, покликаний визначити права і обов'язки громадян, державних структур та недержавних установ у сфері цивільної оборони, а також порядок дії при ліквідації наслідків стихійних лих і терористичних актів.

Прийняття у Великобританії нового закону, який розширює традиційні завдання цивільної оборони, з ухилом до вирішення проблем мирного часу, свідчить про реакцію уряду на зростаючу загрозу тероризму в усьому світі, в тому числі у зв'язку з подіями в Іраку.

Екологічна експертиза та ліцензування підприємств законодавчо закріплені в більшості країн Західної Європи: Ірландії, Франції, Швейцарії та ін.

Так, у Швеції нове законодавство про управління у надзвичайних ситуаціях містить вимоги щодо зменшення наслідків аварій та катастроф за рахунок превентивних заходів та заходів реагування на надзвичайні ситуації відповідними службами підприємств та муніципалітету. Зокрема, у 1986 році було створено Національне управління рятувальних служб, яке координує діяльність 284 органів місцевого самоврядування та служб. У Західній Європі діє регіональна система підготовки та оповіщення про великі аварії на промислових підприємствах, що охоплює країни-члени ЄС [184, с. 275−279].

У той же час у переважній більшості країн між першими двома групами нормативних правових актів та останньою групою законів існує своєрідна межа. Це пояснюється:

- по-перше, складністю, неоднорідністю самого об'єкта управління;

- по-друге, практикою того, що тон всієї діяльності до недавнього часу задавали відомства цивільної оборони, орієнтовані на роботу у воєнний час.

Загалом, аналіз організаційно-правових баз державного управління захистом критичної інфраструктури в кризових ситуаціях у США та країнах Західної Європи дозволив наступні основні риси цієї діяльності:

- системи управління з дій у кризових ситуаціях мають державний статус;

- діяльність з попередження та ліквідації кризових ситуаціях є важливою соціальною функцією кожної держави і реалізується більшістю державних структур;

- право запроваджувати особливий режим діяльності органів управління та населення в зоні стихійного лиха надається не тільки главі держави, а й главам суб'єктів держав (наприклад, губернаторам штатів у США);

- фінансування заходів із захисту критичної інфраструктури в кризових ситуаціях здійснюється головним чином шляхом реалізації державних програм;

- акценти в правовому регулюванні ризику все більше зміщуються у бік превентивних заходів.

Загалом, зарубіжний досвід має важливе значення для формування перспективної системи громадської безпеки та захисту критично важливих об'єктів у надзвичайних ситуаціях. Політичні та економічні умови в Україні, процес реформування системи управління на національному та регіональному рівнях об'єктивно потребують необхідності пошуку оптимального варіанту для формування цієї системи [29; 144].

Межі використання зарубіжного досвіду для розробки системи громадської безпеки та захисту критично важливих об'єктів у надзвичайних ситуаціях та терористичних актах як на національному, так і на регіональному рівнях будуть визначатися ходом адміністративної реформи в Україні, а також типом системи державної влади в найближчі роки.

Окрему увагу слід приділити забезпеченню кібербезпеки критичної інфраструктури в зарубіжних країнах. Специфіка різних сфер, віднесених до критичної інфраструктури, потребує особливої уваги при забезпеченні безпеки. Для кожної конкретної сфери заходи захисту, що застосовуються, повинні відповідати цілям безпеки, часто відмінним від конфіденційності, цілісності або доступності інформаційних ресурсів [21; 23].

Крім того, часто набір заходів захисту коригується у відповідності з обмеженнями фізичних ресурсів і процесів, або вимогами функціональної безпеки. У багатьох випадках це вимагає тісної співпраці регулюючих відомств, а також фахівців, відповідальних за проведення заходів захисту, та представників конкретних підприємств.

Особливо актуальна проблема організації такої взаємодії для приватних підприємств. Програми партнерства державного та приватного секторів у сфері кібербезпеки критичної інфраструктури спрямовані на вирішення саме цієї проблеми [28; 203].

Маючи зрілі механізми управління кібербезпекою критичної інфраструктури на державному рівні, задовольняє поточні потреби в безпеці кожної галузі критичної інфраструктури, враховуючи її специфічні обмеження, і сприяє безпечному розвитку всіх галузей у довгостроковій перспективі.

У зв'язку з цим цікаво простежити та порівняти показники зрілості управління кібербезпекою на державному рівні, наприклад, використовуючи дослідження стосовно досвіду зарубіжних країн.

Так, доцільно провести аналіз профілю з кіберблагополуччя Міжнародного союзу електрозв'язку для 196 країн. Для орієнтовної оцінки зрілості механізмів управління кібербезпекою критичної інфраструктури були розглянуті наступні заходи, які реалізуються на державному рівні:

- чи є офіційно прийнята стратегія або політика кібербезпеки критичної інфраструктури;

- чи створено офіційне відомство, відповідальне за забезпечення кібербезпеки критичної інфраструктури;

- чи створено офіційне відомство, відповідальне за повідомлення і обробку інцидентів кібербезпеки критичної інфраструктури;

- чи є офіційно прийнята програма міжвідомчого співробітництва у сфері кібербезпеки критичної інфраструктури;

- чи існує офіційно прийнята програма державно-приватного співробітництва у сфері кібербезпеки критичної інфраструктури (рис. 2.1).

Поєднання цих параметрів визначає рівень зрілості управління кібербезпекою критичної для держави інфраструктури.

Тим не менш тип стратегії управління кібербезпекою критичної інфраструктури визначається не одним або кількома з цих параметрів, а роллю офіційно відповідального за національну кібербезпеку критичної інфраструктури відомства в процесі реалізації заходів захисту критичних ресурсів від кібератак [38; 194].

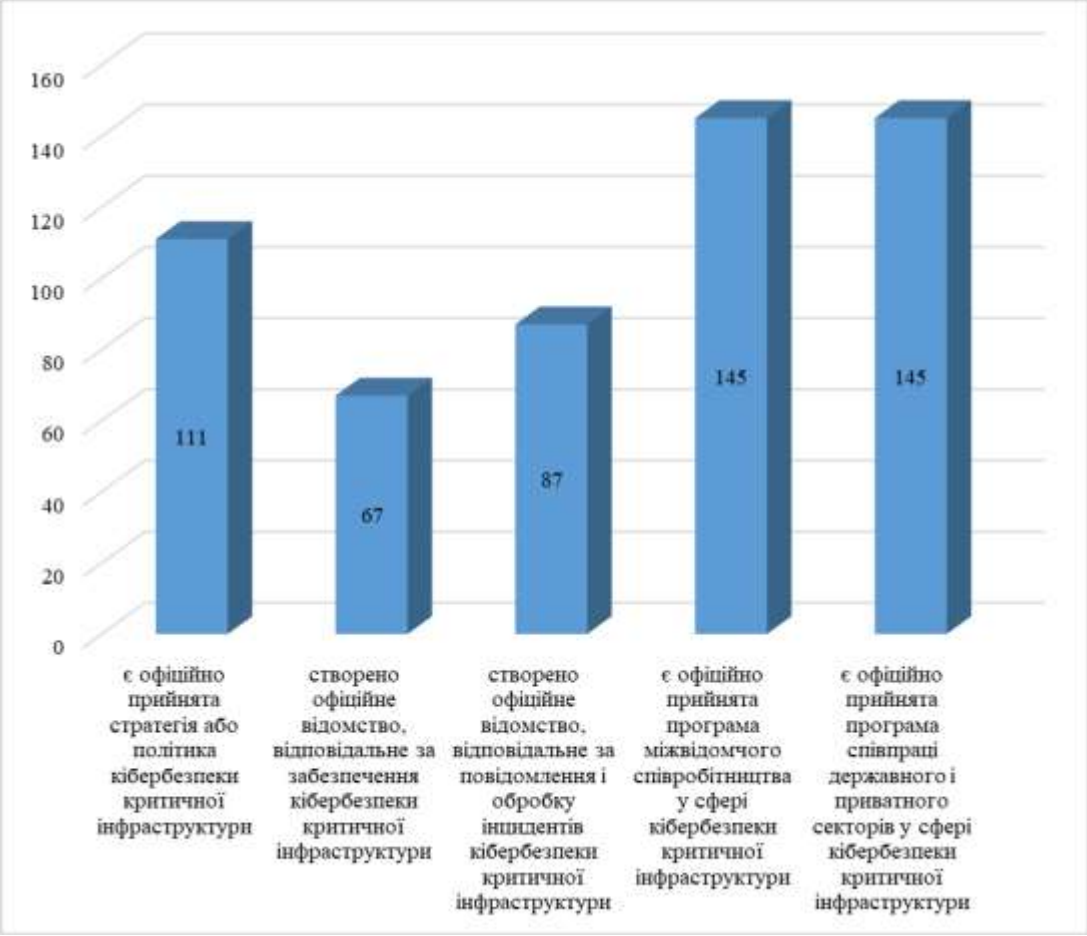

Рис. 2.1. Профіль з кіберблагополуччя Міжнародного союзу електрозв'язку для 196 країн, кількість країн

Джерело: складено на підставі [38]

До компетенції офіційного відомства, як правило, входять такі обов'язки:

- здійснювати управління діяльністю щодо забезпечення кібербезпеки критичної інфраструктури на державному рівні;

- забезпечувати взаємодію між відомствами, інтереси яких зачіпаються питаннями кібербезпеки критичної інфраструктури;

- приймати підзаконні нормативно-правові акти, спрямовані на регулювання заходів кіберзахисту критичної інфраструктури;

- надавати критерії ідентифікації та ідентифікувати життєво важливі системи;

- визначати необхідний набір технічних заходів захисту для кожної складової критичної інфраструктури;

- описувати і по можливості підтримувати процеси кібербезпеки критичної інфраструктури (такі як повідомлення про інциденти);

- реалізовувати оцінку кібербезпеки систем і сертифікацію продуктів кіберзахисту згідно встановленим критеріям;

- сприяти співпраці між державним та приватним сектором у сфері кібербезпеки критичної інфраструктури.

Дослідження практики управління кібербезпекою критичної інфраструктури з точки зору взаємодії між державою та приватним сектором визначило три основні типи стратегій цього управління, розглянуті нижче. Як правило, вибір тієї чи іншої стратегії визначається спільною розробкою регулюючих та виконавчих органів у галузі національної безпеки, кібербезпеки та безпеки окремих компонентів критичної інфраструктури [109; 203].

Своєчасна увага до особливостей стратегії та властивих її недоліків може забезпечити ефективне управління безпекою критичної інфраструктури. Наведене далі порівняння типів стратегії спрямоване на визначення цих недоліків та способів їх усунення.

У цьому контексті перш за все необхідно розглянути централізований підхід до управління цією діяльністю. Існує головне управління − державний орган або департамент, який одноосібно відповідає за забезпечення кібербезпеки критичної інфраструктури. 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. Підхід реалізується, наприклад, в Німеччині, Італії, Чехії, Естонії.

Заходи забезпечення безпеки добре задокументовані і, як правило, застосовуються до всіх областей відповідальності керівництва, за винятком випадків, коли це прямо зазначено.

Головне управління займається питаннями кібербезпеки критичної інфраструктури на державному рівні і, як правило, також відповідає за захист критичної інфраструктури від кібератак. З цією метою вона формулює директиви та рекомендації, які діють відповідно до вимог законодавства, встановлює вимоги до сертифікації, розробляє відповідні керівні документи та підтримує довгострокові державні програми (такі, як програма UP Kritis в Німеччині) [21; 77; 82].

Цей централізований підхід закріплений у Стратегії кібербезпеки Німеччини: "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». Федеральне управління з питань інформаційної безпеки Німеччини є головним органом, відповідальним за захист найважливіших інформаційних інфраструктур на федеральному рівні. Його діяльність контролюється Федеральним міністерством внутрішніх справ. У той час як

критична захист інфраструктури розглядається як мережеве завдання з участю різних органів на різних рівнях, всі відповідні програми та ініціативи кібербезпеки координуються Федеральним відомством з питань інформаційної безпеки Німеччини.

У Чехії основним органом є Управління Національної Безпеки, яке відповідає за кібербезпеку критичної інфраструктури, а також захист класифікованої інформації, управління допусками безпеки та управління криптографічним захистом. Захист критичної інфраструктури здійснюється Національним центром кібербезпеки, який є невід'ємною частиною Управління. У разі значного інциденту кібербезпеки, Управління виступає в якості провідного повноважного органу, який координує роботу інших відомств по обробці цього інциденту (включаючи різні державні та приватні установи). Відповідні суб'єкти можуть бути пов'язані рішеннями Управління національної безпеки у разі надзвичайного стану, а також у роботі з усунення загрози кібербезпеки або її наслідків. Управління підтримує операторів критичної інфраструктури у разі надзвичайних ситуацій та, за необхідності, забезпечує розслідування інцидентів [21; 22; 168].

Деякі країни не мають спеціального регулятора у сфері кібербезпеки критичної інфраструктури, але натомість наділяють офіційне представництво широкими повноваженнями з підтримки безпеки в національному кіберпросторі. Одним з прикладів є Латвія. Його національний орган із захисту критичної інфраструктури (Інститут реагування на інциденти безпеки інформаційної технології Латвійської Республіки) поділяє координуючу роль зі службою державної безпеки, Бюро по захисту Конституції, в рамках Міністерства оборони. Ці органи співпрацюють стосовно оцінки і управління поточними інформаційними ризиками для критичної інфраструктури. Бюро по захисту. Конституція має право перевіряти персонал, який бере участь у забезпеченні функціонування критично важливих об'єктів інфраструктури,

вимагати від Інституту реагування на інциденти безпеки інформаційних технології Латвійської Республіки провести інспекцію об'єктів інфраструктури для визначення її вразливостей та пов'язаних з цим ризиків, та давати рекомендації зацікавленим сторонам щодо усунення виявлених недоліків. Він також може давати рекомендації державним установам, які контролюють власників об'єктів критичної інфраструктури. Крім того, Бюро спільно з Інститутом реагування на інциденти безпеки інформаційної технології Латвійської Республіки періодично інформує Національну Раду Безпеки Інформаційних Технологій щодо актуальних загроз критично важливої інфраструктури.

В принципі, активну співпрацю 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 [28; 194; 203].

У цілому, аналіз профілів кіберблагополуччя Міжнародного союзу електрозв’язку показав, що 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 (це досить непоганий показник розподілу обов'язків у більшості країн). 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.

Таким чином, 64 держави з 196 демонструють зрілий підхід до управління кібербезпекою критичної інфраструктури (рис. 2.2).

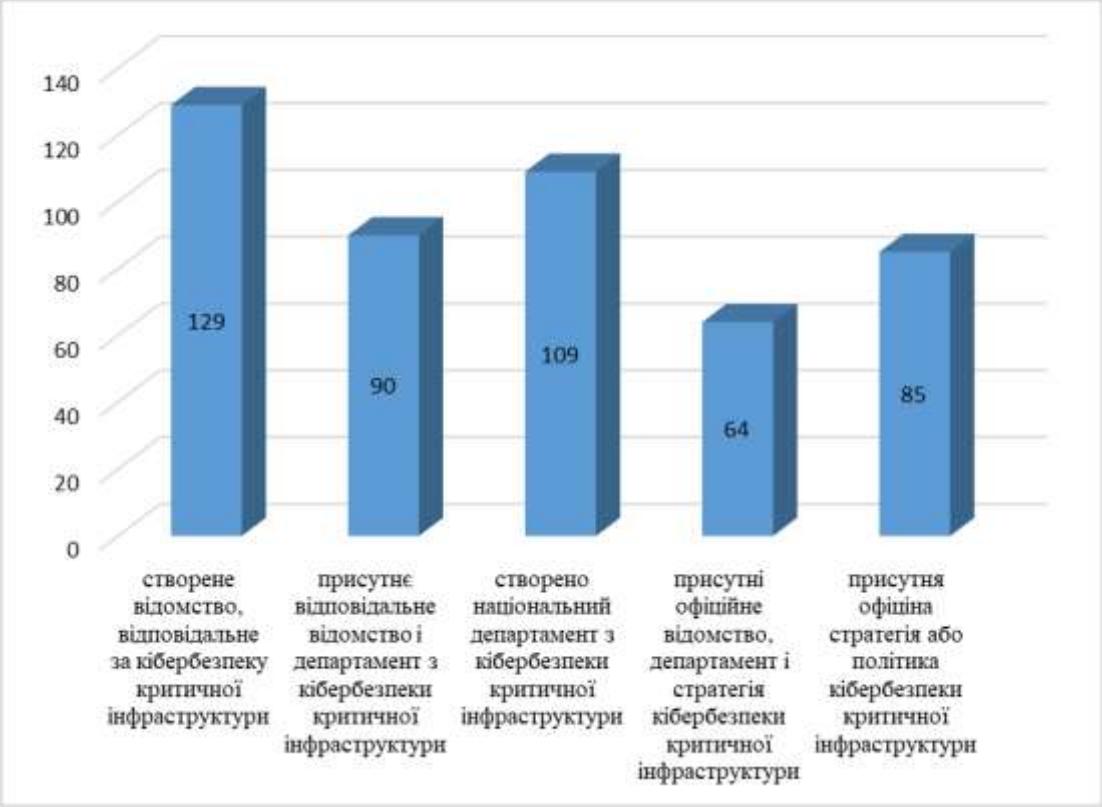

Рис. 2.2. Розподіл індикаторів зрілості управління кібербезпекою критичною інфраструктурою у країнах світу, кількість країн

Джерело: складено на підставі [38]

Незалежно від організаційної форми головного управління, ця стратегія часто має проблеми з побудовою відносин з приватним сектором. Це пов'язано з єдиними вимогами щодо впровадження до реалізації процедур та заходів з кібербезпеки незалежно від специфіки конкретної галузі критичної інфраструктури. Представники сфери критичної інфраструктури можуть сумніватися в тому, що фахівці з кібербезпеки є достатньо компетентні в цій галузі для здійснення будь-яких механізмів, або можуть не побачити зв'язку між кібератаками та можливими фізичними збитками. Власники приватних об'єктів, класифікованих як критична інфраструктура для забезпечення

кібербезпеки, можуть неохоче ділитися інформацією про свої випадки кібербезпеки [15; 23; 194].

Без залучення представників кожної конкретної сфери критичної інфраструктури розробка заходів захисту критичної інфраструктури може покладатися на помилкові цілі безпеки та ігнорувати практичний досвід, встановлюючи вимоги, які важко виконати через обмеження. Для вирішення цього питання деякі країни диверсифікують методи захисту критичної інфраструктури шляхом залучення в процес захисту зацікавлених сторін критичної інфраструктури.

Наприклад, німецький регулятор FederalOfficeforInformationSecurity реалізує згадану раніше програму UP Kritis. Зазначена програма UP Kritis також має справу з поняттями, які виходять за межі сфери інформаційних технологій в цілях підтримки і зміцнення доступності та надійності критично важливої інфраструктури. Для забезпечення всебічного захисту критично важливої інфраструктури слід спільно розробляти та впроваджувати заходи щодо фізичного захисту та безпеки інформаційних технологій. В рамках UP Kritis успішно реалізується співпраця між галузями промисловості і державою. Організації, що беруть участь у програмі, співпрацюють 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. В рамках UP Kritis розробляються нові концепції, встановлюються контакти, проводяться вправи, розробляється і використовується спільний підхід до антикризового управління інформаційними технологіями [21; 227].

За даними Міжнародного союзу електрозв’язку, 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 першому випадку у 17 країнах (рис. 2.3), а у другому - у 15 країнах із 51 (рис. 2.4).

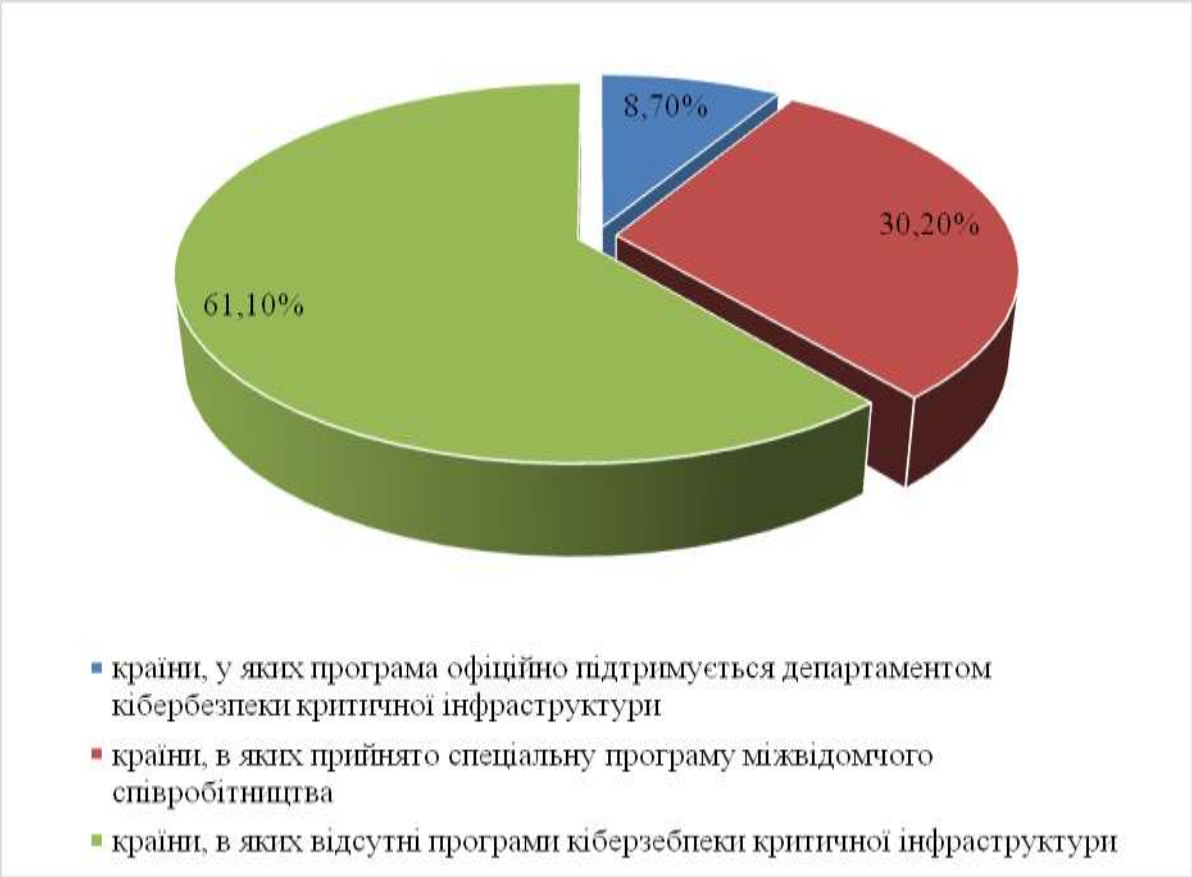

Рис. 2.3. Розподіл країн світу відповідно до рівня підтримки програм кіберзахисту критичної інфраструктури на рівні міжвідомчого співробітництва

Джерело: складено на підставі [109]

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.

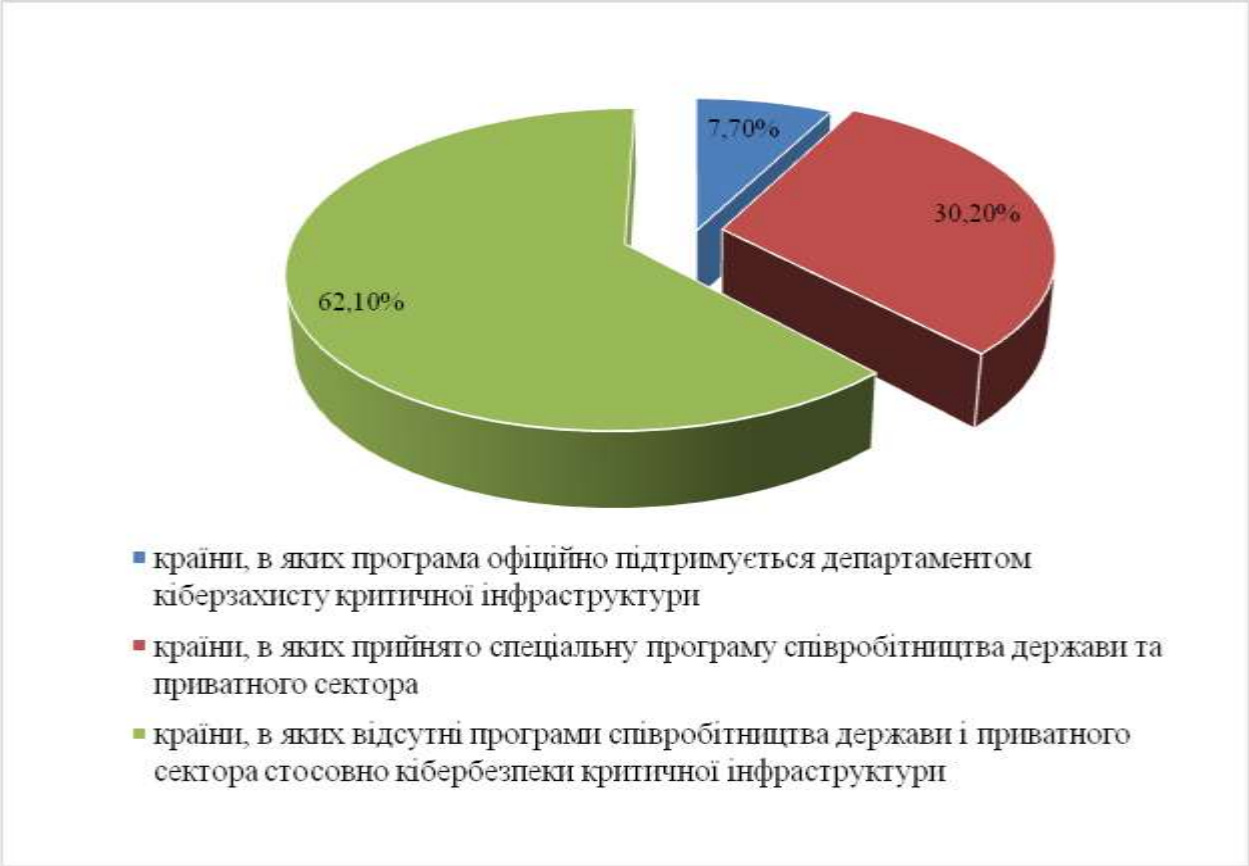

Рис. 2.4. Розподіл країн світу за рівнем підтримки програм кіберзахисту критичної інфраструктури на рівні співпраці держави та приватного сектору

Джерело: складено на підставі [109]

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.

Зокрема, в Австрії Федеральна канцелярія Австрії та Федеральне міністерство внутрішніх справ розподіляють відповідальність за захист критичної інфраструктури на стратегічному рівні. 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. Директор з інформаційних технологій Федеративної Республіки Австрії також є членом цього органу. Представники інших міністерств (зокрема, особи, відповідальні за організації та підприємства, які підлягають контролю або зачіпаються їм) та представники Австрійських федеральних земель приєднуються до Групи управління кібербезпекою критичної інфраструктури в міру необхідності для вирішення конкретних питань. Представники відповідних підприємств залучаються таким же чином. 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:

- 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 [23; 189].

Відомством, координуючим захист найважливіших складових критичної інфраструктури у Франції, є Генеральний секретаріат з питань оборони і національної безпеки (франц. «Secretariat general de la defense et de la securite nationale», SGDSN). 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 з таких питань, як:

- ідентифікація систем критичної важливості;

- визначення відповідних галузевих технічних правил і заходів захисту;

- опис процесів кібербезпеки критичної інфраструктури (таких як повідомлення про інцидент) [21; 28].

У Польщі головна відповідальність за захист критичної інфраструктури покладається на Центр державної безпеки (RCB), і всі відповідні заходи підтримуються через форуми співпраці між державними органами та операторами критичної інфраструктури. Засідання представників відповідних міністерств для обговорення питань захисту критичної інфраструктури проводяться кожні кілька місяців. Крім того, експертна група представників урядових установ збирається кожні два тижні для підготовки рекомендацій для Державного секретаря. Офіційно прийнята Політика захисту кіберпростору Республіки Польща поділяє дії, що стосуються безпеки інфраструктури інформаційних критичних технологій і дії, спрямовані на захист критичної інфраструктури. Зокрема, норми регулювання останніх містяться в Національній програмі захисту критичної інфраструктури. Стратегія національної безпеки Республіки Польща, зокрема, зазначає, що захист критичної інфраструктури є обов'язком операторів та власників, і ця відповідальність підтримується державною та адміністративною спроможністю.

У Фінляндії немає єдиного органу, відповідального за захист всіх секторів критичної інфраструктури. Стратегія кібербезпеки Фінляндії декларує, що більша частина критичної інфраструктури в суспільстві перебуває у приватній власності бізнесу. Ноу-хау та експертиза у сфері кіберсистем, а також послуги та засоби захисту в значній мірі належать приватним компаніям. Національне законодавство у сфері кібербезпеки критичної інфраструктури повинно

забезпечувати сприятливі умови для розвитку підприємницької діяльності. Національний центр кібербезпеки Фінляндії (далі − NCSC-FI) у складі Фінської органу нагляду за комунікаціями (далі − FICORA) є головним відповідальним за кібербезпеку критичної інфраструктури агентством у сфері зв'язку. Національне агентство з надзвичайних ситуацій, пов'язаних з поставками (далі − NESA), несе відповідальність за безпеку поставок, в тому числі забезпечення безперервності функціонування національної критичної інфраструктури. Інші специфічні для сфери критичної інфраструктури органи включають в себе такі:

- Управління з енергетики;

- Управління з радіаційної та ядерної безпеки;

- Орган контролю банківської діяльності;

- Національний орган нагляду в сфері соціального забезпечення та охорони здоров'я;

- Агентство з безпеки транспорту.

Як видно з наведених прикладів, 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 [15; 82].

При такому підході визначення цілей безпеки для кожної складової критичної інфраструктури вимагає менше зусиль. У той же час визначення вимог до заходів безпеки в цьому випадку також повинне бути виконано для кожного регіону окремо. Відсутність загальних вимог або показників веде до того, що процедури та заходи захисту для кожного регіону критичної інфраструктури будуть легалізуватися і застосовуватися неузгодженим чином. Потенційно це загрожує уповільненням процесів забезпечення кібербезпеки критичної інфраструктури [21; 203].

В окремих випадках держава дотримується «доктрини субсидіарності». Це означає повну передачу відповідальності власникам та операторам об'єктів критичної інфраструктури. Цей підхід реалізує, наприклад, Ірландія. 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. Так, в Ірландії немає відомства, відповідального за кібербезпеку критичної інфраструктури.

Ще одна країна, яка реалізує принцип субсидіарності у кіберзахисті критично важливої інфраструктури − Швейцарія. Вважається, що зацікавлені сторони знають власні процеси і системи найкращим чином і, отже, повинні нести відповідальність за виявлення всіх видів небезпеки для цих процесів і систем. Вони також повинні відповідати за прийняття відповідних заходів протидії. Уряд максимально сприяє процесам захисту критичної інфраструктури. Відповідно, оператори критичної інфраструктури самі несуть відповідальність за власну безпеку, але держава реалізує підтримуючі заходи. Таким чином, Центр обліку та аналізу захисту інформації є національним інформаційним центром для обміну даними про загрози та інциденти між приватним та державним секторами. Насправді він є основним органом у галузі кіберзахисту критичної інфраструктури Швейцарії, але використовується для підтримки у випадку інциденту.

Єдине відомство, відповідальне за кібербезпеку, здатне встановити межі, в яких кібербезпека критичної інфраструктури буде поступово покращуватися в усіх галузях критичної інфраструктури. Головною проблемою при цьому є те, що пропоновані в цих межах заходи захисту можуть не відповідати потребам кожного конкретного сектора [68, с. 91−92].

З іншого боку, підхід, заснований на саморегуляції, ідеально відповідає різноманітності потреб критичної інфраструктури. Але неможливо уникнути інцидентів кібербезпеки, багато з яких матимуть серйозні наслідки, якщо критична інфраструктура буде пошкоджена. Метод управління кібербезпекою критичної інфраструктури, який залучує до відповідних процесів кілька компетентних сторін за участю координуючого органу, виглядає «золотою серединою». Однак на практиці не завжди вдається уникнути ані жорсткості авторитарного підходу, ані неузгодженості розвитку, властивого саморегулюванню [15; 67].

Існує проміжний підхід, що передбачає часткову передачу відповідальності зацікавленим сторонам критичної інфраструктури (наприклад, власникам або операторам критичних інфраструктурних систем). Державний контроль за дотриманням вимог забезпечення кібербезпеки критичної інфраструктури здійснюється лише стосовно найважливіших підприємств та організацій, компрометація яких може мати значні наслідки на національному рівні. Такий підхід демонструє, наприклад, вже згаданий французький регулятор ANSSI.

Вимоги до реалізації заходів захисту, рекомендованих для підприємств критичної інфраструктури, застосовуються з пільгами для підприємств середнього рівня критичності, однак, у разі нехтування цими вимогами і при виникненні інциденту кібербезпеки буде відповідне покарання. Відповідальність за кіберзахист некритичних підприємств приватного сектора повністю лежить на їх власниках [21; 227].

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. Наприклад, 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 [39; 203].

Підтримка державою кіберзахисту критичної інфраструктури, будь то повноцінне управління всіма процесами або надання рамкових рекомендацій, повинна доповнюватися консультаціями з боку профільних компаній, експертів і дослідних центрів, а також розробників захисних рішень. Вони являють собою незалежне партнерство третьої сторони між державним та приватним сектором у сфері кібербезпеки критичної інфраструктури (де перший учасник - уповноважене відомство, а другий - представники секторів критичної інфраструктури). Взаємодія з експертною стороною забезпечує поінформованість про актуальні загрози і методи захисту від цих загроз, у тому числі відповідають спеціальним потребам секторів критичної інфраструктури.

Інформований вибір стратегії управління кібербезпекою критичної інфраструктури можливий лише для тих держав, які знаходяться в самому початку цього шляху. Згідно з даними Міжнародного союзу електрозв’язку, офіційний департамент із захисту критичної інфраструктури так чи інакше працює в більшості країн світу. Цей орган, через брак державного регулятора, може офіційно або неофіційно виступати також у ролі відомства відповідального за всі аспекти національної кібербезпеки. 150 країн розпочали діяльність з забезпечення кібербезпеки на національному рівні (принаймні мають або стратегію, офіційний орган, відповідальний за ці питання, або департамент), з яких 64 мають стратегію, відповідне відомство та департамент. 30 з цих 64 країн додатково визначають програми для міжвідомчого співробітництва та взаємодії держави і приватного сектора. Останні демонструють найбільш зрілий підхід до управління кібербезпекою і, як правило, особливу увагу приділяють захисту критичної інфраструктури від кібератак [39; 77].

Запропонований аналіз типів стратегій управління кібербезпекою критичної інфраструктури може бути використаний для своєчасного усунення недоліків цих стратегій. Методи, що застосовуються в рамках однієї стратегії, можуть адаптуватися до іншої для отримання оптимальних результатів.
Прикладом такої адаптації є часткове зняття з оператора системи низької важливості, яка відповідно до встановлених особливостей стосується критичної інфраструктури, формальних обов'язків за реалізацію запропонованих заходів кіберзахисту критичної інфраструктури.

У той же час ключові компанії, незалежні дослідники та відділи захисту критичної інфраструктури поступово займають ключову позицію у відносинах між державою та приватним сектором у сфері кібербезпеки критичної інфраструктури. Часто саме вони сприяють на глобальному рівні обміну сучасними законодавчими, оперативними й технічними практиками кіберзахисту критичної інфраструктури (наприклад, через стандартизацію та адаптацію посібників, що документують ці практики), що в кінцевому підсумку посилює кібербезпеку критичної інфраструктури по всьому світу [66; 71; 227].

2.2. Специфіка державного управління забезпеченням безпеки критичної інфраструктури в Україні

Обґрунтування вибору практичних підходів до вибору в сучасних умовах раціональної державної політики щодо безпеки населення та захисту об’єктів критичної інфраструктури в надзвичайних ситуаціях передбачає дослідження основних теоретичних підходів до організації відповідної системи державного управління та місцевого самоврядування на сучасному етапі [46; 52].

Однак аналіз та оцінка стану державного та муніципального управління в Україні, а також розробка пропозицій щодо її розвитку ускладнюються неоднозначністю ряду суспільно-політичних та економічних проблем, які

служать об’єктивними підставами безпосередньо для розвитку державного управління у сфері забезпечення безпеки критичної інфраструктури. Звідси – висока кон’юнктурність підходів, суб’єктивізм конкретних рішень, легковажне обґрунтування низки конкретних програм, ідей і пропозицій.

Сучасне суспільство, засноване на приватній власності і вільних ринкових відносинах, має тривалу історію і різні рівні розвитку: доіндустріальний, індустріальний, постіндустріальний, інформаційний. Крім того, воно дуже розрізняється за географічною та національною ознаками. В кожній країні її суспільство володіє своїми унікальними властивостями. Відповідно, необхідно, насамперед, визначитися, яким уявляється українське суспільство, що в ньому буде типовим згідно світовим параметрам і стандартам, а що – власне українським, відповідним нашій історії, географії та менталітету [78; 221].

В державному управлінні важливе значення суто в методологічному аспекті надається методам і засобам, завдяки яким досягається висунута мета. Вітчизняна та світова практика накопичила різноманітний досвід дій в трансформаційний період. Він також має значення, оскільки досягнення будь-яких цілей завжди пов’язане з використанням відповідних засобів, ресурсів, форм і методів, і часто останні мають вирішальний відбиток на результати реалізації цілей. Історичних прикладів на цю тему достатньо. Це питання безпосередньо приводить до функцій державного управління, які держава в особі своєї виконавчої влади і покликана виконувати [46; 51].

Особливу складність представляє визначення цілей, що об’єктивно стоять сьогодні перед державним управлінням і місцевим самоврядуванням України. Будучи відображенням усвідомлених потреб та національних інтересів, ідеальний прототип можливих шляхів та засобів їх досягнення, розумова спрямованість діяльності, цілей виконують у житті людей великі мотивуючі, стимулюючі та регулюючі функції. Будучи суб’єктивними за формулюванням, вони є об’єктивними за джерелом їх формування. Цілі державного управління та

місцевого самоврядування виникають на основі цілей, поставлених суспільством перед собою, і є похідними від них. Тим самим неясність у перших цілях призводить до неясності і в останніх.

У загальному та приблизному вигляді можна вважати, що в сучасний період перед державним управлінням, зокрема, стосовно забезпечення безпеки критичної інфраструктури об’єктивно поставлені наступні цілі [45; 53].

1. Формування нових інститутів державної влади та оптимізація діяльності існуючої системи виконавчої влади (адміністративна реформа).

2. Розгортання та зміцнення суспільних інститутів, які забезпечують стійку демократію суспільства та держави.

3. Створення та впровадження в життя соціальних та адміністративно-правових регуляторів, які гарантують конституційно проголошений комплекс прав, свобод та обов’язків громадян України.

4. Формування та практична реалізація державної політики, спрямованої на забезпечення безпеки населення та захист об’єктів критичної інфраструктури.

5. Забезпечення внутрішньої і зовнішньої безпеки регіонів України та сприятливих мирних умов для їх життєдіяльності.

6. Досягнення гармонійного, збалансованого і взаємопов’язаного розвитку регіонів у взаємодії з центром на основі поглиблення процесів формування і функціонування загальноукраїнського ринку.

Проблема встановлення цілей у державному управлінні, стосовно забезпечення безпеки критичної інфраструктури, вбачається не стільки в постановці та формулюванні окремих цілей, які держава покликана реалізовувати, скільки в побудові "дерева цілей", у якому б цілі стратегічні, оперативні і тактичні, кінцеві і проміжні, загальні і приватні, віддалені та близькі узгоджувалися, поєднувалися і представляли певну логічну цілісність.

Також важливо з’єднати «дерево цілей» з необхідними і адекватними засобами, ресурсами, методами і формами їх реалізації [15; 23].

Цілепокладання в державному управлінні об’єктивно пов’язане зі стратегічними національними інтересами України. Загальнонаціональна стратегія об’єднує суспільство і державу, класи й особистість, нації та регіони, а також концентрує енергію руху. Вироблення такої об’єднаної національної стратегії для України – актуальне завдання, реалізація якого закладе міцний фундамент для її зовнішньої і внутрішньої політики.

Питання про зміст та структуру функцій державного управління у сфері забезпечення безпеки населення та захисту об’єктів критичної інфраструктури передбачає визначення місця та ролі регіону України в конкретній галузі життєдіяльності. Саме місце і роль регіону припускають його зміст і форму, а потім функції управління та інші прояви [110; 137; 220].

Зокрема, під функціями державного та муніципального управління розуміються об'єктивно визначені типи влади, цілепокладання, організуючі та регулюючі впливи системи державних органів на певні процеси в суспільстві, природі тощо; ці дії певним чином відображаються на об’єктах, включаючи свідомість, поведінку та діяльність людей.

Сьогодні всі питання державного управління зосереджені як ніколи на проблемі забезпечення національної безпеки України, однією з ключових складових якої є забезпечення безпеки критичної інфраструктури. Управління безпекою в різних сферах життя людини, суспільства і держави, пошук ефективних способів вирішення поставлених перед суспільством завдань пронизують інтереси всіх верств населення, учених та практиків [148; 208].

Очевидно, що серед найгостріших економічних, харчових, енергетичних, соціальних, політичних та інших проблем, які наша країна має вирішити у XXI столітті, особливо на етапі переходу до сталого прогресивного розвитку, самі по собі проблеми природної та техногенної безпеки не є провідними. Але потрібно

враховувати, що вони чинять суттєвий вплив на стан економічного, екологічного та соціального забезпечення.

При цьому набір функцій державного управління залежить, з одного боку, від стану та структури керованих процесів - сукупності керованих об'єктів, а з іншого - від місця та ролі держави у сферах життєдіяльності. Держава пов’язана суспільством, відповідно, напрями розвитку держави визначаються потребами й інтересами суспільного розвитку. Цю взаємозалежність особливо важливо підкреслити, оскільки в багатьох політичних заявах і виступах засобів масової інформації постійно висувається теза про те, що держава має «піти» з суспільства, не заважати його волі, відкрити простір для творчості тощо. Однак вивільнення суспільства, його окремих відносин, процесів, явищ від цілеформуючих, організуючих і регулюючих впливів держави передбачає, що замість них будуть працювати самоврядні механізми (економічні, соціальні, культурні, інформаційні тощо), які підтримують досягнутий рівень організованості і врегульованості, інакше в суспільстві виникає стан некерованості, свавілля, анархії і хаосу [68; 70].

В сучасних умовах виявляються суперечливі суспільні потреби зменшення та зростання ролі держави. Перша полягає в скороченні директивного початку управління, зменшення державного сектора економіки і державного втручання в господарський процес. Друга полягає в розширенні функцій держави, у створенні ринкової інфраструктури, формуванні нових законодавчо-нормативних процедур господарських відносин і нових відносин власності. Необхідно відмовитися від механістичних підходів до визначення ролі та місця держави в суспільстві в трансформаційний період та врахувати складний баланс конфліктуючих потреб та тенденцій.

Розглядаючи функції державного управління у сфері забезпечення безпеки населення та захисту об’єктів критичної інфраструктури в цій роботі, доцільно виходити з аналізу всієї сукупності факторів, які в даний час

впливають на взаємозв'язок держави та суспільства, а також на ту обставину, що суспільство наразі не готове взяти на себе функції, що виконуються державними структурами. Протистояти впливу надзвичайних ситуацій на сталий розвиток України в сучасних умовах можна лише завдяки стратегічній ролі держави у цьому процесі [46; 49; 52].

У світовій практиці й теорії, що стосується державного управління, менеджменту й інших видів управління, до загальних функцій управління цілком обґрунтовано відносять: планування, організацію, регулювання, роботу з персоналом, контроль.

Це особливо важливо при оптимізації функцій органів виконавчої влади регіонів України в рамках адміністративної реформи. Відмова від функцій планування і контролю в державному управлінні, зокрема, стосовно забезпечення безпеки критичної інфраструктури, де довгостроковий (стратегічний) погляд вкрай необхідний, навряд чи виправданий, тому що десятки мільйонів людей беруть участь у соціальних процесах, що підлягають державному управлінню.

На управлінській практиці позначаються ігнорування і недооцінка функції організації, що стосується, зокрема, взаємодії різноманітних організаційних структур: замість свідомої організації (як статичної, так і динамічної), зроблений упор на стихійну самоорганізацію. Однак весь світовий досвід суперечить таким діям і практично скрізь організаційний резерв є найважливішим для вирішення проблем суспільного розвитку.

Потрібен більш серйозний підхід до реалізації функції регулювання як на законодавчому рівні (створення правил поведінки), так і на виконавчому, що забезпечує практичне дотримання встановлених правил, норм й інших регуляторів, що дозволило б уникнути існуючої нерівномірності у сфері суспільної й особистої безпеки.

При цьому необхідно підкреслити, що державне управління на рівні регіону України в теоретичному плані достатньо не вивчено. В цьому випадку для формування раціональних структур управління надзвичайно важливо осягнути глибину і складність реальних проблем України в період проведеної в країні адміністративної реформи, зрозуміти закономірності цього періоду і врахувати їх при реформуванні систем управління. При цьому необхідним є зважений погляд на стан суспільства, його можливості та перспективи, ресурси, резерви, потенціал і джерела зростання [10; 13; 24].

Реформування системи забезпечення безпеки населення та захисту критично важливих при надзвичайних ситуаціях та терористичних актах об'єктів неможливі без здійснення специфічних функцій управління, тих, які притаманні саме державі і повинні реалізовуватися за допомогою управлінських функцій спеціальних державних органів.

Наукова методологія потребує розгляду врахування особливостей державного управління та місцевого самоврядування в Україні як мінімум у чотирьох областях:

- з точки зору наявності існуючих в країні орієнтацій на вікові традиції, зокрема, політичної культури населення і правлячих груп (претендентів на владу), що більшою чи меншою мірою визначають реалізацію розглянутої проблеми. Не обов'язково, щоб ці традиції визначали процес державного управління. Безсумнівно, однак, що заперечення їх у нинішній ситуації в кінцевому рахунку створює тупикову ситуацію;

- урахування сьогоднішнього соціально-політичного та економічного становища. Аналіз цього фактору є необхідним, оскільки він дозволяє, з одного боку, вибудовувати розробку рішень поставленої проблеми на реальному фундаменті, з іншого – дає можливість врахувати минуще, характерне лише для сьогоднішнього моменту, а також зосередитися на дійсно ключових проблемах

оптимізації механізмів та структур державного управління, зокрема, стосовно забезпечення безпеки критичної інфраструктури;

- з урахуванням глобального аспекту завдань державного управління, що вирішуються в Україні. Світовий досвід дає не тільки і не стільки знань про можливі рішення конкретних управлінських завдань. Глобальний контекст дозволяє вибудовувати пропоновані рішення так, щоб спрогнозувати світові поточні тенденції, зберегти українську самобутність і використовувати дійсно оптимальні варіанти вирішення проблем державного управління, зокрема, стосовно забезпечення безпеки критичної інфраструктури;

- використання загальнонаукового принципу подвійної герменевтики, тобто подвійної інтерпретації вирішення дослідницької проблеми, яка зараз є ключовою: строго науковий аналіз проблем державного управління з урахуванням фундаментальних аспектів проблеми, новітніх наукових розробок тощо стосовно державного управління у сфері забезпечення безпеки критичної інфраструктури [46; 54; 78].

В умовах загострення загроз природного та техногенного характеру, а також зростання ймовірності вчинення терористичних актів першорядне значення набуває питання підвищення охорони критично небезпечних та потенційно небезпечних об'єктів. Аналіз життєвого циклу та чинників небезпеки критично важливого об'єкта дозволяє стверджувати про імовірнісний характер небезпек, що виникають при поводженні з небезпечними речовинами.

Так, дослідження ряду робіт показують, що джерело небезпеки за своєю суттю має природне, космічне, технічне і соціально-економічне походження. До найбільш небезпечних джерел виникнення подій надзвичайного характеру відносяться такі:

- несприятливі природні явища;

- стихійні лиха та природні катастрофи;

- природні ризики, що виникають в процесі господарської діяльності людини та пов'язані з накопиченим екологічним збитком;

- техногенні аварії та катастрофи, а також прояви терористичного характеру [34; 148; 182].

У загальному випадку загроза заподіяння шкоди залежить від взаємного положення джерела небезпеки та впливу небезпечних факторів у просторі та в часі на об'єкт (для стаціонарних об'єктів у просторі). Небезпеки становлять загрозу лише тоді, коли вони можуть завдати шкоди конкретним об'єктам. Небезпека або кілька різних небезпек становлять загрозу для об'єкта тільки в тому випадку, якщо їх небезпечні фактори можуть вплинути на його дію. Наприклад, для людей загроза виникає, коли вони працюють на об'єкті підвищеного ризику або в зоні забруднення, а для рухомих об’єктів - коли вони під час небезпечної події знаходяться в зоні впливу небезпечних факторів [91; 179].

Ступінь загрози для життєдіяльності населення в цій місцевості залежить від ступеня її небезпеки, а також від географічних та часових факторів. Якщо об’єкт перенести за межі небезпечної території, загрози йому не буде, хоча небезпека території залишатиметься. Загроза життю з часом змінюється: вона може виникати, збільшуватися, зменшуватися. Безпека населення, різних об'єктів та навколишнього середовища у разі надзвичайних ситуацій, спричинених техногенними ситуаціями та стихійними лихами, встановлюється шляхом оцінки ризику для окремого підприємства чи території порівняно з відповідними нормативними параметрами.

Зокрема, ризик − це ймовірнісна міра небезпеки або сукупності небезпек, встановлена для певного об'єкта у вигляді можливих втрат за заданий час або усвідомлена небезпека (загроза) настання в будь-якій системі негативної події з визначеними у часі та просторі наслідками [18; 20; 231].

Крім того, терміну «ризик» дається таке визначення: це ймовірність заподіяння шкоди життю та здоров'ю громадян, майну фізичних чи юридичних осіб, державній чи муніципальній власності, навколишньому середовищу, життю та здоров'ю тварин та рослин, з урахуванням тяжкості цієї шкоди.

Застосування поняття "ризик" дозволяє перевести небезпеку в категорію вимірюваних категорій. Ризик насправді є мірою небезпеки. При цьому всі практичні заходи щодо управління ризиками базуються на концепції прийнятного ризику, суть якої полягає у прагненні звести його до безпечного рівня. Рівень прийнятного ризику задається пороговими значеннями розміру збитку і ймовірності його виникнення [36; 231].

Число різновидів ризику досить велике, але в зв'язку з надзвичайними ситуаціями розглядаються так звані «чисті ризики», які передбачають тільки небажаний (негативний) ефект. До них можна віднести ризики можливих втрат:

- популяційний;
- диференційований;
- індивідуальний;
- інтегральний (сумарний, сукупний);
- природний;
- фізичний;
- екологічний;
- економічний;
- соціальний (колективний, груповий) тощо.

Для умов надзвичайних ситуацій необхідно отримання оцінок індивідуального і соціального ризиків. В деяких окремих випадках, наприклад, для небезпечних технологічних процесів, виконують оцінку регламентованих параметрів небезпек. Зокрема, індивідуальний ризик (розподіл ризику) – це ймовірність (частота) виникнення небезпечних факторів при надзвичайній ситуації у визначеному місці простору [13; 19; 26].

Соціальний ризик (характерний для масштабу небезпеки), у свою чергу, залежить від ймовірності ураження певної кількості людей від загальної кількості людей, що зазнали факторам впливу в надзвичайних ситуаціях. Існуючі методи проведення аналізу й оцінки ризику, викладені в методичних вказівках щодо проведення оцінки ризику небезпечних виробничих об'єктів, мають переважно якісний характер.

Великі аварії зазвичай характеризуються поєднанням випадкових подій, які відбуваються з різною частотою і на різних стадіях виникнення та розвитку аварій. Логічні та графічні методи аналізу "дерев відмов" та "дерев подій" використовуються для виявлення причинно-наслідкового зв'язку між цими подіями.

Кількісний аналіз ризиків вимагає використання методів теорії надійності, імітаційного та статистичного моделювання, теорії випадкових процесів, а також закономірностей виникнення та розвитку аварій та надзвичайних ситуацій.

Аналіз економічної безпеки для страхових компаній готується на основі ступеня оцінки ризику надзвичайних ситуацій на критичних та потенційно небезпечних об'єктах, що в свою чергу визначатиме розмір страхового внеску підприємства, його страхового зобов'язання перед третіми особами, а також страхування підприємства в цілому. У цьому випадку існує інтерес потенційно небезпечних об'єктів у ланцюжку "вартість - безпека - вигода", щоб виключити або значно зменшити фінансування заходів безпеки та створити ланцюг "ціна - вигода".

Використовуються результати аналізу ризику виникнення надзвичайних ситуацій природного та техногенного характеру:

- декларування промислової безпеки небезпечних виробничих об'єктів;

- експертизи промислової безпеки та погодження паспортів безпеки;

- обґрунтування технічних рішень по забезпеченню безпеки критично важливих об'єктів;

- страхування;

- економічного аналізу безпеки за критеріями «вартість – безпека − вигода»;

- оцінки інтегрального впливу на навколишнє природне середовище

та інших процедурах, пов'язаних з аналізом безпеки [148; 248].

При цьому з внутрішніх подій виникнення аварійних ситуацій на критично важливих об’єктах, наприклад, можна розглядати наступні.

1. У зоні зберігання і перевезення потенційно небезпечної речовини в ємностях:

- падіння ємності (боєприпасу) внаслідок помилки людини або відмови механічного обладнання, результатом чого є вибух, розгерметизація і витік небезпечної речовини;

- удар по ємності (боєприпасу) з порушенням його цілісності при проведенні вантажно-розвантажувальних робіт внаслідок помилки людини або відмови механізмів з виникненням або без виникнення вибуху з пожежею;

- пожежа всередині складського приміщення в результаті загоряння з технічних причин;

- підтікання ємності (боєприпасу) внаслідок порушення герметичності в результаті корозії (заводський брак);

- аварія з транспортним засобом, що перевозить ємності (боєприпаси), із зіткненням і перекиданням, в результаті чого мають місце вибух, пожежа, розгерметизація (пробій) або термічний вплив на них.

2. У промисловій зоні, де проводяться роботи з небезпечними речовинами:

- пробій (руйнування) ємності (боєприпасу) до надходження його в цех (ділянку) знаряддя або переробки;

- руйнування (відмова) технічних засобів знаряддя або переробки;

- порушення цілісності ємності і трубопроводів;

- руйнування ємності детоксикації, накопичувача і зберігання продукції детоксикації або переробки хімічних речовин.

З зовнішніх подій виникнення аварійних ситуацій можуть розглядатися наступні:

- пожежа всередині приміщення, що містить небезпечну речовину або її елементи, в результаті займання від зовнішнього джерела;

- удар блискавки в ємності (боєприпаси), розташовані на відкритих майданчиках;

- руйнування об'єктів, будівель, систем, що містять небезпечні речовини, в результаті урагану, смерчу;

- падіння літального апарату (космічного апарату, літака, гвинтокрила, планера, повітряної кулі) в результаті авіаційної катастрофи;

- руйнування об'єктів у результаті землетрусу, наслідком чого є падіння або удар з порушенням герметичності або (і) виникнення пожежі ємності (боєприпасів);

- падіння метеорита в зону зберігання об'єкта;

- терористичний акт, в тому числі підрив заряду вибухової речовини, обстріл об'єкта з термобаричної (реактивної) запальної зброї;

- катастрофа з виділенням енергії, достатньої для руйнування об'єкта;

- катастрофа на об'єкті поблизу залізничних (автомобільних) магістралей з виділенням енергії, достатньої для руйнування об'єкта [121; 182].

Необхідно при цьому проаналізувати кількісні показники надзвичайних ситуацій в Україні, зокрема, стосовно об’єктів критичної інфраструктури протягом 2018-2019 років.

Так, статистичні дані щодо кількості надзвичайних ситуацій у 2018 році за джерелом походження відображені у табл. 2.1.

Таблиця 2.1

Кількість надзвичайних ситуацій за джерелом походження у 2018 році

Джерело походження надзвичайних ситуацій	Кількість
Техногенні	48
Природні	77
Соціальні	3
Разом	128

Джерело: складено на підставі статистичних даних ДСНС

Відсотковий розподіл надзвичайних ситуацій в Україні у 2018 році можна побачити у табл. 2.2.

Таблиця 2.2

Відсотковий розподіл надзвичайних ситуацій за джерелом походження у 2018 році

Джерело походження надзвичайних ситуацій	Відсоток від загальної кількості, %
Техногенні	37,5
Природні	60,1
Соціальні	0,4
Разом	100

Джерело: складено на підставі статистичних даних ДСНС

З табл. 2.1 та 2.2 можна побачити, що у 2018 році в Україні надзвичайні ситуацій природного походження склали 60% від загальної їх кількості.

Що стосується 2019 року, то розподіл надзвичайних ситуацій за джерелом їх походження наведено у табл. 2.3.

Таблиця 2.3

Кількість надзвичайних ситуацій за джерелом походження у 2019 році

Джерело походження надзвичайних ситуацій	Кількість
Техногенні	60
Природні	81
Соціальні	5
Разом	146

Джерело: складено на підставі статистичних даних ДСНС

Відсотковий склад надзвичайних ситуацій в Україні у 2019 році за джерелом їх походження представлено у табл. 2.4.

Таблиця 2.4

Відсотковий розподіл надзвичайних ситуацій за джерелом походження у 2019 році

Джерело походження надзвичайних ситуацій	Відсоток від загальної кількості, %
Техногенні	41,1
Природні	55,5
Соціальні	3,4
Разом	100

Джерело: складено на підставі статистичних даних ДСНС

З табл. 2.3 та 2.4 можна побачити, що надзвичайні ситуації природного характеру у 2019 році знову знаходяться на першому місці та складають 55,5% від загальної кількості надзвичайних ситуацій. Однак їх відсоткова частка стала меншою на 4,9%.

Нижче доцільно провести аналіз надзвичайних ситуацій виключно на об’єктах критичної інфраструктури. Так, у табл. 2.5 представлено відповідний розподіл надзвичайних ситуацій в Україні у 2018 році.

Таблиця 2.5

Кількість надзвичайних ситуацій на різнохарактерних об’єктах критичної інфраструктури України у 2018 році

Причина походження надзвичайних ситуацій	Кількість
Раптове руйнування будівель і споруд	0
Аварії в електроенергетичних системах	1
Аварії у системах життєзабезпечення	5
Разом	6

Джерело: складено на підставі статистичних даних ДСНС

Нижче, у табл. 2.6 показано відсотковий розподіл надзвичайних ситуацій на об’єктах критичної інфраструктури України протягом 2018 року.

Таблиця 2.6

Відсотковий розподіл надзвичайних ситуацій на різнохарактерних об’єктах критичної інфраструктури України у 2018 році

Причина походження надзвичайних ситуацій	Відсоток від загальної кількості, %
Раптове руйнування будівель і споруд	0
Аварії в електроенергетичних системах	16,7
Аварії у системах життєзабезпечення	83,3
Разом	100

Джерело: складено на підставі статистичних даних ДСНС

З табл. 2.5 та 2.6 можна побачити, що аварії у системах забезпечення займали у 2018 році найбільший відсоток від загальної кількості надзвичайних ситуацій на різнохарактерних об’єктах критичної інфраструктури України – 83,3%.

Що стосується 2019 року, то розподіл надзвичайних ситуацій на об’єктах критичної інфраструктури України наведено у табл. 2.7.

Таблиця 2.7

Кількість надзвичайних ситуацій на різнохарактерних об’єктах критичної інфраструктури України у 2019 році

Причина походження надзвичайних ситуацій	Кількість
Раптове руйнування будівель і споруд	3
Аварії в електроенергетичних системах	4
Аварії у системах життєзабезпечення	0
Разом	7

Джерело: складено на підставі статистичних даних ДСНС

Відповідний відсотковий розподіл надзвичайних ситуацій на об’єктах критичної інфраструктури України у 2019 році наведено у табл. 2.8.

Таблиця 2.8

Відсотковий розподіл надзвичайних ситуацій на різнохарактерних об’єктах критичної інфраструктури України у 2019 році

Причина походження надзвичайних ситуацій	Відсоток від загальної кількості, %
Раптове руйнування будівель і споруд	42,9
Аварії в електроенергетичних системах	57,1
Аварії у системах життєзабезпечення	0
Разом	100

Джерело: складено на підставі статистичних даних ДСНС

З табл. 2.7 та 2.8 можна побачити, що у 2019 році 57,1% склали аварії в електроенергетичних системах. Відповідно, вони посідають перше місце надзвичайних ситуацій на різнохарактерних об’єктах критичної інфраструктури України.

При цьому прогнозування наслідків надзвичайних ситуацій здійснюється в кілька етапів.

На І етапі встановлюють параметри впливів − значущих вражаючих факторів, що викликають основні руйнування і ураження, з характеристиками, що зазвичай приймаються з використанням існуючих методик.

На ІІ етапі встановлюють закони поразки − опір елементів ризику впливів, під якими розуміють залежності ймовірності поразки від інтенсивності прояву вражаючих факторів, застосовуючи для їх формалізації ті чи інші функції, відповідні даній надзвичайній ситуації

На ІІІ етапі прогнозування дається оцінка наслідків сполученням моделей впливу і законів ураження (руйнування / пошкодження). Використовуючи цей методичний підхід, оцінюються наслідки майже всіх природних катастроф та техногенних аварій для прийняття рішень щодо організації екстреної евакуації населення з надзвичайних районів та його життєзабезпечення на безпечних територіях, залучення сил та засобів Державної служби України з надзвичайних ситуацій різного рівня для ліквідації надзвичайних ситуацій [34; 94; 182].

При цьому вплив вражаючих чинників на об'єкти і людей при аваріях і катастрофах з можливими наслідками описують з використанням моделей. Моделі впливу − це залежність, що визначає розміри поля потенційної небезпеки (негативного впливу), розподіл інтенсивності вражаючих факторів в межах поля і частоту події. Поля потенційної небезпеки, зокрема, можна описати у вигляді аналітичних, табличних або графічних залежностей.

Таким чином, за результатами аналізу статистичних даних 1999–2019 рр. у 2020 році в Україні очікується така ситуація щодо надзвичайних ситуацій на

критичних об'єктах в регіонах України: у лютому 2020 року - високий ризик виникнення аварій на шахтах та раптових руйнувань будівель, а також пожеж та вибухів у Запорізькій, Донецькій, Дніпропетровській, Одеській, Харківській, Черкаській областях

2.3. Оцінка вітчизняного нормативного й адміністративного забезпечення державного управління забезпеченням безпеки критичної інфраструктури

Перш ніж проводити оцінку вітчизняного нормативного та адміністративне забезпечення державного управління критичною інфраструктурою, слід зазначити, що, наведене в параграфах. 2.1 Аналіз, в країнах Європи концепція критичної інфраструктури надійшла в обіг у 1998 році через зростаючу терористичну загрозу. Зокрема, першою країною, яка звернула увагу на необхідність захисту телекомунікаційних мереж, систем банківського і фінансового сектору, устаткування з водопостачання, енергозбереження тощо та інших об’єктів, які забезпечують життєдіяльність країни й її економічний потенціал, була Британія. Після того, як у вересні 2001 року в США відбувся масштабний теракт, країна почала активно здійснювати заходи щодо захисту економічної безпеки. Зокрема, до переліку основних об’єктів критичної інфраструктури країни було включено наступне:

- культурні пам'ятки національного значення;
- ядерні електростанції;
- дамби і греблі;
- будівлі урядового та комерційного призначення;
- інші місця, в яких одночасно може концентруватися велика кількість людей.

У зв'язку з цими світовими тенденціями Україна також почала приділяти увагу створенню власної системи захисту об'єктів критичної інфраструктури. Зокрема, була опублікована Зелена книга − збірник матеріалів, що містять роботи міжнародних експертів, які висвітлюють питання захисту критичної інфраструктури [22; 95].

Що стосується практичної імплементації нових підходів до забезпечення захисту критичної інфраструктури, то вона була зафіксована з прийняттям Закону України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII. Крім того, було підготовлено проект Закону «Про критичну інфраструктуру та її захист», який був покликаний забезпечити формування необхідної для цього нормативно-правової бази [88; 189; 208].

Необхідно відмітити, що, розробляючи вітчизняну стратегію захисту критичної інфраструктури, доцільно звернутися до досвіду США, який передбачає дотримання таких напрямів:

- запобігання і нейтралізація терористичних дій, а також стримування, або пом'якшення наслідків спричинених діями терористів, та спрямованих на повне знищення, часткове виведення з ладу або використання зі зловмисними цілями об’єктів критичної інфраструктури;

- посилення готовності до терористичних дій на національному рівні;

- своєчасне реагування та якнайшвидше відновлення та відбудова об’єктів критичної інфраструктури у разі стихійних лих, атак чи інших надзвичайних ситуацій.

Крім того, у межах державної системи захисту критичної інфраструктури повинні бути об'єднані зусилля різнохарактерних інституцій щодо захисту об’єктів критичної інфраструктури і своєчасного реагування на негативні випадки. Зокрема, до подібних інституцій слід віднести такі складові:

- підсистема цивільного захисту;

- підсистема фізичного захисту;

-підсистема кібернетичного захисту;

- підсистема антитерористичного захисту.

Зазначені підсистеми повинні бути об’єднані в узгоджену систему, яка уможливлює адекватне і своєчасне реагування на різнохарактерні загрози. Детальне впровадження запропонованого підходу дозволить сформувати сучасну систему захисту критичної інфраструктури на державному рівні, яка зможе відповідати на нові типи викликів [22; 70].

Відповідно, на Міністерство розвитку економіки, торгівлі та сільського господарства України було покладено урядове завдання стосовно розробки проекту Закону «Про критичну інфраструктуру України та її захист» [189].

З цією метою була створена робоча група, до складу якої входили представники міністерств та інших центральних органів виконавчої влади. Відповідно до цього законопроекту, забезпечення захисту критичної інфраструктури є складовою забезпечення національної безпеки України. Щодо державної політики у сфері захисту критичної інфраструктури України, то вона має базуватися на таких принципах:

- визнання об’єктивної необхідності забезпечення стабільного і безперервного функціонування критичної інфраструктури;

- законодавче встановлення вимог щодо забезпечення захисту об’єктів критичний інфраструктурі;

- визначення повноважень та відповідальності суб'єктів державної системи захисту критичний інфраструктурі;

- створення сприятливих умов, спрямованих на мінімізацію поширення можливих загроз, а також усунення або мінімізацію наслідків перетворення загрози в надзвичайну ситуацію;

- забезпечення можливості швидкого та ефективного відновлення процесів функціонування критичної інфраструктури у випадках перетворення загроз у надзвичайні ситуації;;

- побудова системи оперативного виявлення загроз критичній інфраструктурі;

- забезпечення взаємодії держави, суб'єктів господарювання, представників експертного середовища та населення з питань забезпечення безпеки та стабільного функціонування критичної інфраструктури;

- забезпечення співпраці щодо захисту критичної інфраструктури на міжнародному рівні [22; 145].

В Україні очікується комплексне створення державної системи захисту критичної інфраструктури на період з 2017 по 2027 роки. Зазначена система визначає створення якісно нового рівня державного управління у цій галузі:

- вироблення сучасних інноваційних підходів до управління ризиками безпеки критичної інфраструктури;

- оптимізоване застосування наявних ресурсів, гнучке і швидке реагування на інциденти і кризи.

Разом з тим, необхідно розуміти, що з одного боку необхідно закріпити модель формування державної системи захисту критичної інфраструктури з законодавчої точки зору, а з іншого боку необхідно створити ефективний механізм реагування на загрози критичній інфраструктурі. А це вимагає наявності консолідації зусиль усього сектору безпеки та оборони держави.

У цьому контексті Служба безпеки України забезпечує захист економічної безпеки держави виходячи з того, що економічні злочини в сучасних умовах є однією з ключових загроз для об'єктів критичної інфраструктури. Так, Закон України «Про службу безпеки України» 25 березня 1992 року № 2229-XII із останніми змінами і доповненнями наділив Службу безпеки України повноваженнями щодо захисту об'єктів критичної інфраструктури. Слід при цьому підкреслити, що Служба безпеки України займається зазначеним питанням вже понад 5 років. Це, перш за все, визначається тим, що складна ситуація щодо забезпечення безпеки в державі потребує застосування

відповідних заходів як превентивного, так і реагувального характеру з метою забезпечення стабільності функціонування об'єктів життєзабезпечення [92; 208].

Деякі цільові повноваження Служби безпеки України підлягають деталізації з урахуванням поточних тенденцій в новому проекті Закону «Про критичну інфраструктуру України», де вони:

- більш конкретні;

- зрозумілі для широких верств населення;

- надають інструменти та вказують вектори діяльності, за яким служба буде рухатися в бік ефективного захисту критичної інфраструктури з метою забезпечення стійкості держави до різнохарактерних викликів і загроз [189].

В контексті забезпечення захисту критичної інфраструктури досвід Польщі є дуже корисним для України. Зокрема, для цього в Україні у 2019 році відбувся Міжнародний науково-практичний семінар "Становлення та перспективи розвитку державної системи захисту критичної інфраструктури в Україні" в рамках проекту Організації з безпеки і співпраці в Європі (ОБСЄ) «Технічна підтримка реформування спеціальних служб і органів кримінальної юстиції України з метою забезпечення дотримання зобов'язань в сфері захисту прав людини», розробленого на запит Служби безпеки України і спрямованого на підтримку зобов'язань України щодо забезпечення національної безпеки. Зазначений семінар є складовою комплексу спільних з ОБСЄ міжнародних заходів, орієнтованих на формування і становлення національної системи захисту критичної інфраструктури в Україні. Зокрема, рекомендації та знання, отримані від країн, які вже мають масштабний досвід стосовно забезпечення безпеки критичної інфраструктури, дозволять зміцнити засади функціонування державної системи захисту критичної інфраструктури [21; 92; 208].

Ключовим державним органом в Україні щодо управління критичною інфраструктурою є Державна служба України з надзвичайних ситуацій (Далі – ДСНС України).

Основними завданнями ДСНС України є такі:

- реалізація державної політики у сфері запобігання та ліквідації надзвичайних ситуацій природного та техногенного характеру (аварії, катастрофи, стихійні та інші катастрофи), забезпечення пожежної, промислової та радіаційної безпеки, цивільної оборони;

- здійснення державного нагляду, контрольних, дозвільних та інших спеціальних функцій у галузі захисту населення та територій від надзвичайних ситуацій природного та техногенного характеру, забезпечення пожежної, промислової та радіаційної безпеки, цивільної оборони;

- 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 функціонування державної системи запобігання та ліквідації надзвичайних ситуацій та державної системи пожежної безпеки;

- керівництво органами і підрозділами з надзвичайних ситуацій;

- 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;

- виконання інших завдань за дорученням Президента України. [46; 80; 145].

Що стосується функцій ДСНС України, то, відповідно до покладених на неї завдань, можна виділити наступне:

- здійснює організаційне та науково-технічне забезпечення функціонування державної системи запобігання та ліквідації надзвичайних ситуацій та державної системи пожежної безпеки;

- розробляє та вносить у встановленому порядку пропозиції щодо вдосконалення законодавства з питань, що належать до компетенції ДСНС України;

- здійснює в установленому порядку міжнародне співробітництво у сфері запобігання та ліквідації надзвичайних ситуацій природного та техногенного характеру, забезпечення пожежної, промислової та радіаційної безпеки, цивільної оборони, включаючи взаємні попередження про надзвичайні ситуації та надання допомоги, бере участь у розробці проектів міжнародних договорів з питань, що належать до компетенції ДСНС України;

- здійснює фінансування заходів щодо попередження і ліквідації надзвичайних ситуацій у межах виділених бюджетних асигнувань, вносить пропозиції Уряду України про використання наявних у складі державних та мобілізаційних резервів запасів матеріально-технічних, продовольчих, медичних та інших ресурсів, а також коштів загальнодержавного фонду фінансування витрат, пов'язаних зі стихійними лихами, аваріями та катастрофами, на ліквідацію надзвичайних ситуацій та відшкодування шкоди;

- бере участь у розробленні та здійсненні заходів щодо запобігання надзвичайним ситуаціям природного та техногенного характеру, забезпечення умов для їх ліквідації, підвищення стійкості роботи організацій [34; 145];

- здійснює в установленому порядку ліцензування відповідних видів діяльності;

- забезпечує здійснення державного нагляду за дотриманням вимог пожежної безпеки міністерствами, іншими органами державного управління, іншими організаціями, посадовими особами та громадянами;

- організовує і проводить пожежно-технічні обстеження організацій, видає розпорядження, попередження, висновки і рекомендації щодо усунення порушень;

- призупиняє повністю або частково роботу організацій, будівництво, реконструкцію, технічне переозброєння, ремонт об'єктів і проведення інших робіт при порушенні протипожежних вимог або невиконанні відповідних приписів;

- забороняє експлуатацію будівель, споруд, приміщень, машин, приладів, устаткування й інших пристроїв, що функціонують з порушенням вимог пожежної безпеки, а також випуск, реалізацію та використання продукції, що не відповідає протипожежним вимогам;

- відповідно до законодавства проводить дізнання та здійснює провадження у справах про адміністративні правопорушення;

- здійснює в установленому порядку погодження проектів на будівництво об'єктів, по яким відсутні протипожежні вимоги;

- організовує ліквідацію аварій, катастроф, стихійних та інших лих, авіаційне виявлення пожеж у лісах та на торфовищах, гасіння пожеж, рятування людей, координує роботу органів державного управління, місцевих виконавчих і розпорядчих органів, інших організацій щодо запобігання та ліквідації надзвичайних ситуацій;

- забезпечує постійну бойову готовність сил і засобів органів і підрозділів з надзвичайних ситуацій до дій при виникненні надзвичайних ситуацій, організовує несення гарнізонної та вартової служби у пожежних аварійно-рятувальних підрозділах;

- розробляє, затверджує і (або) погоджує в установленому законодавством України порядку нормативні правові акти, стандарти, норми і правила у сфері захисту населення і територій від надзвичайних ситуацій, забезпечення пожежної, промислової та радіаційної безпеки, цивільної оборони;

- призупиняє дію нормативних документів системи протипожежного нормування і стандартизації, що суперечать вимогам пожежної безпеки;

- інформує органи державного управління, місцеві виконавчі і розпорядчі органи, інші організації, населення з питань запобігання та ліквідації надзвичайних ситуацій, забезпечення пожежної, промислової та радіаційної безпеки, цивільної оборони;

- взаємодіє із засобами масової інформації;

- бере участь у розробці та реалізації єдиної державної науково-технічної політики у сфері запобігання та ліквідації надзвичайних ситуацій та пожеж;

- координує проведення наукових досліджень та державних випробувань у сфері запобігання та ліквідації надзвичайних ситуацій, забезпечення пожежної, промислової та радіаційної безпеки, цивільної оборони, бере участь в проведенні даних досліджень та випробувань;

- проводить відповідно до своєї компетенції сертифікацію у сфері запобігання та ліквідації надзвичайних ситуацій, пожежної, промислової та радіаційної безпеки, цивільної оборони [177; 180; 184];

- узагальнює та впроваджує в практику передовий досвід зарубіжних пожежних та аварійно-рятувальних служб;

- здійснює керівництво діяльністю органів та підрозділів з надзвичайних ситуацій, надає їм консультаційну, методичну та наукову допомогу, здійснює їх інспектування;

- організує інформаційне забезпечення діяльності органів та підрозділів з надзвичайних ситуацій, формує загальнодержавні довідково-інформаційні фонди;

- забезпечує оперативне управління силами та засобами органів та підрозділів з надзвичайних ситуацій при проведенні загальнодержавних та міжрегіональних заходів щодо запобігання та ліквідації надзвичайних ситуацій та пожеж;

- забезпечує ефективну кадрову політику, добір, розстановку та виховання кадрів органів та підрозділів з надзвичайних ситуацій, підвищення їх кваліфікації та професійної підготовки;

- розробляє загальні вимоги, умови та порядок служби в органах і підрозділах з надзвичайних ситуацій, стандартні умови їх штатного розпису, а також вимоги до кваліфікації працівників до цих органів та підрозділів;

- забезпечує правовий та соціальний захист працівників та пенсіонерів органів та підрозділів з надзвичайних ситуацій, членів їх сімей, розробляє для них комплекс профілактичних, лікувальних, оздоровчих та реабілітаційних заходів;

- розглядає в установленому порядку звернення громадян з питань, що належать до компетенції ДСНС України;

- організовує і контролює фінансово-господарську діяльність органів і підрозділів з надзвичайних ситуацій;

- визначає порядок матеріально-технічного та речового постачання органів та підрозділів з надзвичайних ситуацій;

- виконує функції державного замовника на пожежну та аварійно-рятувальну техніку, спорядження та озброєння, організовує їх розробку та виробництво в Україні;

- надає платні послуги юридичним та фізичним особам у встановленому порядку;

- виконує інші функції, передбачені законодавством України [102; 160].

Керівництво системою органів і підрозділів з надзвичайних ситуацій здійснює Міністр внутрішніх справ (далі − Міністр) через Кабінет Міністрів України, який несе персональну відповідальність за виконання завдань, покладених на органи і підрозділи з надзвичайних ситуацій.

Зокрема, у контексті функціонування Державної служби України з надзвичайних ситуацій України Міністр внутрішніх справ:

- затверджує структуру та штатний розпис органів та підрозділів з надзвичайних ситуацій у межах чисельності, встановленої Президентом України, а також коштів на їх утримання, затверджує структуру та штатний розпис підпорядкованих організацій;

- перерозподіляє між органами та підрозділами з надзвичайних ситуацій, виходячи з оперативної обстановки та важливості завдань, що виконуються, штатну чисельність працівників цих органів та підрозділів;

- притягає згідно із законодавством для ліквідації надзвичайних ситуацій та пожеж людські та матеріально-технічні ресурси організацій;

- приймає рішення відповідно до законодавства щодо формування, реорганізації та припинення діяльності підпорядкованих органів та підрозділів з надзвичайних ситуацій, а також підпорядкованих організацій, затверджує їх положення, статути, а також положення про структурні підрозділи ДСНС України;

- інформує в установленому порядку Президента України та Уряд України про діяльність у сфері запобігання та ліквідації надзвичайних ситуацій, забезпечення пожежної, промислової та радіаційної безпеки, цивільної оборони, а також надає інформацію з даних питань засобам масової інформації;

- у межах своєї компетенції вносить у встановленому порядку до Кабінету Міністрів України проекти нормативних правових актів, а також пропозиції про скасування нормативних правових актів інших органів державного управління, що суперечать законодавчим актам України і рішення Уряду України;

- визначає порядок прийому громадян в органах та підрозділах з надзвичайних ситуацій [118; 148];

- встановлює єдині вимоги до забезпечення режиму секретності, організації діловодства в органах і підрозділах з надзвичайних ситуацій;

- укладає в установленому порядку міжнародні договори;

- визначає та затверджує порядок виплати грошового забезпечення особам рядового та вищого складу органів та підрозділів з надзвичайних ситуацій;

- розподіляє в установленому порядку кошти, що виділяються загальнодержавним бюджетом на утримання органів і підрозділів з надзвичайних ситуацій;

- встановлює відповідно до законодавства України тарифні коефіцієнти для визначення посадових окладів та інших основних видів фінансового забезпечення осіб рядового та вищого складу органів та підрозділів з надзвичайних ситуацій;

- встановлює відповідно до законодавства України розміри та порядок надання матеріальної допомоги працівникам та пенсіонерам органів та підрозділів з надзвичайних ситуацій;

- розподіляє обов'язки між своїми заступниками по керівництву напрямками діяльності ДСНС України;

- у встановленому порядку призначає на посаду та звільняє з посади працівників органів та підрозділів з надзвичайних ситуацій, усуває їх від виконання службових обов'язків;

- вносить пропозиції Президенту України про присвоєння спеціальних звань вищого навчального складу, старшим працівникам органів та підрозділів з надзвичайних ситуацій;

- вносить у встановленому порядку подання щодо відзначення державними нагородами працівників органів та підрозділів з надзвичайних ситуацій, заохочує їх та накладає на них штрафні санкції відповідно до законодавства України;

- нагороджує грамотами, подяками ДСНС України, вносить в установленому порядку пропозиції щодо нагрудних знаків ДСНС України;

- у встановленому порядку присвоює перше та наступне спеціальне звання працівникам органів та підрозділів з надзвичайних ситуацій, скорочує та відновлює їх у спеціальних званнях, позбавляє спеціальних звань;

- організовує та контролює службово-бойову та морально-психологічну підготовку працівників органів та підрозділів з надзвичайних ситуацій;

- діє без довіреності від імені ДСНС України, представляє його інтереси в установленому порядку розпоряджається державним майном, що знаходиться на балансі ДСНС України;

- організовує і контролює тилове забезпечення, затверджує відповідно до законодавства України норми автотранспорту, засобів зв'язку, аварійно-рятувальної та іншої спеціальної техніки, озброєння, інших матеріально-технічних засобів, необхідних для оснащення органів і підрозділів з надзвичайних ситуацій;

- визначає відповідно до законодавства України порядок та умови списання основних засобів з балансу органів та підрозділів з надзвичайних ситуацій;

- делегує за необхідності частину наданих йому повноважень заступникам Міністра, керівникам органів і підрозділів з надзвичайних ситуацій шляхом видання відповідних наказів;

- здійснює інші повноваження відповідно до законодавства України.

Територіальні органи та підпорядковані підрозділи ДСНС України призначені для виконання завдань та функцій у сфері:

- цивільного захисту;

- захисту населення та територій від надзвичайних ситуацій природного та техногенного характеру;

- забезпечення пожежної безпеки та безпеки людей на водних об'єктах на територіях регіонів України [94; 141; 248].

Основними завданнями територіальних органів та підпорядкованих підрозділів ДСНС України є такі:

- здійснення в межах своєї компетенції державної політики у сфері цивільного захисту, захисту населення та територій від надзвичайних ситуацій, забезпечення пожежної безпеки та безпеки людей на водних об'єктах;

- здійснення контрольних функцій у сфері цивільного захисту, захисту населення і територій від надзвичайних ситуацій, забезпечення пожежної безпеки та безпеки людей на водних об'єктах;

- здійснення в межах своєї компетенції діяльності з організації та ведення цивільного захисту, захисту населення та територій від надзвичайних ситуацій та пожеж, забезпечення безпеки людей на водних об'єктах, а також екстреного реагування при надзвичайних ситуаціях загальнодержавного рівня [166; 213].

Територіальні органи та підпорядковані підрозділи ДСНС України здійснюють такі основні функції:

- організовує прогнозування надзвичайних ситуацій у системі моніторингу та прогнозування надзвичайних ситуацій, роботу з запобігання та ліквідації надзвичайних ситуацій загальнодержавного рівня, рятування та життєзабезпечення людей у надзвичайних ситуаціях, забезпечує підтримку ліквідації надзвичайних ситуацій регіонального та міжмуніципального характеру, а також своєчасні управлінські рішення при переході цих надзвичайних ситуацій на національний рівень;

- організовує в установленому порядку роботу з запобігання пожежам, а також контроль за організацією гасіння пожеж на об'єктах, критично важливих для національної безпеки країни, інших особливо важливих пожежонебезпечних об'єктах, особливо цінних об'єктах культурної спадщини України, при проведенні заходів загальнодержавного рівня з масовим скупченням людей, перелік яких затверджується Урядом України;

- організовує в установленому порядку пошук та рятування людей на водних об'єктах;

- організовує в установленому порядку разом із зацікавленими органами виконавчої влади України формування та доставку вантажів гуманітарної допомоги населенню, постраждалому внаслідок надзвичайних ситуацій, у тому числі населенню зарубіжних країн;

- організовує облік атестованих аварійно-рятувальних служб, пожежників, пожежно-рятувальних, пошуково-рятувальних та аварійно- рятувальних формувань, громадських об'єднань, що мають статутні завдання з проведення аварійно-рятувальних робіт і гасіння пожеж;

- організовує фінансове забезпечення головних управлінь ДСНС України та підпорядкованих підрозділів, підготовку і затвердження кошторисів доходів і видатків по бюджетних і позабюджетних коштах, а також оперативний, бухгалтерський і статистичний облік фінансово-господарської та іншої діяльності, ревізійну роботу;

- організовує взаємодію сил і засобів, що беруть участь у аварійно-рятувальних операціях у надзвичайних ситуаціях та гасінні пожеж;

- організовує проведення атестації аварійно-рятувальних служб, пожежно-рятувальних, аварійно-рятувальних формувань і рятувальників державних органів виконавчої влади, регіональних органів виконавчої влади, органів місцевого самоврядування й організацій [47; 104; 114];

- здійснює контроль за створенням та забезпеченням готовності сил і засобів цивільного захисту в регіонах України, муніципальних утвореннях і організаціях;

- здійснює поточне та перспективне планування мобілізаційного розгортання з'єднань та військових частин військ цивільної оборони та військових частин протипожежної служби у воєнний час;

- здійснює контроль за створенням, збереженням та використанням страхового фонду документації для об'єктів високого ризику та об'єктів систем життєзабезпечення населення;

- здійснює у межах своєї компетенції в установленому порядку заходи щодо запобігання, виявлення та припинення терористичної діяльності на об'єктах ДСНС України, а також ліквідації наслідків терористичних актів;

- бере участь у межах своєї компетенції в інформуванні населення за допомогою засобів масової інформації та інших каналів про прогнозовані та виникаючі надзвичайні ситуації та пожежі, заходи щодо забезпечення безпеки населення та територій, прийоми та методи захисту, а також здійснює пропаганду у сфері цивільного захисту, захисту населення та територій від надзвичайних ситуацій, забезпечення пожежної безпеки та безпеки людей на водних об'єктах;

- бере участь в управлінні єдиною державною системою запобігання та ліквідації надзвичайних ситуацій у межах своєї компетенції;

- бере участь у підготовці пропозицій щодо питань надання державної допомоги населенню та територіям, які постраждали від надзвичайних ситуацій регіонального, національного та транскордонного характеру;

- бере участь у координації діяльності всіх видів пожежної охорони [150; 216].

Для реалізації завдань, покладених на територіальні органи та підпорядковані підрозділи ДСНС України, вони наділені наступними основними повноваженнями:

- здійснює підготовку проектів нормативно-правових актів та інших документів з питань цивільного захисту, захисту населення і територій від надзвичайних ситуацій, забезпечення пожежної безпеки, безпеки людей на водних об'єктах;

- здійснює в установленому порядку контроль за організацією діяльності головними управліннями ДСНС України за регіонами України щодо дотримання встановлених вимог законодавства у сфері цивільного захисту, захисту населення та територій від надзвичайних ситуацій, забезпечення пожежної безпеки та безпеки людей на водних об'єктах місцевими органами влади, організаціями, а також посадовими особами, громадянами України, іноземними громадянами та особами без громадянства;

- здійснює керівництво підлеглими підрозділами, а також регіональними головними управліннями ДСНС України з питань бойової та мобілізаційної готовності, проходження військової служби, матеріально-технічного та фінансового забезпечення;

- здійснює в установленому порядку функції з управління закріпленим державним майном;

- здійснює повноваження розподільника коштів державного бюджету стосовно регіональних головних управлінь ДСНС України та підпорядкованих підрозділів відповідно до законодавчих та іншими нормативно-правовими актів України;

- створює координаційно-дорадчі органи (комісії, групи) на представницькій основі, а також інші колегіальні органи для обговорення актуальних питань діяльності регіонального центру ДСНС України та ін.

Загалом 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 [32; 169].

Територіальні органи та підпорядковані підрозділи ДСНС України відновлюють норму керованості. Їх формування, очевидно, також є актом

вертикальної деконцентрації повноважень президентської влади, наближення державного апарату управління до регіонів України, до населення.

Одночасно активізується процес деконцентрації повноважень державної виконавчої влади через перебудову й оптимізацію системи територіальних структур державних органів виконавчої влади, а також формування їх регіональних структур.

На регіональному рівні також є можливість підвищити ефективність державної політики у сфері громадської безпеки та захисту критичних об'єктів у надзвичайних ситуаціях та терористичних актах. Оптимізація територіального управління не може бути здійснена одночасно. Це розгорнутий у часі процес послідовного реформування державної системи. 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 та муніципальної адміністрації [169].

У зв'язку з цим принципово важливо зазначити ще одну обставину. Найважливішим завданням повноважних представників є і створення ефективних механізмів взаємодії держави і суспільства, «зворотного зв'язку» між Президентом України і жителями міст і населених пунктів.

Особливу увагу потрібно приділити критичній інфраструктурі, що стосується кібербезпеки.

Сучасні інформаційно-комунікаційні технології можуть бути використані для вчинення терористичних актів. Найпривабливішими мішенями є об'єкти критичної інфраструктури [28; 203].

Об'єкти національної інфраструктури завжди розглядалися противником в якості потенційних мішеней. Серед них особливо виділяються об'єкти, часткова деградація або повна втрата функціональності яких здатна впливати на стан

національної безпеки і приводити до надзвичайних ситуацій певного рівня і масштабу – об'єкти критичної інфраструктури.

Сьогодні головним викликом для операторів найважливіших об'єктів інфраструктури стають кібератаки, і в першу чергу для операторів найважливіших об'єктів енергетичної інфраструктури [109; 203].

Існують різні визначення кібертероризму. Часто спроби визначити цей термін концентруються на наслідки – 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.

Але можна визначити кібертероризм як тероризм, пов'язаний з кіберпростором, а кібертеракти як терористичні акти, спрямовані на кіберінфраструктуру, зокрема, на системи управління найважливішими об'єктами [28; 39].

Міністерство національної безпеки США визначає найважливіші об'єкти 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.

Директива NIS Європарламенту і Єврокомісії від 07.12.2015 з «Мережевої та інформаційної безпеки», якою встановлюються вимоги щодо управління ризиками, а також за поданням даних про інциденти на об'єкти критичної інфраструктури, виокремлює такі сектори критичної інфраструктури:

- енергетика: електрика, природний газ і нафта;
- кредитно-фінансові заклади і біржі;
- транспорт: повітряний, морський, залізничний;

- охорона здоров'я;

- інформаційні і комунікаційні технології (ІКТ);

- органи державного управління.

Для підтримки роботи найважливіших об'єктів інфраструктури виключно важливо зберігати стабільність в енергетичному секторі та інших найважливіших інфраструктурних галузях (наприклад, необхідно постійно підтримувати стабільну роботу електромереж, оскільки в разі збоїв наслідки можуть проявитися в лічені секунди) [15; 22; 129].

Розлади в системі електропостачання часто мають серйозні наслідки каскадного ефекту, неминуче зачіпаючи інші сектори та їх інфраструктуру. В цьому відношенні трансформаторним підстанціям і високовольтним лініям електропередачі часто надається більше значення, ніж електростанціям, оскільки розлади в роботі електростанції зазвичай можна компенсувати, в той час як аварію мережі або аварію на критичних ділянках мережі компенсувати неможливо. У той же час, мережі передачі енергії розподілені на великій території, є об'єктами енергетичної мережі, що важко захищаються.

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 [132; 148].

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.

94,3% відсотка світового енерговиробництва припадає на неядерні енергоносії. Тому об'єкти без ядерної енергетичної інфраструктури являють собою привабливу, хоча і не завжди вразливу ціль для всякого роду диверсій і атак, як зазначається в «Керівництві по передовій практиці захисту найважливіших об'єктів неядерної енергетичної інфраструктури від терористичних актів у зв'язку з погрозами, які виходять від кіберпростору» (ОБСЄ – 2013) [131; 200].

Превентивні та антикризові заходи управління, що застосовуються для захисту найважливіших об'єктів критичної енергетичної інфраструктури, повинні бути узгоджені на міжнародному рівні. У деяких країнах уряди розробляють спеціальні галузеві плани. У Сполучених Штатах спеціальні галузеві плани розроблені для кожного сектору, включаючи енергетичний і сектор комунікацій.

Прийнята до кібератак на Прикарпаття обленерго, Київобленерго і Чернівціобленерго «Стратегія Національної безпеки України» (затверджена 26 травня 2015 року) 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 [41; 57; 235].

Але в «Концепції розвитку сектора безпеки і оборони України» (затвердженій 14 березня 2016 року) об'єкти енергетики у зв'язку з розглядаються як можлива мета атак. Зокрема, в цьому документі йдеться про

кіберзагрози «автоматизованим системам державного та військового управління, об'єктам критичної інформаційної інфраструктури».

Висновки до другого розділу

1. Проаналізовано організаційно-правові основи державного управління захистом критичної інфраструктури у кризових ситуаціях у США та країнах Західної Європи, зокрема, виділено наступні основні риси цієї діяльності: системи управління з дій у кризових ситуаціях мають державний статус; діяльність щодо запобігання та ліквідації кризових ситуацій є важливою соціальною функцією кожної держави і реалізується більшістю державних установ; право запроваджувати особливий режим діяльності органів управління та населення в зоні стихійного лиха надається не тільки главі держави, але й главам суб'єктів держави (наприклад, губернаторам штатів у США); фінансування діяльності щодо захисту критичної інфраструктури в кризових ситуаціях здійснюється переважно по лінії реалізації державних програм; акценти в правовому регулюванні ризику все більше зміщуються у бік превентивних заходів.

2. Зазначено, що деякі країни не мають спеціального регулятора у сфері кібербезпеки критичної інфраструктури, але натомість наділяють офіційне представництво широкими повноваженнями з підтримки безпеки в національному кіберпросторі.

Підкреслено, що інформований вибір стратегії управління кібербезпекою критичної інфраструктури можливий лише для тих держав, які знаходяться в самому початку цього шляху. Згідно з даними Міжнародного союзу електрозв’язку, офіційний департамент із захисту критичної інфраструктури так чи інакше працює в більшості країн світу. Цей орган через відсутність

державного регулятора також може офіційно чи неофіційно діяти також у ролі відповідального відомства за всі аспекти національної кібербезпеки.

3. Відмічено, що в сучасний період перед державним управлінням, зокрема, стосовно забезпечення безпеки критичної інфраструктури об’єктивно стоять наступні цілі: формування нових інститутів державної влади та оптимізація діяльності існуючої системи виконавчої влади (адміністративна реформа); розгортання та зміцнення суспільних інститутів, які забезпечують стійку демократію суспільства та держави; створення та впровадження в життя соціальних та адміністративно-правових регуляторів, які гарантують конституційно проголошений набір прав, свобод та обов'язків громадян України; формування та практична реалізація державної політики, спрямованої на забезпечення громадської безпеки та захисту об’єктів критичної інфраструктури; забезпечення внутрішньої і зовнішньої безпеки регіонів України та сприятливих мирних умов для їх життєдіяльності; досягнення гармонійного, збалансованого та взаємопов’язаного розвитку регіонів у співпраці з центром на основі поглиблення процесів формування та функціонування всеукраїнського ринку.

4. Показано, що аварії в системах забезпечення займали у 2018 році найбільший відсоток від загальної кількості надзвичайних ситуацій на різнохарактерних об'єктах критичної інфраструктури України - 83,3%.

Що стосується 2019 року, то в цей період 57,1% склали аварії в електро-енергосистемах. Відповідно, вони займають перше місце в надзвичайних ситуаціях на різнохарактерних об'єктах критичної інфраструктури України.

5. Підкреслено, що в Україні комплексне створення державної системи захисту критичної інфраструктури на період з 2017 по 2027 роки. Ця система визначає створення якісно нового рівня державного управління в цій галузі:

- розробка сучасних інноваційних підходів до управління ризиками безпеки критичної інфраструктури;

- оптимізоване застосування наявних ресурсів, гнучке і швидке реагування на інциденти і кризи.

Матеріали даного розділу оприлюднені в наступних публікаціях автора: [67; 70; 71].

РОЗДІЛ 3. ШЛЯХИ УДОСКОНАЛЕННЯ ДЕРЖАВНОГО УПРАВЛІННЯ ЗАБЕЗПЕЧЕННЯМ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

3.1. Державні механізми забезпечення безпеки та підвищення ефективності захисту критичної інфраструктури

Поняття «захист» може набувати різного значення. Найбільш популярне значення цього терміну означає турботу про запобігання небезпеки, різного шкідливого впливу середовища на соціальний суб'єкт чи матеріальний об'єкт, які можуть поставити під загрозу його безпеку. Захист може розглядатися в двох його основних значеннях:

- захист як діяльність, метою якої є забезпечення безпеки об'єктів захисту;

- захист як засіб або ж системне упорядкування коштів для забезпечення безпеки об'єктів захисту.

Захист критичної інфраструктури можна визначити як сукупність заходів, які плануються та здійснюються з метою:

- пізнавати та захищати ці критичні сектори інфраструктури держави з точки зору збереження їх безпеки, функціональності, економічної та суспільної стабільності, причому необхідно рівноцінно оцінювати як державну, так і приватну сферу;

- забезпечити функціональність системи раннього попередження прояву кризових ситуацій та захист тієї інфраструктури, яка має важливе значення для вирішення кризових ситуацій [22; 66].

У цьому контексті ми говоримо передусім про сектори критичної інфраструктури, які є важливими з точки зору:

- забезпечення належного функціонування уряду, органів державного управління та місцевого самоврядування, переважно у сфері безпеки та

забезпечення та функціонування основних (життєво важливих) товарів та служб;

- функціональності державної та приватної сфери їх забезпеченням належного руху економіки та функціонування суспільних служб;

- забезпечення внутрішнього порядку, громадської стабільності та безпеки громадян.

Захист критичної інфраструктури буде виконуватися як результат аналітичного процесу, зміст якого складається з:

- ідентифікації областей та секторів критичної інфраструктури на національному, регіональному та місцевому рівні;

- ідентифікації релевантних ризиків для секторів критичної інфраструктури;

- аналізу вразливості певних секторів критичної інфраструктури;

- оцінки ризиків порушення або знищення секторів критичної інфраструктури;

- вжиття відповідних запобіжних заходів, зокрема, у створенні системи захисту критичної інфраструктури.

Захист критичної інфраструктури - це сукупність організаційно-технічних заходів, що забезпечують захист критично важливих секторів інфраструктури від різних загроз (терористи, диверсанти, екстремісти), як у випадку надзвичайних ситуацій чи кризових ситуацій [15; 63; 220].

Сучасні системи захисту критичної інфраструктури засновані на базі використанні різних засобів та містять такі складові частини (підсистеми):

- механічні бар'єри, огорожі, ворота, ґрати тощо.

- система контролю та управління доступом;

- система охоронної сигналізації;

- система телевізійного спостереження;

- організаційні заходи;

- служба охорони та сили реагування.

Система фізичного захисту критичної інфраструктури – це інтегрований комплекс реальних елементів, видів діяльності та процесів, які логічно та функціонально упорядковані в такий спосіб, що вона створює знаряддя для забезпечення безпеки об'єктів критичної інфраструктури в певний час та в заданому просторі. З точки зору системного підходу таку систему можна вважати синергетичною системою з цільовою поведінкою [22; 220].

При цьому бажаними функціями системи фізичного захисту є такі:

- відлякувати потенційних нападників від нападів на об'єкт, що охороняється;

- детектування порушення об'єктів, приміщень, зон, що охороняються, або детектування виникнення небезпечної обстановки на об'єкті, або його близькій околиці;

- затримка руху атакуючих;

- реакція на порушення функціонування або структури об'єктів, просторів або зон, що охороняються, з ціллю допустити підступ атакуючих до цих об'єктів, просторів чи зон, або поставити під загрозу об'єкт, його функцій або людей.

Слід зазначити зростаюче значення місцевого та територіального самоврядування України - основи для створення законодавчих та нормативно-правових документів. З її допомогою деталізуються процедури участі громадськості в прийнятті рішень про розміщення і спорудження критично важливих об'єктів.

Таким чином, громадянське суспільство стає третім, альтернативним бізнесу і державі, сектором, що забезпечує як виробництво економічних благ, так і якість життя населення, включаючи безпеку. Але традиції і правова культура долі українського суспільства у прийнятті рішень про розміщення і спорудження критично важливих небезпечних об'єктів поки не розвинені.

Норми участі громадськості, задані в загальному вигляді, реалізуються найчастіше формально. Що стосується результату обговорення, то його визначає сформований рівень соціального партнерства та суспільної злагоди, іноді − випадкові фактори.

Основною формою ухилення від процедур громадського обговорення стало приховування суспільно значущих відомостей щодо офіційної інформації та інформації прес-служби інвесторів. При цьому відсутні відомості про:

- об'єкт;

- його технічні характеристики;

- терміни будівництва;

- відповідальних (контактних) осіб;

- процедурах або порядку ознайомлення з проектом.

Крім того, не ведеться реєстрація й облік висловлених думок.

Дану діяльність пропонується розвивати шляхом застосування системного підходу, що містить такі складові:

- економічна;

- адміністративно-кримінальна (штрафи, судові розгляди);

- соціально-психологічна.

Для успішного вирішення проблеми вважається доцільним:

- сприяти впровадженню показників стану навколишнього середовища в систему оцінювання ефективності діяльності регіональних органів виконавчої влади;

- поступово впроваджувати систему технічних регламентів та привести її у відповідність із міжнародними стандартами;

- заявляти з найвищих трибун, що надзвичайні ситуації не знають політичних кордонів, вимагають довгострокової перспективної роботи і потребують участі громадянського суспільства, активної позиції людей.

В даний час функції щодо забезпечення безпеки та контролю розосереджені серед міністерств та відомств. Державна служба України з надзвичайних ситуацій повинна стати єдиним органом із забезпечення безпеки та контролю, в тому числі в інформаційній сфері критично важливих об'єктів. Наразі Державна служба України з надзвичайних ситуацій відповідає за ведення реєстру критично важливих об'єктів. Основними структурними елементами системи моніторингу, які забезпечують вирішення покладеної на неї задачі, повинні бути центри моніторингу державних органів виконавчої влади, регіональних органів виконавчої влади та органів місцевого самоврядування.

Організації, що експлуатують потенційно небезпечні об'єкти, підлягають обов'язковій оцінці готовності до запобігання та ліквідації надзвичайних ситуацій (надалі − оцінки готовності об'єктів) [41; 169; 172].

Оцінка готовності об'єктів здійснюється комісіями Державної служби України з надзвичайних ситуацій, Головними управління ДСНС України в областях та місті Києві, управліннями ДСНС України в областях, Центрами забезпечення діяльності, а також оперативно-координаційними центрами.

Проведення оцінки готовності об'єкта передбачається з періодичністю не рідше одного разу на п'ять років у вигляді самостійного заходу або із включенням у плани регулярних та позачергових перевірок організацій з питань попередження надзвичайних ситуацій. Для проведення оцінки допускається залучення спеціалізованих науково-дослідних, проектних та інших організацій, які мають відповідні ліцензії.

В нашій країні здійснюється паспортизація територій та небезпечних об'єктів. Паспортизація, безсумнівно, стала постійним веденням обліку та контролю над територією та особливо небезпечними об'єктами для запобігання та ліквідації надзвичайних ситуацій. При цьому типовий паспорт безпеки небезпечного об'єкта і території повинен враховувати таку категорію як критично важливі об'єкти.

При цьому слід зазначити наступну обставину − критично важливі об'єкти потребують насамперед запобігання надзвичайних ситуацій. І на перший план при цьому виходять заходи фізичного захисту від зовнішніх і внутрішніх впливів. Розглядаючи проблему забезпечення безпеки критично важливих об'єктів, слід мати на увазі два напрями:

- захист об'єктів від зовнішніх впливів з метою недопущення їх руйнування та аварійних ситуацій;

- захист людей та навколишнього середовища від негативних факторів, які утворюються у випадку, якщо аварія все-таки сталася.

Технічні регламенти встановлюють обов'язкові вимоги для застосування і застосування до об'єктів технічного регулювання (продукції, будівлям, будовам і спорудам, процесам виробництва, експлуатації, зберігання, перевезення, реалізації і утилізації). Необхідно виробити єдину національну нормативну базу з проблем оцінки ризику критично важливих об'єктів. Цій меті буде служити категоріювання критично важливих об'єктів.

Захищеність об'єктів критичної інфраструктури має першорядне значення для забезпечення безпеки особистості, суспільства та держави. В даний час питання захищеності цих об'єктів регулюються на підзаконному рівні. При цьому існує необхідність прийняття базового закону в цій галузі, який би визначив основні поняття, види та категорії критично важливих об'єктів, а також встановлював би вимоги щодо забезпечення безпеки окремих категорій таких об'єктів [15; 22; 82].

Загалом, слід відзначити, що Державна служба України з надзвичайних ситуацій володіє найбільш широкими можливостями щодо комплексного вирішення завдань, пов'язаних з:

- виявленням техногенної обстановки;

- аналізом і оцінкою ризику;

- підготовкою та прийняттям управлінських рішень щодо організації заходів забезпечення безпеки критично важливих об'єктів.

Єдиним органом щодо забезпечення безпеки та контролю, зокрема, в нормативно-правовому регулюванні забезпечення безпеки критично важливих об'єктів повинна стати Державна служба України з надзвичайних ситуацій.

Основним шляхом вдосконалення нормативно-правової бази для забезпечення безпеки критично важливих об'єктів є прийняття базового закону в цій галузі, який би визначив основні поняття, види та категорії критично важливих об'єктів, а також встановив би вимоги щодо забезпечення безпеки окремих категорій таких об'єктів [169].

У процесі державного управління критичною інфраструктурою також необхідно враховувати різнохарактерні залежності. Постачання основних товарів та послуг суспільству все частіше є результатом взаємодії між декількома постачальниками. Ці провайдери охоплюють всі сектори і підсектори об’єктів критичної інфраструктури, утворюючи складні взаємозв'язки. Хоча взаємозв'язок активів, систем і процесів заснований на більш ефективному управлінні ресурсами, він збільшує залежності. Вони можуть бути широко визначені як взаємозв'язок між двома продуктами або послугами, в якій один продукт або послуга потрібна для створення іншого продукту або послуги. Наприклад, постачання продуктів харчування залежать від транспорту, банківський і фінансовий сектор використовує телекомунікації для аутентифікації транзакцій, а телекомунікації залежать від розподілу електроенергії [22; 66].

Більшість основних послуг залежать від одночасного надання послуг з кількох секторів. Наприклад, охорона здоров'я не може бути реалізована за відсутності електроенергії, води та аварійних служб одночасно. Залежності можуть викликати ефекти різної інтенсивності та складатися з різних типів.

Зокрема, після терористичного нападу, об’єкти критичної інфраструктури можуть постраждати від:

- фізичних залежних об'єктів: функціонування одних об'єктів інфраструктури залежать від поставок матеріальних продуктів з інших об'єктів інфраструктури;

- кіберзалежності: функціонування одних об'єктів інфраструктури залежить від інформації, переданої через інформаційну інфраструктуру.

Важливо відзначити, що залежності підвищують рівень уразливості. Загроза стає все гострішою внаслідок широкої залежності урядових установ та приватного сектору від інформаційно-комунікаційних технологій, що збільшують вплив міжгалузевих та транснаціональних залежностей.

У зв'язку з цим слід зазначити, що сценарій, який, викликає найбільшу стурбованість у експертів, полягає в комбінованому використанні кібератаки на об’єкти критичної інфраструктури в поєднанні з фізичною атакою. Таке використання кібертероризму може призвести до посилення ефектів фізичної атаки. Прикладом цього може бути звичайна бомбова атака на будівлю в поєднанні з тимчасовою відмовою в електропостачанні або телефонному зв'язку. Підсумкове погіршення аварійного реагування, поки резервні електричні або комунікаційні системи не будуть задіяні та використані, може збільшити число жертв і громадську паніку [39; 203].

Коли уразливості ведуть до збоїв в результаті терористичної атаки, залежності можуть викликати «каскадні ефекти». Наприклад, розповсюдження токсичних речовин у ланцюжку водопостачання призводить до збоїв у системі охорони здоров'я. Для стратегій захисту об’єктів критичної інфраструктури вкрай важливо використовувати причинно-наслідковий зв'язок, що існує між взаємозв'язками об’єктів критичної інфраструктури, залежностями та вразливими, як спосіб:

- досягти достатнього рівня розуміння (від усіх зацікавлених сторін, приватного чи державного сектору);

- точок системної уразливості, що повинно бути відображено в більш точному управлінні ризиками та кризами.

При цьому завдання інтеграції концепції залежностей у процеси управління ризиками та кризами ускладнюється тим фактом, що залежності можуть змінюватися відповідно від режиму роботи даного об’єкту критичної інфраструктури. Наприклад, хоча зазвичай лікарня не залежить від дизельного палива, після збою в електричній системі вона може раптово стати залежною від подачі дизельного палива для роботи аварійного генератора. Відповідно, стратегії захисту об’єктів критичної інфраструктури повинні формувати залежності як нестатичні, а, швидше, як динамічні й мінливі відносини. При цьому має спостерігатися підвищення обізнаності про взаємозалежності через міжсекторальні мережі (засновані, наприклад, на обговоренні сценаріїв ризику), щоб стимулювати подальшу співпрацю між різними учасниками процесів [1%; 215].

Необхідно вказати на те, що не існує єдиної, заздалегідь певної інституційної моделі, яка визначає, як країни повинні захищати свої об’єкти критичної інфраструктури. Таким чином, очікується, що уряди виберуть структуру, яка найкраще відповідає їх характеристикам з точки зору:

- виникаючих загроз;

- розміру і структури економіки;

- культури суспільної політики і ситуації;

- загальної інституційної практики.

Важливо, щоб управління архітектурою захисту об’єктів критичної інфраструктури повинно враховувати основну конституційну структуру країни, тобто унітарні, централізовані та федеративні, а також децентралізовані

держави. Це особливо важливо при розподілі ролей та обов'язків між різними рівнями уряду.

Архітектура захисту об’єктів критичної інфраструктури варіюється між двома основними моделями. На одному кінці спектру державне управління об’єктами критичної інфраструктури засноване на принципах саморегулювання, стимулах та добровільному дотриманні стандартів. Так званий «добровільний підхід» підкреслює політику, спрямовану на необов’язковому керівництві. Відповідно до цієї моделі всім зацікавленим сторонам (незалежно від державного чи приватного сектору) рекомендується вносити вклад у формування та реалізацію політики захисту об’єктів критичної інфраструктури шляхом надання рекомендацій, переконань та створення загального сприйняття для досягнення спільної мети.

Зобов'язуюча сила законодавства і схем регулювання використовується слабо і лише в якості додаткового інструменту, за винятком певних секторів (таких як атомний сектор), де вони можуть відігравати домінуючу роль. На іншому кінці спектру лежить так званий «обов'язковий підхід, заснований на ідеї, що співпраця у галузі захисту об’єктів критичної інфраструктури найкращим чином досягається шляхом створення обов'язкових правових рамок, що супроводжуються заходами покарань для операторів об’єктів критичної інфраструктури, які не відповідають необхідним стандартам в рамках встановлених термінів. На практиці країни не використовують жоден з підходів у їх базових формах. Швидше вони приймають елементи обох. Їх системи можуть бути визначені лише як переважно добровільні або обов'язкові за своєю природою [22, с. 50−80].

Прикладами перших є США, Великобританія, Канада і Швейцарія. Прикладами останніх є Франція, Іспанія, Бельгія та Естонія. Країнам може бути важко визначити, яка модель краще всього відповідає їх потребам. Зокрема, коли вони вперше встановлюють політику захисту об’єктів критичної

інфраструктури, вони можуть прийняти структури і процеси, які в кінцевому підсумку виявляться неадекватними. З цієї причини країни часто створюють механізми для забезпечення того, щоб стратегії періодично піддавалися перегляду. США пропонують приклад країни, яка почала з чистої концепції добровільної участі операторів об’єктів критичної інфраструктури в цьому процесі. Незважаючи на те, що такий підхід ґрунтується на вищезазначеному принципі, з часом він все частіше стикається з необхідністю зміцнення своєї правової бази щодо захисту об’єктів критичної інфраструктури. Суть цієї ситуації полягає в тому, що країни повинні вчитися на своєму досвіді [239, с. 5–24].

Інституційні рамки захисту об’єктів критичної інфраструктури повинні, як мінімум, охоплювати наступні аспекти:

- визначити урядове агентство, яке відіграє загальну координуючу роль у формуванні та реалізації національної стратегії щодо захисту об’єктів критичної інфраструктури;

- розподіл обов'язків за конкретними секторах, як правило, окремими міністерствами на основі встановленого досвіду і предметної компетенції;

- визначити масштаби та форми взаємодії між зацікавленими урядовими установами та операторами об’єктів критичної інфраструктури.

Також слід враховувати роль державно-приватного партнерства для захисту об’єктів критичної інфраструктури. В більшості країн переважна більшість активів критичної інфраструктури перебувають у приватній власності. Крім того, приватні оператори знаходяться в авангарді інвестицій та головних зусиль у розробці нових технологій виробництва і захисту. Ці обставини в поєднанні з тим фактом, що головна відповідальність за захист активів та систем об’єктів критичної інфраструктури покладається на їх власників та операторів, що, у свою чергу, підкреслює важливість створення

ефективного державно-приватного партнерства для досягнення адекватного рівня стійкості.

При роботі з державно-приватним партнерством розробники стратегій захисту об’єктів критичної інфраструктури повинні прагнути на створення умов для їх ефективності шляхом:

- оцінки факторів успіху і стримуючих чинників;

- визначення обсягів;

- визначення форм;

- розгляд проблем і викликів [23; 82].

Зокрема, стосовно оцінки факторів успіху та стримуючих чинників державно-приватного партнерства, «Меридіанский процес», відкритий форум для обміну ідеями щодо захисту об’єктів критичної інфраструктури та співпраці між високопоставленими урядовими політиками, визначив наступні фактори, що лежать в основі ефективного державно-приватного партнерства:

- довіра: оскільки державно-приватне партнерство часто стосується проблемних суб'єктів (комерційних питань, репутації, безпеки, перерозподілу обов'язків), важливо створити атмосферу довіри, в якій всі організації будуть усвідомлювати потребу одне одного в обачності і послідовно діяти відповідно. Чіткі керівні принципи членства в оперативних правилах можуть сприяти зміцненню довіри;

- цінність: участь у державно-приватному партнерстві повинна приносити користь, інакше інтерес до участі швидко згасне;

- повага: всі організації повинні визнавати і поважати додану вартість, яку інші організації вносять до співпраці.

- кодекс поведінки: необхідно мати чіткі, конкретні та передбачувані правила, які не надають можливості для роз'єднання і запобігають будь-якому конфлікту інтересів;

- обізнаність про можливості та обмеження один одного: це запобігає конфлікту через неправильне судження про причини негативної відповіді і дозволяє оптимально окупити зусилля альянсу. Це означає, що обидві організації повинні бути інформовані про діяльність одне одного. Хороший спосіб добитися цього − працювати разом довгий час, переважно роки;

- реалістичні очікування: всі організації повинні враховувати доступність ресурсів, бюджет розвитку тощо, щоб мати можливість формувати реалістичні очікування державно-приватного партнерства.

Для визначення сфери державно-приватного партнерства не потрібно зосереджуватися на одному конкретному етапі циклу захисту об’єктів критичної інфраструктури, а необхідно охоплювати їх усі, від розробки та реалізації заходів до етапів управління ризиками та кризами [22; 60].

Переваги об'єднання ресурсів, взаємної підтримки та спільного прийняття рішень між державним сектором та приватними операторами об’єктів критичної інфраструктури поширюються на такі сфери, як:

- оцінка безпеки;

- огляд заходів безпеки;

- визначення критично важливих активів і процесів;

- розробка планів дій у надзвичайних ситуаціях;

- навчання реагуванню на інциденти тощо.

Обмін інформацією є ключовим (хоча і не виключним) аспектом державно-приватного партнерства і ставить конкретні завдання, наприклад, стосовно захисту даних.

Найбільш прийнятна форма даного партнерства залежить від безлічі факторів, зокрема, таких:

- переслідувані цілі;

- число зацікавлених сторін, які будуть залучені, і від того очікується, що партнерство вирішить стратегічні або операційні питання.

Державно-приватне партнерство може приймати різнохарактерні форми від дуже неформальних форм співробітництва до більш формальних умов. Ступінь формальності часто пов'язаний з рівнем контролю, який прагнуть здійснювати органи державної влади. З іншого боку, стверджується, що державно-приватне партнерство, орієнтоване на проект, як правило, ефективніше, ніж орієнтоване на процес, оскільки перший підхід зазвичай передбачає більш чітко визначені місії, терміни та бюджети [53; 80].

Однак не надто добре розроблене державно-приватне партнерство ризикує забезпечити обмежену або нульову додану вартість для захисту об’єктів критичної інфраструктури.

Щоб гарантувати, що державно-приватні домовленості про співпрацю народжуються і продовжують залишатися актуальними і продуктивними зусиллями, країнам необхідно пам'ятати про найбільш часті причини невдач. Недоліки можуть бути пов'язані з наступними факторами:

- розривом очікувань між приватним та державним секторами;
- нестійкими моделями фінансування;
- нечітким поділом праці тощо.

Можна стверджувати, що переваги і сприйняття витрат і вигід сторін в кінцевому підсумку визначать успіх або провал партнерства. Почуття невідкладності допомагає створити зв'язок між державним і приватним секторами, сприяючи готовності до співпраці і досягненню спільного бачення, що в кінцевому підсумку дозволяє партнерству розвиватися і надалі. Довговічність партнерства залежить від взаємодії цих факторів і являє собою динамічний процес з періодами як слабких, так і сильних показників [10; 46].

Інші проблеми можуть бути пов'язані з відсутністю мотивації бізнесу інвестувати фінансові ресурси для захисту власних об’єктів критичної інфраструктури. У цьому контексті обговорюється необхідність стратегій захисту об’єктів критичної інфраструктури для визначення відповідних типів

стимулів в цьому відношенні. ОБСЄ розробила базову 8-ступеневу рекомендацію щодо того, як країни повинні максимізувати вигоди, які можуть бути отримані від державно-приватного партнерства, використовуючи спільні інтереси всіх зацікавлених сторін.

Незважаючи на те, що керівні принципи були розроблені в рамках передової практики для критично важливої енергетичної інфраструктури, вони, як видається, в цілому застосовні у всіх секторах. Нижче більш докладно розглянуто етапи зазначеної рекомендації [10; 51].

Крок 1: необхідність аналізу і визначення мотивації кожного партнера, який буде включений до партнерства з захисту критичної інфраструктури, щоб уточнити взаємні очікування і вклади.

Крок 2: визначення амбіцій та цілей партнерства щодо захисту об’єктів критичної інфраструктури на основі загальних національних цілей забезпечення безпеки об’єктів критичної інфраструктури; уточнити цілі партнерства щодо захисту об’єктів критичної інфраструктури та завдання, які необхідно виконати.

Крок 3: перевірка існуючої нормативної бази, що відноситься до кожного критично важливого сектору інфраструктури; визначення обов'язкових і самозобов’язуючих норм, правила і принципів; оцінка адекватності існуючої нормативної бази з урахуванням очікуваних ризиків та існуючих рівнів готовності; обговорення, як закрити можливі прогалини.

Крок 4: забезпечення механізмів, захисту та правової визначеності для обміну інформацією, пов'язаною із захистом об’єктів критичної інфраструктури, між усіма зацікавленими сторонами. Крім того, забезпечення механізмів для добровільних зусиль, включаючи розробку і обмін передовим досвідом, консультації та діалог для забезпечення постійного та ефективного партнерства.

Крок 5: створення інституційної структури, яка сприяє міжорганізаційній співпраці й обміну інформацією; уточнення ролі та внеску кожного партнера

(наприклад, урядових установ, власників та операторів критично важливої інфраструктури, постачальників продукції, асоціацій); визначення окремих точок контакту для кожного партнера; встановлення керівних принципів для співпраці.

Крок 6: зосередження на одному або двох критично важливих секторах інфраструктури; неухильний розвиток, спираючись на готовність всіх зацікавлених сторін до співпраці і розгляду рівнів загрози.

Крок 7: визначення критично важливих етапів, щоб розглянути, що було досягнуто, і визначення потенційних наступних кроків.

Крок 8: забезпечення постійного процесу перевірки для перегляду і оновлення партнерських відносин, щоб гарантувати постійний прогрес, співрозмірний із загальною картиною ризику і заходами безпеки, які необхідні для забезпечення оптимального рівня захисту.

Схоже, що для практичної реалізації заходів державного управління стосовно стратегічних ризиків для критичної інфраструктури повинні застосовуватися системно-правовий, політичний, інформаційний, економічний та організаційно-адміністративний механізми.

Зокрема, з арсеналу політичних заходів, перш за все, необхідно офіційно визнати на вищому рівні концепцію стратегічного управління ризиками для критичної інфраструктури як методологічну основу для вирішення завдання забезпечення сталого розвитку України [23; 55].

Що стосується системно-правового забезпечення вимагається розробка на загальнодержавному та регіональному рівнях нового та розвиток чинного законодавства, яке дозволить охопити найбільш важливі, значущі та пріоритетні з точки зору національної безпеки держави види стратегічних ризиків для критичної інфраструктури та обумовлені ними загрози.

Це потребує копіткої і ємної роботи по внесенню коректив та приведення у відповідність кримінального, кримінально-процесуального, податкового, страхового і адміністративного права.

Щодо удосконалення організаційно-адміністративних механізмів потрібно створення в рамках проведеної в державі адміністративної реформи державного компетентного органу, свого роду «стратегічного ризик-менеджера» з усім необхідним для його функціонування і повноцінною координацією інфраструктури.

Реформа органів державної влади потребуватиме залучення висококваліфікованих ризик-менеджерів в структурах управління на загальнодержавному, регіональному і місцевому рівнях [40; 215].

Важливу роль у справі становлення організаційних важелів стратегічного управління ризиками для критичної інфраструктури гратимуть:

- вдосконалення державних систем нагляду та контролю;

- оптимальний розподіл виконавчих та контрольних функцій між рівнями державного та муніципального управління;

- оптимізація діяльності всіх органів державної влади, які беруть участь у процесі управління критичною інфраструктурою.

Обмін інформацією повинен координуватися компетентним органом, починаючи з введення складу та показників стратегічних ризиків для критичної інфраструктури, оцінки очікуваної шкоди від їх реалізації, до їх подання органам управління, засобам масової інформації та громадськості в зручному та зрозумілому вигляді.

У цілому, що економічний механізм зниження стратегічних ризиків для критичної інфраструктури повинен включати як пряме регулювання на основі цільових витрат державних бюджетів, так і непряме економічне регулювання за рахунок вдосконалення податкового та кредитного механізмів щодо зниження податкового навантаження [18; 36].

Усі зазначені механізми можуть бути об’єднанні у комплексний механізм управління забезпеченням безпеки критичної інфраструктури (рис. 3.2).

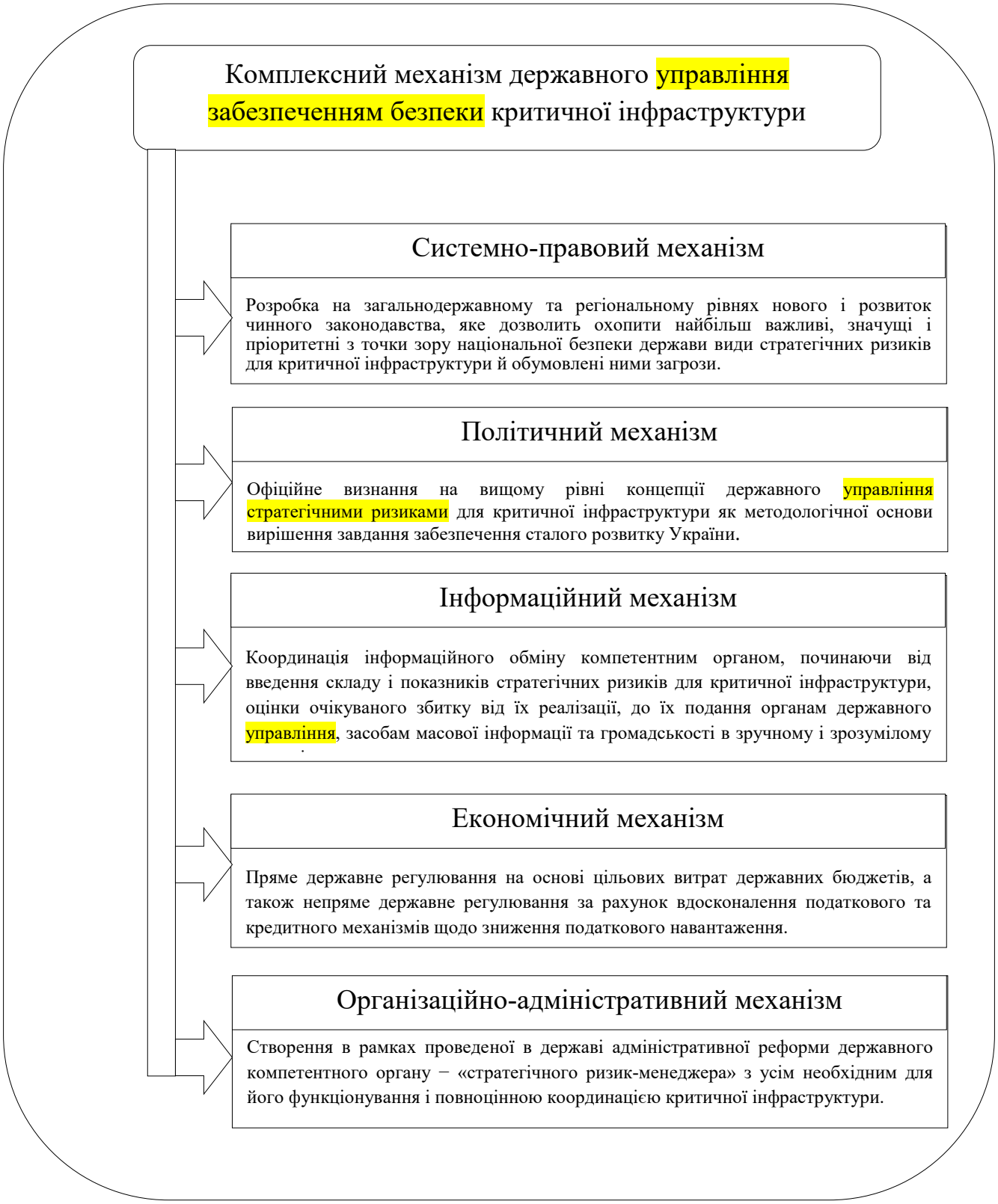

Рис. 3.1. Комплексний механізм державного управління забезпеченням безпеки критичної інфраструктури в Україні

Джерело: авторська розробка

Для практичного здійснення комплексу заходів щодо управління стратегічними ризиками для критичної інфраструктури необхідно спиратися на всю вертикаль державної влади, яка будується в державі, під координацією незалежного органу державного управління [10; 20; 53].

3.2. Розвиток системи державного управління захистом критичної інфраструктури

Зважаючи на зазначене вище, видається, що в найбільш загальній формі система державного управління щодо захисту критичної інфраструктури повинна включати два рівні прийняття рішень:

- загальнодержавний;

- регіональний, а також відповідні механізми: політичні, правові, інституційні, адміністративні, економічні, науково-технічні та ін.

Для кожного з рівнів слід визначити відповідні повноваження та визначити ступінь відповідальності за прийняті рішення: на загальнодержавному − щодо управління зовнішніми та внутрішніми стратегічними ризиками для критичної інфраструктури, регіональними - внутрішніми ризиками для критичної інфраструктури [22; 55].

Державне управління протидією стратегічним ризикам та загрозам критичній інфраструктури є пріоритетним впровадженням здійснення системного комплексу організаційно-технічних, фінансових та інших заходів, в першу чергу попереджувального характеру, які вживаються на основі експертно-аналітичних методів вирішення ряду взаємопов'язаних завдань щодо:

- ідентифікації;

- оцінки часткових та інтегральних стратегічних загроз критичній інфраструктурі;

- ранжування та вибору пріоритетних стратегічних ризиків для критичної інфраструктури;

- визначення методів по зменшенню впливу на стратегічні ризики для критичної інфраструктури до прийнятного та подання пропозицій для прийняття рішень на відповідному рівні.

Слід підкреслити, що ефективне управління стратегічними ризиками для критичної інфраструктури неможливе без формування загальної культури безпеки на всіх рівнях соціальної структури суспільства, і, перш за все, це стосується тих, хто приймає стратегічні державні рішення. По суті справи, це завдання формування національного менталітету, в якому ризик має стати світоглядною, ціннісною категорією [36; 70].

Існуюча класифікація ризиків і загроз критичній інфраструктурі дозволяє суспільству більш ефективно використовувати різні інструменти, наявні в розпорядженні, та якими можливо забезпечити запобігання чи подолання надзвичайних подій.

Насамперед, можливо:

- створити систему юридичних актів і норм;

- створити і навчити виконавчі служби;

- створити матеріальні і фінансові резерви;

- підвищити рівень освіти популяції;

- створити професійне матеріально-технічне забезпечення;

- застосовувати відповідні структури управління, які забезпечать раціональне та кваліфіковане планування і вирішення виникаючих ситуацій;

- створити контрольні механізми.

У деяких країнах зазначені категорії позначають різними кольорами, при цьому послідовність кольорів: жовтий, помаранчевий і червоний. Таке позначення є основою системи попередження й оповіщення населення у разі необхідності.

Кінцевим результатом підготовки є стан, в якому:

- кожен громадянин здатний подолати аварійні ситуації нескладної категорії завдяки своєму вихованню і підготовці;

- у державі існує система аварійних та рятувальних служб для забезпечення подолання надзвичайних подій вищих категорій;

- у державі існує система кризового управління для подолання надзвичайних ситуацій найвищої категорії.

Всі такі події можуть значним чином завдати шкоди існуючій спільноті або знищити джерела, необхідні для виживання. Єдиною можливістю, наявною в розпорядженні спільноти, є бездоганна підготовка з метою виключення остаточних збитків [32; 241].

При цьому мінімізацію збитків можна здійснювати декількома способами, які взаємно доповнюються, і, як правило, насправді реалізуються всі.

Принципове значення має рішення про те, який спосіб буде мажоритарними, а який, навпаки, − тільки додатковим. Теоретично є можливість обрати такі шляхи.

1. Активної превенції:

- мінімізація можливостей виникнення факторів, які завдають шкоди;

- створення системи реакції на події;

- моніторинг.

2. Пасивна превенція:

- підвищення стійкості елементів системи, що перебувають під загрозою;

- створення резервів;

- розробка регулюючих заходів з метою економії резервів при їх нестачі.

При цьому мінімізація можливостей виникнення факторів, що завдають шкоди критичній інфраструктурі, означає, перш за все, послідовний та системний пошук ризиків, пов'язаних із можливістю виникнення події, що

завдає шкоди майну, життю та здоров'ю населення та навколишньому середовищі.

При цьому основою аналізу ризиків для об’єктів критичної інфраструктури є пошук та класифікація можливих надзвичайних ситуацій та подальше впровадження таких заходів, які допоможуть запобігти або принаймні мінімізують ймовірність їх виникнення.

У загальному розумінні під аналізом ризику зазвичай розуміється використання наявної в розпорядженні інформації для оцінки ризику для осіб, організацій, суспільства, майна або навколишнього середовища, які йдуть із загрози [83; 215].

Аналіз ризиків, найчастіше, складається з таких компонентів:

- дефініції рамок і можливостей загрози (небезпеки);
- прогнозу ймовірності загрози;
- оцінки вразливості елементів, що знаходяться під загрозою;
- ідентифікації наслідків і прогнозу ризику.

Як і інші аналізи, так і аналіз ризиків в першу чергу поділяє систему і джерела ризику на його окремі складові, які потім досліджує.

Кваліативний аналіз застосовує словесну оцінку або відносну цифрову оцінку для опису розмірів можливої шкоди і ймовірності, з якою вона може настати.

Квантитативний аналіз ризиків заснований на оцінці ймовірності загрози, уразливості і можливих наслідків у цифрах.

Аналіз можливого виникнення надзвичайних подій є вихідною точкою, перш за все, у сфері аварійного та кризового планування. У рамках цього аналізу, найчастіше, ідентифікується місце можливого виникнення і його ймовірність; розмір можливої загрози в залежності від часу та інших умов, а також передбачуваних наслідків для працівників або населення, інфраструктури, довкілля тощо.

У тому випадку, якщо надзвичайна подія вже настала, необхідно мати систему реагування. Її завданням є максимальне скорочення часу дії несприятливих чинників, а значить, − і мінімізація втрат.

Окремі держави створюють свої власні системи співробітництва суб'єктів, включених до вирішення великих подій. Принципово вони можуть бути поділені на основні складові, що будуть вирішувати всі негативні події, для яких необхідна зовнішня допомога. Сюди можна включити, наприклад, поліцію, протипожежні служби порятунку і медичні служби порятунку, а також організації, які будуть покликані згідно з актуальними потребами, обсягом і характером події. Зокрема, сюди можна включити, наприклад, гуманітарні організації, аварійні служби, різні цивільні спільноти, можливо, деякі складові армій. Дуже важливо зрозуміти, що мова йде про складові, які будуть безпосередньо усувати загрозу небезпеки або існуючу небезпеку критичній інфраструктурі.

Крім цих складових або системи їх співпраці повинна існувати система, що підтримує постраждале населення та елементи критичної інфраструктури. Ця система створюється на рівні громадського управління (державного управління та самоврядування) і включає в себе власну передачу інформації між окремими суб'єктами, оскільки тут немає можливості використання радіозв'язку чи іншого спеціалізованого зв'язку [10; 198].

Система передачі інформації повинна базуватися на стандартних засобах зв’язку, таких як телефон, електронні скриньки зв'язку, веб-сайти, засоби масової інформації або спеціалізовані засоби комунікації з громадськістю, наприклад, місцеві радіосистеми або сирени.

Останнім названим елементом активної превенції є система моніторингу актуальної ситуації. У даному випадку мова йде, насамперед, про побудову та експлуатацію електронних систем, які реєструють дані про виникнення певного

чинника та надають інформацію про перевищення попередньо встановленого рівня. До таких систем можна включити:

- системи моніторингу рівня водних потоків або проточність;
- датчики, що фіксують концентрації деяких хімічних речовин;
- температуру;
- наявність іонізуючого випромінювання.

Сьогодні мова йде про первинні елементи, що дозволяють робити дистанційне зчитування параметрів, що записуються, більш того, часто з можливістю створення центральних місць спостереження [130; 172].

Пасивною превенцією можна вважати такі заходи, які безпосередньо не впливають на небезпеку та можливі прямі збитки, але які спрямовані на суб'єкт, який перебуває під загрозою. В такому випадку це може бути як конкретна організація, так і держава або інший вид співтовариства.

Заходи, що реалізуються в цих ситуаціях, мають підвищити стійкість суб'єкта, якому загрожує небезпека. В країнах Європи для цих цілей застосовується поняття «resilience», і це один з найактуальніших трендів останніх років.

Поняття «resilience» можна розуміти як здатність системи, громади або спільноти, що знаходяться в небезпеці, протистояти, абсорбувати, адаптуватися до ситуації і відновитися від втрат із збереженням функціонування критичних структур і елементів.

При цьому основним заходом, який веде до зростання стійкості систем, особливо громадських, є створення резервів. На здатність долати негативні явища значним чином впливає доступність джерел. Якщо існує достаток таких джерел, суспільство може дозволити собі більш масивну протидію, що значно знижує наслідки великих негативних подій, без якого-небудь впливу на ймовірність їх виникнення або їх інтенсивність.

Всі держави Європи, за своїми можливостям і впевненістю, створюють систему резервів. Такі резерви можна поділити на:

- матеріальні резерви – складаються з обраної основної сировини, матеріалів, напівфабрикатів та виробів. Вони призначені для забезпечення обороноздатності держави, для усунення наслідків кризових ситуацій та захисту особливо важливих господарських інтересів держави;

- мобілізаційні резерви – складаються з обраної основної сировини, матеріалів, напівфабрикатів, продукції, автомобілів та інших матеріальних цінностей, призначених для забезпечення мобілізаційних поставок (для підтримки збройних сил збройних служб безпеки після оголошення загрози державі та введення воєнного стану);

- аварійні запаси – обрані основні матеріали та вироби, призначені для забезпечення необхідних поставок для підтримки населення, діяльності аварійних служб і протипожежних служб порятунку після оголошення кризового становища, а також в системі аварійного господарювання, які неможливо забезпечити звичайним способом і для матеріальної гуманітарної допомоги, що надається за кордон;

- запаси для гуманітарної допомоги – це обрані матеріали та вироби, призначені для безкоштовного надання фізичним особам, особливо матеріально постраждалим після оголошення кризової ситуації. При цьому крім системи запасів необхідно створювати системи, які дозволять знизити потребу в стратегічній сировині, і цим продовжити термін, на який запаси будуть достатніми.

Конкретні системи регулюючих заходів, а також областей, в яких будуть прийматися регулюючі заходи, залежать від кожної держави. Як правило, можна зіткнутися з регулюючими заходами, які забезпечують такі сфери:

- електроенергетику (постачання електроенергією);

- газове виробництво (постачання газом);

- теплогосподарство (теплопостачання);

- електронний зв'язок;

- поштові послуги;

- постачання водою;

- виробництво і дистрибуція продуктів харчування;

- транспорт (використання комунікацій і створення коридорів) [10; 53].

Найбільш критичними в цій групі є регулюючі заходи в галузі постачання електроенергією і продуктами харчування. У сфері електроенергії це характеризується технічною неможливістю створення резервів з подальшим високим ступенем залежності від їх поставки.

Всесвітньо сьогодні розповсюджена думка, що розвинені європейські та північноамериканські держави не здатні в довгостроковому горизонті витримати без електричної енергії. Цивілізація настільки просунулася, що люди вже втратили здатність обходитися без електроенергії, і не підготовлені до цього технічно. Прикладом може служити залежність від електроенергії:

- зберігання продуктів харчування;

- захист майна (електронні системи забезпечення);

- управління транспортом всіх видів, а також функціонуванням каналізаційних і водопровідних систем.

Деякі з регулюючих заходів при цьому застосовують історичні знання періодів нестачі, перш за все, після другої світової війни − наприклад, системи надання продуктів харчування за талонами. У тому випадку, якщо надзвичайна подія вже настала, необхідно мати систему реагування. Її завданням є максимальне скорочення часу дії несприятливих чинників, а значить, − і мінімізація втрат від їх поставки. Всесвітньо сьогодні приймається думку, що розвинені європейські та північноамериканські держави не здатні в довгостроковому горизонті витримати без електричної енергії. Цивілізація настільки просунулася, що люди вже втратили здатність обходитися без

електроенергії, і не підготовлені до цього технічно. Прикладом може служити залежність від електроенергії при зберіганні продуктів харчування, захисту майна (електронні системи забезпечення), в управлінні транспорту всіх видів, каналізаційних і водопровідних систем. Деякі з регулюючих заходів при цьому застосовують історичні знання періодів нестачі, перш за все, після Другої світової війни - наприклад, системи надання продуктів харчування за талонами.

Першим кроком у процесах ідентифікації об’єктів критичної інфраструктури зазвичай є прийняття всебічного визначення того, що розуміється під об’єктом критичної інфраструктури. Це корисно для створення основи, на якій будуть розроблятися подальші політичні та нормативні рамки.

Об’єкти критичної інфраструктури можуть бути визначені, зокрема, з врахуванням тієї ролі, яку вони відіграють у просуванні та захисті прав людини (наприклад, інфраструктура, яка є життєво важливою для функціонування систем надання медичної допомоги, систем аварійного обслуговування, систем водопостачання та каналізації тощо), а також з врахуванням впливу на права людини через пошкодження, порушення або руйнувань об'єктів інфраструктури (наприклад, неможливість надання адекватних або навіть життєво важливих медичних послуг; шкода навколишньому середовищу, яка може призвести до загибелі людей; вимушене переселення людей, що негативно впливає на здоров'я тощо) [15; 22; 126].

Такий підхід відповідає духу існуючих визначень. Наприклад, ЄС визначає «критично важливі об'єкти інфраструктури» як «актив, систему чи її частину, яка необхідна для підтримки життєво важливих функцій суспільства, здоров'я, безпеки, збереження, економічного чи соціального благополуччя людей», порушення або руйнування яких матиме значний вплив «в результаті недотримання цих функцій». У тому ж дусі закон «Про збройні конфлікти» надає особливий захист інфраструктури, яка необхідна для виживання цивільного населення або руйнування якої може призвести до серйозних жертв

або завдати шкоди здоров'ю та виживанню населення (Перший додатковий протокол до Женевських конвенцій, ст. 54−56, 1949 року).

Другий етап в ідентифікації об’єктів критичної інфраструктури є найбільш складним, оскільки саме тут відбувається розстановка пріоритетів. Зокрема, цей етап спрямований на виявлення секторів та підсекторів (або послуг), які розглядаються як критично важливі.

Первісний підхід міг би полягати у розгляді інших країн, які мають подібність у соціальних і географічних особливостях, а також значний рівень технічного й економічного розвитку. Ряд секторів, швидше за все, буде розглядатися як «критично важливі» у всіх країнах. Енергетичний сектор є яскравим прикладом цього. Країни залежать від постачання електроенергією для виконання майже всіх соціальних і економічних функцій, від електрозв'язку до надання життєво важливих медичних послуг.

У той же час важливо зазначити, що певний сектор або підсектор може мати вирішальне значення для однієї нації, але не для іншої. Розмір та особливості певної національної економіки цілком можуть визначити, що є критичним, а що менш критичним.

Наприклад, деякі країни можуть значною мірою залежати від індустрії туризму в отриманні доходів. Для цих країн захист індустрії туризму як критично важливої може зіграти важливу роль у забезпеченні надання основних послуг суспільству [17; 66; 73].

Крім того, той факт, що певний сектор, визначений як критично важливий, не повинен автоматично означати, що всі базові служби є критично важливими. Наприклад, в енергетичному секторі служба централізованого теплопостачання, швидше за все, не буде включена до числа критично важливих на національному рівні.

Третій крок пов'язує раніше встановлені сектори і підсектори зі списком окремих інфраструктурних активів, систем і процесів. Числа можуть значно

варіюватися від незначної кількості до кількох тисяч, залежно від розміру країн, рівня економічного розвитку тощо.

Країни розробили безліч наборів показників для визначення певних інфраструктур як критично важливих. Ці індикатори зазвичай прагнуть виміряти наслідки руйнування об'єктів інфраструктури або функціонального збою і включають вибір / комбінацію з наступного:

- географічне охоплення впливу;

- тривалість впливу;

- тяжкість потенційних наслідків з точки зору:

а) економічних наслідків (вплив на ВВП, прямі і непрямі економічні втрати, чисельність зайнятого персоналу, податкові надходження);

б) кількості жертв і масштабів евакуації населення;

в) втрати влади урядом / порушення державного управління;

г) шкоди навколишньому середовищу.

Можна при цьому використовувати різноманітні методології для ідентифікації рівня критичної важливості об’єкта [53; 146; 214].

Консорціум на чолі з TNO, голландської дослідницькою організацією, спробував схематично згрупувати зазначені вище критерії ідентифікації за трьома основними типами:

- підхід, заснований на послугах (наприклад, Швейцарія), де уряд ідентифікує критично важливі активи на основі галузевих критеріїв, що визначають порогові значення / кількісне вироблення рівня обслуговування активів, наприклад кількість доставлених мегават;

- підхід, заснований на операторі (наприклад, Франція), де завдання визначення того, які активи або послуги є критично важливими, залишається за окремими операторами критично важливих об’єктів;

- підхід, заснований на активах або гібридах (наприклад, у Великобританії), в якому використовуються елементи підходів, орієнтовані як на послуги, так на оператора.

В якості рекомендованого підходу до ідентифікації рівня критичної важливості об’єкта пропонується наступний сценарій:

1. Проаналізувати наявність об'єктів інфраструктури, що знаходиться у власності організації, яка використовується в інтересах сторонніх осіб та для організації інформаційної взаємодії систем, що не належать самій організації.

2. У разі ідентифікації відповідних об’єктів інфраструктури з'ясувати наявність в організації чітких інструкцій на рівні законодавчих актів та нормативних вимог, що покладає на організацію обов'язки щодо забезпечення інформаційної взаємодії між сторонніми системами. У разі наявності зазначених зобов'язань зробити запит власникам сторонніх систем про визнання даних систем об'єктами критичної інфраструктури. У разі позитивної відповіді організація визнається суб'єктом критичної інфраструктури [23; 82].

3. У разі наявності інфраструктури організації, яка використовується для інформаційного обміну сторонніми системами, робиться запит власникам даних систем про їх належність до суб'єктів критичної інфраструктури. У разі позитивної відповіді конкретизується використання наданої інфраструктури для організації взаємодії об’єктів критичної інфраструктури. У разі позитивного висновку організація визнається суб'єктом критичної інфраструктури.

4. Далі організація розглядає свою інфраструктуру (або її частину, безпосередньо залучену до забезпечення взаємодії об'єктів критичної інфраструктури) в якості об'єкта критичної інфраструктури.

Доцільно при цьому детальніше розглянути фактори загрози для вищезазначених об’єктів критичної інфраструктури.

Перша категорія – це загрози, які походять від стихійних явищ.

1. Екстремальні погодні умови. За даними страхових компаній шкода, заподіяна стихійними лихами, виникає здебільшого внаслідок екстремальних атмосферних явищ. Сюди відносяться такі явища, як:

- паводки (включаючи підвищення рівня ґрунтових вод);
- повені;
- затоплення;
- штормові припливи;
- сніг;
- лід;
- посухи;
- бурі. Особлива небезпека в разі паводків виникає в результаті дії вод, що підмивають дороги, мости, дамби тощо. Небезпека забруднення питної води і виникнення тим самим значного ризику для здоров'я ще більше підвищується внаслідок витоку шкідливих речовин і відходів, які переносяться повеневими водами. Внаслідок підйому рівня грантових вод можуть затопляться також і більш віддалені райони. Вихори і град можуть бути наслідком сильної грози та створювати додаткову небезпеку. Бурями називається рух повітря зі швидкістю 75 км/год, а ураганами – за швидкістю від 120 км/год. Крім безпосереднього збитку в результаті тиску вітру і наступних сильних поривів бурі й урагани можуть викликати додаткові загрози, які виходять від уламків і сміття, шо переносяться, у воронці, яка обертається з неймовірною швидкістю. Бурі займають одну з перших позицій як по частоті виникнення, так і по відсотковому розподілу економічного збитку для критичної інфраструктури [15; 132].

2. Епідемії. Під епідемією розуміється масове в географічному та часовому відношеннях поширення будь-якої інфекційної хвороби у тварин чи людей. Підвищена небезпека виникає, наприклад, у зв'язку з глобальним товарообігом і туризмом, промисловим вмістом тварин, а також повенями і

засухами. Пандемія є епідемією, що охоплює населення ряду країн або навіть всього світу. Внаслідок епідемій усі об’єкти критичної інфраструктури змінюють режим свого функціонування. Яскравим прикладом є пандемія, що охопила увесь світ, протягом зимово-весняного періоду у зв’язку з розповсюдженням коронавірусу COVID-19.

Друга категорія – це загрози, які походять від людських прорахунків і технічних збоїв.

1. Пожежі. Пожежа є вогнем, який безконтрольно розповсюджується, та що виник в результаті:

- людських прорахунків і технічних збоїв, включаючи підпал;

- удару блискавки;

- виділення небезпечних речовин або вибухів.

В залежності від їх масштабу пожежі класифікуються, як дрібні, середні (наприклад, в межах будівлі) та великі (наприклад, на промислових підприємствах, великих установках, складах) [138; 145].

2. Вивільнення небезпечних речовин.

До небезпечних речовин належать будь-які хімічні, біологічні, радіологічні або ядерні речовини, що можуть мати шкідливий вплив на довкілля або людину, або призводити до вибухів і пожеж. Небезпечні речовини за своїми властивостями дуже різні: від дратівливих, легкозаймистих і аж до вибухонебезпечних, що становлять загрозу для навколишнього середовища, та завдають хронічного і токсичного збитку.

За допомогою індивідуального реєстру небезпечних речовин можна забезпечити ідентифікацію небезпечних речовин, що використовуються на підприємстві [152; 238].

3. Вибухи − є наслідком раптового об'ємного розширення газів в результаті виділення енергії, що призводить до виникнення ударної хвилі, можливо і з виділенням тепла. Вибухи на критично важливих об'єктах можуть

бути наслідком помилок людини та технічних збоїв, включаючи навмисні дії, удари блискавки або викид небезпечних речовин.

Третя категорія − інші види внутрішнього і зовнішнього фізичного впливу на критичну інфраструктуру.

Внутрішній та зовнішній фізичний вплив на критично важливі об’єкти може бути наслідком нещасних випадків та аварій, таких, як, наприклад:

- дорожньо-транспортні події;

- аварії на виробництві;

- авіакатастрофи.

Поряд з руйнуванням установки нещасні випадки та аварії можуть також призвести до пожеж та вибухів, до викиду небезпечних речовин на об’єктах критичної інфраструктури, а також до інших шкідливих наслідків [114; 115; 152].

Четверта категорія − загрози, які виходять від тероризму або злочинних дій (рис. 3.2).

При цьому більш докладно зазначені на рис. 3.2 форми прояву сучасного внутрішнього тероризму розкрито у табл. 3.1.

В результаті аналізу загальної ситуації щодо наявності загроз критичній інфраструктури, загрози, що виникають внаслідок тероризму чи злочинних діянь, можуть бути віднесені до певних видів загроз залежно від ступеня небезпеки.

При цьому по кожному окремому виду подібних загроз дається коротка характеристика:

- потенційних злочинців;

- можливих або характерних методів дій потенційних злочинців, їх цілей і мотивів;

- ступеня кримінальної активності потенційних злочинців.

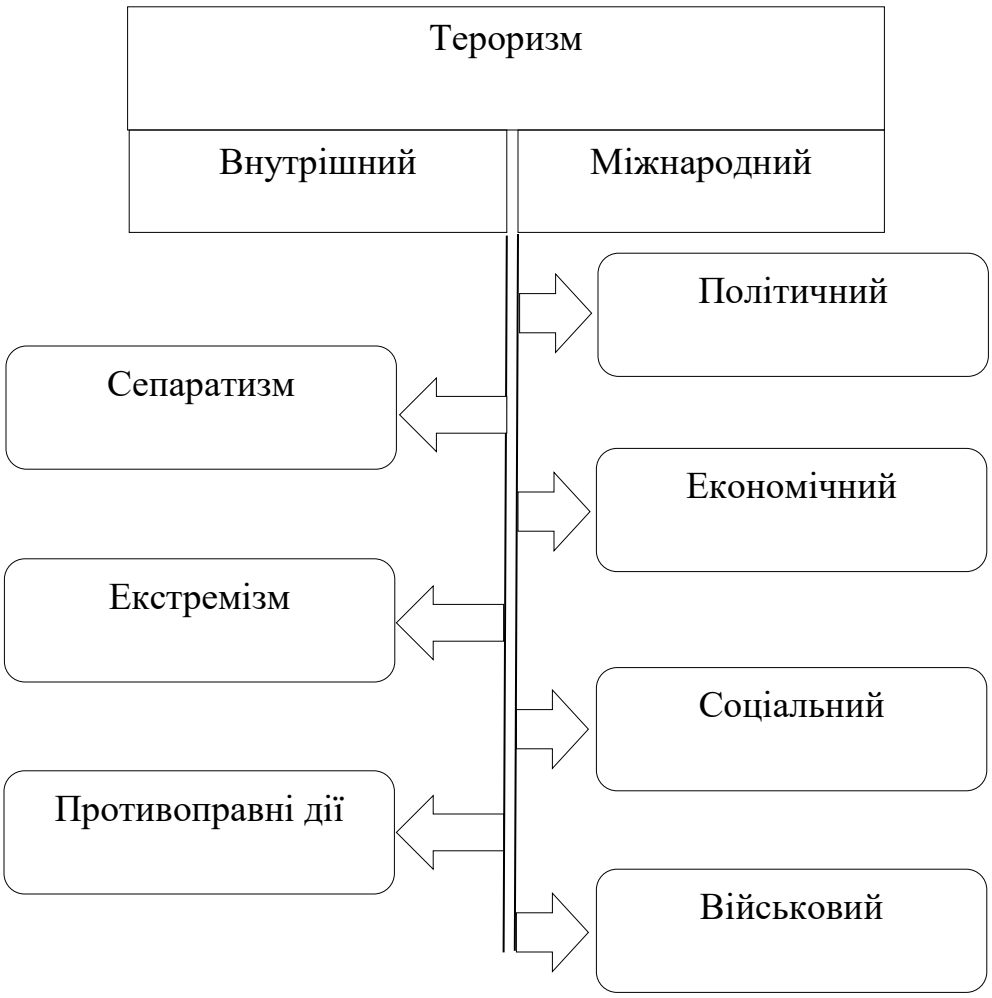

Рис. 3.2. Форми прояву сучасного тероризму

Джерело: авторська розробка

У табл. 3.2 показано характерні особливості різновидів міжнародного тероризму.

Ці види загроз дозволяють наочно показати, які ризики необхідно враховувати. У той же час припущення про те, що такі загрози критичній інфраструктури належать до відповідного типу загроз, базується на криміналістичному досвіді, але не обов'язково знаходить повне підтвердження у кожному конкретному випадку.

Таблиця 3.1

Характерні особливості різновидів внутрішнього тероризму

Різновид внутрішнього тероризму	Особливості
Сепаратизм	Створення незаконних військових формувань Організація систем фіксування і матеріально-технічного забезпечення терористичної діяльності Створення систем інформаційно-політичної підтримки
Екстремізм	Створення та підтримка релігійних екстремістських організацій Створення та підтримка політичних екстремістських організацій Сприяння структурам економічного екстремізму в тіньовій економіці
Протиправні дії	Організація протиправних дій проти юридичних осіб Організація протиправних дій проти фізичних осіб Організація протиправних дій проти державних і громадських діячів Організація протиправних дій, спрямованих на дестабілізацію громадської обстановки, вплив на органи державного управління

Джерело: авторська розробка

Таблиця 3.2

Характерні особливості різновидів міжнародного тероризму

Різновид міжнародного тероризму	Особливості
Політичний	Організація терористичних актів, спрямованих на ослаблення внутрішньої політики держави Організація терористичних, актів, спрямованих на ослаблення зовнішньої політики держави
Економічний	Організація впливу на законотворчу діяльність з метою нанесення економічних збитків державі Організація терактів, що мають наслідком утруднення зовнішньої торгівлі Організація терактів, що впливають на внутрішню економіку Організація каналів фінансування міжнародних терористичних організацій
Соціальний	Створення та підтримка терористичних організацій (осіб, груп), націлених на проведення терактів з метою порушення громадської безпеки і залякування населення Створення та підтримка громадських організацій і рухів, діяльність яких спрямована на дискредитацію соціально-економічної політики держави
Військовий	Організація терактів, що призводять до розв'язування внутрішніх конфліктів, що вимагають залучення збройних сил Організація терактів, спрямованих на знищення військового майна і загибелі особового складу збройних сил Організація терактів, спрямованих на дискредитацію військової політики держави Організація терактів, що впливають на ефективність експорту озброєння і військової техніки

Джерело: авторська розробка

Цілком природно, що не можна однозначно відповісти на питання про потенційних злочинців та їх спосіб дій. Однак, на підставі досвіду щодо забезпечення безпеки підприємств критичної інфраструктури, винних або,

відповідно, злочинців, можна розділити на приблизні групи, виходячи з їх конкретних мотивів та можливих методів дії., а також скласти таблицю, що відображає відповідні ступені небезпеки. При цьому не враховуються необережні дії, оскільки вони стосуються загроз, що виникають внаслідок людських прорахунків та технічних збоїв [36; 60; 61].

Наскільки потенційні злочинці можуть на практиці завдати серйозної шкоди, та в яких місцях це можливо, повинно бути предметом оцінки ризиків критичній інфраструктурі з урахуванням виявлених вразливих місць розташування підприємства, що є об’єктом критичної інфраструктури.

Подібні види загроз критичній інфраструктурі містять ряд вихідних положень, з допомогою яких можна визначити їх співвідношення з виявленою обстановкою в плані наявності загроз. Переважно мова йде про такі посилання:

- можливі супутні для дії обставини;
- можливі мотиви і характерні методи дій;
- допоміжні кошти, використання яких ймовірно;
- очікувана кримінальна активність.

Виходячи зі сполучної ланки між злочинцями, включаючи їх мотивацію, і варіантів дій, зумовлених властивостями самих об'єктів критичної інфраструктури, можна, крім того, провести відмінність залежно від можливостей впливу.

Принципово можливі, наприклад, такі варіанти впливу.

1. Навмисна помилка в обслуговуванні обладнання. Під цим розуміються будь-які навмисні дії, що здатні привести до збоїв в результаті застосування простих прийомів без використання знарядь вчинення злочину. До таких дій можуть, наприклад, належати:

- включення/відключення обладнання;
- відкриття/закриття заглушок трубопроводів (шиберів);
- обертання маховиків і управління важелями по ходу процесу.

При цьому умисна помилка в обслуговуванні може здійснюватися як власними працівниками, так і сторонніми особами.

2. Маніпуляція. Маніпуляція означає навмисну зміну або зміщення компонентів будь-якої системи з метою приведення установки до критичного стану. Можливі приклади:

- неправильне програмування систем управління;

- порушення юстування вимірювальних установок;

- усунення видачі повідомлень про перебіг процесу, розлади або аварійно-попереджувальні сигнали;

- відключення систем захисту.

Потенційними порушниками в цьому випадку виступають переважно інсайдери з детальним знанням установки.

3. Аварія транспортного засобу. Аварії транспортних засобів під час автомобільних або залізничних перевезень в межах виробничої зони об’єкта критичної інфраструктури можуть призвести до викиду небезпечних речовин або пошкодження або руйнування важливих частин установки [15; 117].

Відповідними прикладами є такі:

- утворення течі в бочках у результаті аварії автонавантажувача;

- сходження з рейок вагонів-цистерн;

- руйнування установок внаслідок наїзду вантажних автомобілів.

4. Несанкціоновані дії з використанням елементарних знарядь вчинення злочину. У цьому випадку це означає навмисне, часто спонтанне втручання в роботу важливих частин установки, використовуючи наявні на будь-якому підприємстві, включаючи, зокрема, критичну інфраструктуру, допоміжні засоби та інструменти. Можливі приклади:

- розбивання скляних частин установки;

- заклинювання рухомих частин установки;

- домішування заборонених речовин по ходу процесу.

Потенційними порушниками при цьому виступають, в першу чергу, працівники самого підприємства.

5. Несанкціоновані дії з застосуванням великовагових знарядь вчинення злочину. При даній можливості впливу передбачається, що мова йде про заздалегідь підготовлене насильницьке руйнування частин установки.

Прикладами при цьому можуть слугувати такі дії:

- злом дверей з подальшим руйнуванням обладнання;

- розбивання вимірювальних та керуючих пристроїв та нанесення ударів по резервуарах і трубопроводах з утворенням значної течі внаслідок їх пошкодження.

На зміну цілеспрямованим несанкціонованим діям може прийти вандалізм, наприклад, у вигляді сліпої спраги руйнування після невдалого злому.

6. Підпал із застосуванням елементарних засобів. Під елементарними засобами, зокрема, розуміється займання з використанням сірників, запальничок або недопалків. Тому така можливість впливу існує тільки при наявності достатньої кількості горючих та легкозаймистих матеріалів. Можливі приклади:

- запалювання горючих рідин, що використовуються у виробничому процесі;

- підпал складських приміщень, що призводить до вивільнення небезпечних речовин;

- підпал периферійних приміщень або обладнання, що має наслідки для важливих частин установки.

7. Підпал із застосуванням речовин, що сприяють горінню. У цьому випадку мова йде про підпали об’єктів критичної інфраструктури за допомогою речовин, що швидко та інтенсивно згорають. Можливі приклади таких диверсій:

- виливання і запалювання горючих рідин (наприклад, бензину);

- встановлення професійних пристроїв з запальним складом і таймером або дистанційним підривником.

Такі диверсії можуть вчинятися також ззовні та припускають наявність яскраво вираженої кримінальної активності.

8. Використання вибухових речовин на об’єктах критичної інфраструктури. У цьому випадку можливе застосування саморобних, промислових або військових вибухових речовин. Можливими прикладами таких диверсій є, наприклад, наступні:

- розміщення саморобної бомби-вогнегасника у чутливих ділянках установки або, що більш імовірно, − на периферії будівлі;

- вибух резервуарів і трубопроводів;

- підрив несучих елементів конструкцій, що тягне за собою перекидання резервуарів, руйнування ділянок установки.

9. Обстріл. У найпростішому випадку слід виходити з обстрілу з пневматичних гвинтівок або рогаток (сталевими кулями), але мова може йти і про застосування важкої зброї терористами ñ наприклад зенітної ракетної зброї. Приклади можливого впливу на критичну інфраструктуру:

- заподіяння течі окремо встановлених резервуарів або трубопроводів;

- організація вибуху.

Обстріл можливий переважно із-за зовнішнього огородження виробничої території або промислового парку, причому більшій загрозі піддаються розташовані поблизу від огорожі ділянки установки.

10. Авіакатастрофа. У даному випадку вплив можуть чинити як кінетична енергія падаючих літаків, так і вибух запасу пального або можливої вибухівки, що знаходиться на борту літака вибухівки. Крім того, літак можна використовувати, як транспортний засіб з метою поширення хімічних, біологічних, радіологічних або ядерних речовин.

Диверсії, що призводять до падіння літака, можуть вчинятися ззовні, наприклад, шляхом:

- ракетного обстрілу;

- ініціювання вибуху вибухових речовин на відстані;

- дистанційної маніпуляції бортовою електронікою;

- виведення з ладу авіадиспетчерської служби;

- зсередини шляхом захоплення/порушення керування літаком або вчинення вибуху смертниками.

11. Застосування хімічної, біологічної, радіологічної або ядерної зброї. Залежно від наявності відповідних агентів / знарядь, скоєння такого злочину на об’єктах критичної інфраструктури, ви можете уявити собі широке коло можливих застосувань, яке необхідно розглядати окремо. Такі можливості застосування охоплюють як умисне викликання захворювань або епідемій, так і застосування брудних бомб з метою деморалізації населення і аж до застосування отруйних речовин, наприклад, у районі транспортних вузлів.

12. Об'єднані дії на об’єктах критичної інфраструктури. У цьому випадку також можна собі представити широкий спектр можливостей:

- вищезазначені брудні бомби, що поєднують вибухову дію з радіоактивним зараженням;

- руйнування виробничого обладнання в поєднанні з поширенням небезпечних речовин;

- голосно поширені у ЗМІ індивідуальні акції з серйозними наслідками для діяльності підприємства − об’єкту критичної інфраструктури або постачання населення.

3.3. Удосконалення державної політики захисту критичної інфраструктури в Україні

Об’єкти критичної інфраструктури схильні до поліморфних типів загроз. Ці загрози можуть бути природними, або спричинені необережною поведінкою людини.

Деякі загрози можуть бути спричинені терористичними цілями або іншими злочинними цілями. Кібератаки з метою отримання викупу є прикладом комерційної діяльності, яка може серйозно вплинути на об’єкти критичної інфраструктури, зашифровувавши дані користувачів та вимагаючи оплату в обмін на розблокування даних [29; 109].

Загрози для об’єктів критичної інфраструктури також можуть бути пов'язані із злочинною поведінкою та непрямим чином. Так, багато компаній у будівельному секторі купують невідповідні, неякісні матеріали, які впливають на міцність інфраструктури та піддають їх більшому ризику обвалення. Оскільки країни покликані захищати об’єкти критичної інфраструктури від різних рівнів ризику, ключовим питанням є наступне: чи повинні уряди країн прийняти єдиний план, який охоплює всі можливі загрози, або, скоріше, передбачити прийняття стратегій, пов’язаних із конкретною небезпекою чи ризиком? Фактично будь-який підхід відповідає міжнародно-правовій базі. Серед країн, які прийняли стратегії об’єктів критичної інфраструктури, більшість застосовують підхід з урахуванням усіх небезпек. Це означає, що стратегічні цілі та організаційні структури сформовані таким чином, щоб враховувати випадкові, навмисні та природні загрози для об’єктів критичної інфраструктури в цілому.

Підхід, орієнтований на всі небезпеки, часто розглядається як передумова для найкращого використання обмежених наявних ресурсів та запобігання

непотрібного дублювання. 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 [171; 214]/

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.

Керівні принципи доповнюють загальну стратегію країни щодо забезпечення безпеки об’єктів критичної інфраструктури, яка розширює сферу її дії через охоплення інших небезпек [23; 82].

В Іспанії інституційна архітектура для захисту об’єктів критичної інфраструктури викладена в законі 8/2011 «Про встановлення заходів для захисту критично важливих об'єктів інфраструктур». Фактично зазначений іспанський закон спрямований на протидію терористичній загрозі, хоча він застосовується і до інших (не вказаних) ризиків.

У відповідності з резолюцією 2341 (2017) Ради Безпеки необхідно, щоб терористична загроза повністю і в терміновому порядку відбивалася при підготовці стратегічних планів урядів щодо захисту об’єктів критичної інфраструктури. Зважаючи на це, кожна країна може визначити в рамках своєї національної політики найкращі форми та способи захисту об’єктів критичної інфраструктури від терористичних актів у середовищі з численними загрозами.

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. Це вимагає, зокрема, щоб країни вирішили наступні питання:

- взаємодія між цими іншими політиками захисту об’єктів критичної інфраструктури та конкретною стратегією захисту об’єктів критичної інфраструктури;

- ступінь, в якій ці інші політики та саму стратегію захисту об’єктів критичної інфраструктури необхідно налаштувати і оптимізувати, щоб уникнути конфліктів і забезпечити загальну координацію комплексної політики захисту об’єктів критичної інфраструктури на національному рівні.

Відповідно, далі наведено огляд типів державної політики, які чинять значний вплив на забезпечення безпеки об’єктів критичної інфраструктури, але не обов'язково (або повністю) присвячені цілям захисту об’єктів критичної інфраструктури [29; 173].

Зокрема перший тип державної політики щодо захисту об’єктів критичної інфраструктури − це політика щодо «легких мішеней». Так, у резолюції 2396 (2017) Ради Безпеки підкреслюється, що державам-членам необхідно розробляти, переглядати або вносити поправки в національні оцінки ризиків і загроз з урахуванням легких цілей з тим, щоб розробити відповідні плани дій в нештатних і надзвичайних ситуаціях при терористичних атаках.

У тому ж році Європейська комісія розробила план, сфокусований на громадських місцях як ключовій категорії легких цілей (Європейська комісія, 2017 рік). При цьому необхідно зауважити, що поняття легких цілей концептуально відрізняється від поняття критичної інфраструктури. Основним наслідком цього є те, що політика країн щодо легких цілей автоматично не відповідає умовам та вимогам щодо захисту об’єктів критичної інфраструктури, особливо коли йде мова про здійснення норм та правил резолюції 2341 (2017)

Ради Безпеки. Однак це не означає, що ці дві сфери повинні оброблятися роз'єднано.

Національна політика та практика, розроблена для легких цілей, цілком може виявитися корисною та послужити джерелом передової практики у сфері захисту об’єктів критичної інфраструктури та навпаки. Це явний підхід, прийнятий Радою Європейського Союзу − організацією, що представляє європейську індустрію безпеки і 25 дослідницьких співтовариств. Визнаючи дублюючі функції між політиками з легким цілям і критичною інфраструктурою, Рада Європейського Союзу працює з обома в одній і тій же робочій групі.

Замість того, щоб використовувати роздільний підхід, слід вивчити потенціал взаємодоповнюваності. Беручи до уваги відмінності в концептуальних і нормативних межах, що застосовуються до «легких» цілей та об’єктів критичної інфраструктури, країнам рекомендується розвивати взаємодію, беручи до уваги, що часто одні і ті ж державні установи несуть інституційні й оперативні обов'язки в обох сферах діяльності одночасно.

Другий різновид державної політики захисту об’єктів критичної інфраструктури − це політика національної безпеки. Слід при цьому прийняти до уваги, що національна безпека − це концепція, що змінюється. Країни переводять її на різні підпункти і підходи в залежності від ряду факторів і уявлень, пов'язаних з їх конкретною історією, географічним положенням або геополітичним контекстом [29; 173].

У більшості випадків національна безпека включає в себе принципи, політику, процедури і функції, які спрямовані на те, щоб гарантувати незалежність, суверенітет і цілісність країни, а також права громадян. Деякі країни чітко включають об’єкти критичної інфраструктури до числа своїх пріоритетів національної безпеки. Тісна прив'язка забезпечення безпеки об’єктів критичної інфраструктури до сфери завдань національної безпеки може

допомогти забезпечити посилену політичну підтримку для подальшої розробки спеціалізованих стратегій захисту критичної інфраструктури та полегшити їх реалізацію.

Третій різновид державної політики щодо захисту об’єктів критичної інфраструктури − антитерористична політика. Хоча в більшості контртерористичних стратегій конкретно не згадуються об’єкти критичної інфраструктури, ряд цілей та інституційних механізмів, викладених у них, допомагають зберегти цілісність об’єктів критичної інфраструктури та життєво важливі соціальні функції, які вони виконують.

Наприклад, контртерористичні стратегії опосередковано зачіпають проблеми захисту об’єктів критичної інфраструктури, коли вони встановлюють процедури спільного антикризового управління після терористичної атаки.

Більш того, стратегії боротьби з тероризмом часто встановлюють широкі рамки для запобігання вчинення терористичних злочинів (наприклад, шляхом вивчення підготовчих законодавчих актів, створення взаємодії між розвідувальними та правоохоронними органами тощо).

Глобальна антитерористична стратегія Інтерполу включає сферу захисту об’єктів критичної інфраструктури до свого потоку дій 4.6 «Зброя і матеріали», визначаючи мандат цієї організації з точки зору «підвищення спроможності держав-членів захищати свою критично важливу інфраструктуру і вразливі цілі від фізичних та кібертерористичних атак». При цьому стратегії забезпечення безпеки об’єктів критичної інфраструктури повинні об'єднувати концепції та процедури, викладені в основах політики боротьби з тероризмом шляхом їх адаптації до конкретних потреб та умов захисту критичної інфраструктури.

Четвертий різновид державної політики щодо захисту об’єктів критичної інфраструктури − це політика кібербезпеки. Кібербезпеку, зокрема, можна

визначити як «набір інструментів, політик, концепцій безпеки, заходів безпеки, посібників, а також підходів до управління ризиками, дій, навчання, передового досвіду, гарантій і технологій, які можна використовувати для захисту кіберсередовища, організації та активів користувача» [28; 109].

Політики у сфері кібербезпеки займають центральне місце в захисті об’єктів критичної інфраструктури, оскільки вони забезпечують основу, в якій країни визначають цілі та засоби захисту критично важливих інформаційних інфраструктур. У той же час, ряд регіональних інструментів захисту об’єктів критичної інфраструктури чітко пов'язують поняття концепції кібербезпеки. Наприклад, Конвенція Африканського союзу про кібербезпеку (2014 рік) вимагає, щоб держави-члени зобов'язалися розробити, у співпраці із зацікавленими сторонами, національну політику в сфері кібербезпеки, в якій визнається важливість критично важливої інформаційної інфраструктури для нації, а також визначити ризики, з якими стикається нація при використанні підходу всіх небезпек, та визначає, яким чином повинні бути досягнуті цілі такої політики.

Іншим прикладом є стратегія кібербезпеки Європейського Союзу 2013 року, згідно з якою Європейська комісія зобов'язалася продовжувати свою діяльність, що проводиться спільним дослідницьким центром в тісній координації з владою держав-членів і власниками й операторами критично важливої інфраструктури, по виявленню уразливості європейських критично важливих об'єктів інфраструктури та стимулюванню розвитку відмовостійких систем.

Згідно з директивою Європейського Союзу про мережеву та інформаційну безпеку, (Директива NIS), держави-члени ЄС повинні призначити операторів послуг життєзабезпечення і ввести нові вимоги до безпеки та звітності для

таких організацій. Враховуючи це, не всі національні стратегії кібербезпеки забезпечують однакове місце і важливість для об’єктів критичної інфраструктури, і між країнами існують значні відмінності. Зокрема, деякі стратегії були написані тільки з точки зору кіберзлочинності або тільки з точки зору мережі Інтернету. Вони, як правило, упускають з виду національні явища дестабілізації і антикризове управління для критичної інфраструктури, а також міжгалузевий вплив [28; 38; 203].

Стратегії, написані з точки зору кібербезпеки, засновані на національній оцінці ризику, дістануть більш широких перспектив, які уможливлять забезпечення безпеки критичної інфраструктури.

Корисним інструментом, запропонованим Міжнародним союзом електрозв’язку, є сховище національних стратегій з кібербезпеки. Воно включає в себе велику колекцію національних стратегій кібербезпеки у вигляді одного або декількох документів та як частину більш широких стратегій у сфері інформаційно-комп’ютерних технологій забезпечення національної безпеки. [28; 77].

Враховуючи різноманітність підходів між різними існуючими стратегіями захисту об'єктів критичної інфраструктури та кібербезпеки, Міжнародний союз електрозв'язку в даний час очолює зусилля сумісно з різними глобальними учасниками по створенню загального довідкового керівництва національних стратегій з кібербезпеки. Цей документ покликаний:

- 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.

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. Наприклад, у 2017 році Сінгапур прийняв закон «Про охорону інфраструктури». Даний закон, спеціально присвячений захисту інфраструктур від терористичних дій, вводить ряд таких понять, як:

- «зона під охороною»;

- «місце, що охороняється»;

- «інфраструктура під охороною».

Проте, в ньому не міститься прямого посилання на критично важливі об'єкти інфраструктури з точки зору активів або систем, які виконують важливі функції для спільноти.

У подібних випадках необхідно визначити роль і місце існуючих нормативних рамок в загальних цілях захисту об’єктів критичної інфраструктури. Деякі політики можуть не згадувати об’єкти критичної інфраструктури просто тому, що вони були прийняті в той момент, коли саме поняття забезпечення безпеки об’єктів критичної інфраструктури ще не вступила в основні дискусії щодо політики або з інших причин. Якщо вони вирішують істотні питання, пов'язані з об’єктами критичної інфраструктури, їх слід ретельно проаналізувати, щоб забезпечити їх сумісність та взаємодоповнення з нещодавно розробленими національними стратегіями по

захисту критичної інфраструктури. Інша відповідна політика випливає з міжнародних зобов'язань країн у різних сферах. Наприклад, для дотримання відповідних міжнародно-правових актів, країни розробили цілий ряд політик, законів, положень, стратегій, планів та заходів щодо підвищення безпеки хімічних, біологічних, радіологічних та ядерних об'єктів та відповідної інформації. Забезпечення безпеки автоматизованих систем управління критичною інфраструктурою неможливо без забезпечення безпеки автоматизованих систем управління критично важливими об’єктами та критичної інформаційної інфраструктури загалом [15; 17; 23].

Подібна ситуація обумовлена:

- повсюдним впровадженням широкого спектра інформаційних технологій в системи управління виробничими і технологічними процесами критично важливих об’єктів;

- глобалізацією сучасних інформаційно-телекомунікаційних мереж;

- перетворенням їх у єдину світову інформаційно-телекомунікаційну мережу з розмитими межами національних сегментів;

- значним збільшенням частки розподілених автоматизованих систем управління критично важливими об’єктами та все більш широким використанням інформаційно-телекомунікаційних мереж та мереж зв'язку загального використання для їх обміну інформацією.

Водночас серед факторів, що впливають на формування державної політики у сфері забезпечення безпеки автоматизованих систем управління критично важливою інфраструктурою, слід виділити наступне:

- інтеграція в єдині комплекси автоматизованих систем управління критично важливими об’єктами та інших інформаційних систем, що

використовуються в управлінні виробничо-транспортними структурами, а також адміністративними та фінансовими ресурсами;

- постійне ускладнення програмного забезпечення й обладнання, що використовується в автоматизованих системах управління критично важливими об’єктами;

- практика здійснення іноземними фірмами технічного обслуговування та віддаленого налагодження автоматизованих систем управління критично важливими об’єктами загалом або їх компонентами, а також телекомунікаційного обладнання, що входить до складу критичної інформаційної інфраструктури;

- прагнення організацій, що розробляють програмне забезпечення для автоматизованих систем управління критично важливими об'єктами до зменшення витрат і, як наслідок, використовувати стандартні рішення та запозичене програмне забезпечення;

- інтенсивне вдосконалення засобів та методів використання інформаційно-комунікаційних технологій для заподіяння шкоди Україні, а також спроби їх використання в незаконних цілях та конкуренції, які в майбутньому все частішають;

- збільшення загрози тероризму, зростання кількості незаконних дій з використанням інформаційно-комунікаційних технологій;

- тенденція приховування спроб або фактів порушення штатного функціонування автоматизовані системи управління критично важливими об’єктами, що склалася серед операторів і власників інформаційних систем;

- недостатній рівень освіти та професійної підготовки персоналу, що обслуговує автоматизовані системи управління критично важливими об’єктами, зниження технологічної культури виробництва;

- відсутність достатнього нормативно-правового регулювання процесів забезпечення безпеки автоматизованих систем управління критично важливими об’єктами, в тому числі в частині визначення рівня їх реальної захищеності;

- вимушене залучення у створенні автоматизованих систем управління критично важливими об’єктами іноземних фірм − виробників та постачальників програмних та апаратних засобів обробки, зберігання та передача інформації та використання зарубіжних програмно-апаратних рішень, що створюють передумови для виникнення технологічної та іншої залежності від зарубіжних держав [167; 198]. При цьому основні принципи державної політики у сфері забезпечення безпеки автоматизованих систем управління критично важливими об’єктами повинні бути такі:

- дотримання законодавства України, а також вимог міжнародних договорів України всіма учасниками процесу створення й експлуатації автоматизованих систем управління критично важливими об’єктами;

- поєднання інтересів та взаємної відповідальності держави, громадян, а також організацій, що беруть участь у розробці, створенні та експлуатації автоматизованих систем управління критично важливими об’єктами;

- персоніфікація відповідальності посадових осіб, операторів, персоналу та інших осіб, які беруть участь у розробці, створенні, введенні в дію, експлуатації та модернізації автоматизованих систем управління критично важливими об’єктами;

- забезпечення комплексного захисту критичної інформаційної інфраструктури загалом, включаючи створення єдиної державної системи виявлення та попередження комп'ютерних атак на критичну інформаційну інфраструктуру та оцінку рівня реального захисту її елементів;

- забезпечення дозвільного характеру діяльності в сфері забезпечення безпеки автоматизованих систем управління критично важливими об’єктами з використанням механізмів ліцензування та сертифікації;

- розподіл функцій між ключовим державним органом виконавчої влади у галузі забезпечення безпеки критично важливих об'єктів та інших елементів критичної інформаційної інфраструктури та іншими державними органами виконавчої влади, що здійснюють діяльність у сфері забезпечення безпеки критично важливих об'єктів та інших елементів критичної інформаційної інфраструктури, а також органами державного нагляду та контролю за діяльністю критично важливих об'єктів та інших елементів критичної інформаційної інфраструктури, посилення координації їх діяльності;

- регламентація прав та обов'язків власників автоматизованих систем управління критично важливими об’єктами та іншими об'єктами критичної інформаційної інфраструктури, а також організацій, що їх експлуатують;

- запобігання технологічної чи іншої залежності від іноземних держав при здійсненні діяльності в галузі забезпечення безпеки автоматизованих систем управління критично важливими об’єктами [82; 184].

У зазначеному контексті принципів державної політики в галузі забезпечення безпеки автоматизованих систем управління критично важливими об’єктами є основні завдання, що стосуються вдосконалення нормативно-правової бази у сфері забезпечення безпеки автоматизованих систем управління критично важливими об’єктами повинні бути наступними:

- визначення та розмежування повноважень:

а) ключового державного органу виконавчої влади у сфері забезпечення безпеки критично важливих об'єктів та інших елементів критичної інформаційної інфраструктури;

б) інших органів виконавчої влади, які функціонують у сфері забезпечення безпеки критично важливих об'єктів та інших елементів критичної інформаційної інфраструктури;

в) органів державного нагляду та контролю за діяльністю критично важливих об'єктів та інших елементів критичної інформаційної інфраструктури;

- законодавче визначення та закріплення прав та обов'язків власників автоматизованих систем управління критично важливими об’єктами та іншими об'єктами критичної інформаційної інфраструктури та експлуатуючих організацій у сфері забезпечення безпеки автоматизованих систем управління критичною інфраструктурою;

- визначення порядку:

а) розробки, введення в дію, експлуатації та модернізації автоматизованих систем управління критично важливими об’єктами та інших елементів критичної інформаційної інфраструктури;

б) отримання державним органом виконавчої влади у галузі забезпечення безпеки критичної інфраструктури інформації про автоматизовані системи управління критично важливими об’єктами та інші елементи критичної інформаційної інфраструктури;

в) використання сил та засобів виявлення та попередження комп'ютерних атак на критичну інформаційну інфраструктуру;

г) використання сил та засобів ліквідації наслідків комп'ютерних інцидентів критичної інформаційної інфраструктури;

д) дій посадових осіб, персоналу та власників автоматизованих систем управління критично важливими об’єктами та іншими елементами критичної інформаційної інфраструктури при виявленні спроб або фактів порушення нормативного функціонування цих об'єктів у разі комп'ютерних інцидентів;

- створення правових засад та визначення порядку застосування заходів примусової зміни інформаційного обміну з об'єктами інформатизації, які є джерелами комп'ютерних атак, аж до його повного припинення;

- нормативно-правове забезпечення функціонування єдиної державної системи виявлення комп'ютерних атак на критичну інформаційну інфраструктуру та моніторингу рівня її реальної безпеки;

- встановлення відповідальності за порушення порядку розробки, введення в дію, експлуатації та модернізації автоматизованих систем управління критично важливими об’єктами та іншими елементами критичної інформаційної інфраструктури;

- посилення відповідальності за створення чи застосування засобів комп'ютерних атак на критичну інфраструктуру;

- оптимізація законодавства України в частині ліцензування діяльності, пов'язаної з розробленням, виробництвом, експлуатацією та технічним обслуговуванням автоматизованих систем управління критично важливими об'єктами [24; 46; 80].

При цьому основні завдання державного управління у сфері забезпечення безпеки автоматизованих систем управління критично важливими об’єктами є такими:

- розвиток механізмів державного управління та контролю, а також посилення координації у сфері забезпечення безпеки критичної інформаційної інфраструктури;

- виділення (залучення) необхідних обсягів та джерел фінансових ресурсів (бюджетних та позабюджетних) для реалізації програм та планів заходів у галузі забезпечення безпеки автоматизованих систем управління критично важливими об’єктами та критичної інформаційної інфраструктури в цілому;

- створення єдиної державної системи виявлення та попередження комп'ютерних атак на критичну інформаційну інфраструктуру та оцінки захищеності її елементів;

- забезпечення сталого функціонування національного сегмента єдиної світової інформаційно-телекомунікаційної мережі в умовах масованого деструктивного інформаційного впливу з територій, що перебувають поза юрисдикцією України;

- створення умов, стимулюючих розвиток на території України виробництва телекомунікаційного обладнання, стійкого до комп'ютерних атак;

- створення та підтримка в постійній готовності сил та засобів ліквідації наслідків комп'ютерних інцидентів критичної інформаційної інфраструктури;

- розвиток міжнародного співробітництва, включаючи вдосконалення міжнародної кооперації у сфері забезпечення інформаційної безпеки;

- стимулювання, зокрема, матеріальне, проведення приватними організаціями та особами досліджень стосовно виявлення вразливостей програмного забезпечення і устаткування, що застосовується в автоматизованих системах управління критично важливими об’єктами і на інших об'єктах критичної інформаційної інфраструктури, з поданням результатів державному органу виконавчої влади у сфері забезпечення безпеки критичної інфраструктури [193; 221].

При цьому основні завдання щодо вдосконалення промислової та науково-технічної політики в галузі забезпечення безпеки автоматизованих систем управління критично важливими об’єктами повинні бути такі:

- проведення комплексу заходів з розвитку систем, засобів та методів технічної оцінки рівня реальної захищеності автоматизованих систем

управління критично важливими об’єктами та критичною інформаційною інфраструктурою загалом;

- створення єдиних реєстрів програмних і апаратних засобів, що використовуються в автоматизованих системах управління критично важливими об’єктами; створення баз даних, що стосуються надійності функціонування автоматизованих систем управління критично важливими об’єктами, стану їх захищеності, технічного стану обладнання, а також оцінки ефективності заходів безпеки, що діють і впроваджуються на критично важливих об'єктах;

- проведення комплексу організаційно-технічних заходів щодо виключення обміну інформацією між автоматизованими системами управління критично важливими об'єктами через територію зарубіжних країн, а у разі технічної неможливості такого виключення - створення та застосування захисних заходів, що забезпечують відсутність будь-яких негативних наслідків на процеси, керовані автоматизованими системами управління критично важливими об'єктами, у разі порушення штатного функціонування цього каналу зв'язку;

- розробка комплексу заходів по створенню і впровадженню телекомунікаційного обладнання, стійкого до комп'ютерних атак;

- створення сховища еталонного програмного забезпечення, що використовується в автоматизованих системах управління критично важливими об’єктами і на інших об'єктах критичної інформаційної інфраструктури;

- розвиток (з урахуванням мобілізаційної готовності) науково- виробничої бази, що забезпечує випуск систем (засобів) забезпечення безпеки автоматизованих систем управління критично важливими об’єктами та іншими об'єктами критичної інформаційної інфраструктури;

- розробка та впровадження імпортозамінюючих технологій, матеріалів, комплектуючих та інших видів продукції, які використовуються в автоматизованих системах управління критично важливими об’єктами [22; 144].

Основні завдання в галузі розвитку фундаментальної та прикладної науки, технологій та засобів забезпечення безпеки автоматизованих систем управління критичною інфраструктурою та критичною інформаційною інфраструктурою:

- розробка методів та засобів своєчасного виявлення загроз та оцінки їх небезпеки для автоматизованих систем управління критичною інфраструктурою та інших елементів критичної інформаційної інфраструктури;

- розробка та впровадження спеціалізованих інформаційно-аналітичних систем, розвиток досліджень у галузі математичного моделювання процесів забезпечення безпеки автоматизованих систем управління критичною інфраструктурою та іншими об'єктами критичної інформаційної інфраструктури, спрямованих на розробку ймовірних сценаріїв розвитку ситуації та підтримку управлінських рішень;

- розробка та впровадження комплексних систем захисту та забезпечення безпеки автоматизованих систем управління критичною інфраструктурою й іншими об'єктами критичної інформаційної інфраструктури, що відповідають сучасному рівню розвитку інформаційних технологій та мінімізують участь обслуговуючого персоналу в налаштуванні та експлуатації програмно-апаратних засобів, що входять до їх складу;

- розробка автоматизованих систем управління критичною інфраструктурою спеціалізованих економічно доцільних інформаційних технологій, що виключають або мінімізують обмін інформацією на технологічному рівні, що підлягає обов'язковому захисту [70; 71].

Основні завдання вдосконалення освіти, підготовки та підвищення кваліфікації кадрів у галузі забезпечення безпеки автоматизованих систем управління критичною інфраструктурою, а також підвищення загального рівня культури інформаційної безпеки громадян:

- вдосконалення системи підготовки, перепідготовки та атестації персоналу (включаючи керівників) у галузі забезпечення безпеки автоматизованих систем управління критичною інфраструктурою та критичною інформаційною інфраструктурою на базі профільних освітніх установ;

- підвищення загального рівня культури інформаційної безпеки громадян, включаючи підвищення інформованості населення про критичну інформаційну інфраструктуру, загрозу інформаційної безпеки та способи захисту від цих загроз;

- формування у суспільній свідомості нетерпимості до осіб, які вчиняють протиправні дії із застосуванням інформаційних технологій стосовно критичної інфраструктури.

Реалізація цих основних механізмів забезпечується шляхом консолідації зусиль органів державної влади та інститутів громадянського суспільства, спрямованих на захист інтересів України за допомогою комплексного використання правових, організаційних, технічних, соціально-економічних, спеціальних та інших заходів підтримки.

Координацію діяльності державних органів виконавчої влади з реалізації цих основних механізмів Державна служба України з надзвичайних ситуацій [169; 206].

Зазначені основні напрями реалізуються в рамках:

- існуючих і планованих державних програм;

- плану заходів щодо реалізації цих основних механізмів, який затверджується Урядом України.

Основні механізми та етапи реалізації державної політики у сфері забезпечення безпеки автоматизованих систем управління критичної інфраструктури полягають в наступному [29, с. 20−55].

На першому етапі (2020−2022 роки) необхідно здійснити:

- підготовку плану заходів щодо реалізації цих основних механізмів;

-нормативно-правове визначення та розмежування повноважень та відповідальності державних органів виконавчої влади у сфері забезпечення безпеки, інших державних органів виконавчої влади, які здійснюють діяльність у сфері забезпечення безпеки, органів державного нагляду та контролю, управління діяльністю критично важливих об’єктів та об'єктів критичної інформаційної інфраструктури;

- визначення порядку використання сил та засобів виявлення та попередження комп'ютерних атак на критичну інформаційну інфраструктуру;

- розробку концепції використання сил та засобів ліквідації наслідків комп'ютерних інцидентів критичної інформаційної інфраструктури;

- визначення необхідних обсягів та джерел фінансових ресурсів (бюджетних та позабюджетних) для реалізації програм та планів заходів у галузі забезпечення безпеки автоматизованих систем управління критично важливими об’єктами та критичною інформаційною інфраструктурою в цілому на період другого етапу впровадження цих основних механізмів;

- підготовку пропозицій щодо внесення змін у затверджені державні програми і коригування запланованих державних програм стосовно захисту критичної інфраструктури [22; 65].

На другому етапі (2022−2025 роки) необхідно здійснити:

- розробку нормативних правових актів, які визначають:

а) порядок отримання державним органом виконавчої влади у галузі забезпечення безпеки критичної інфраструктури інформації про автоматизовані системи управління критично важливими об’єктами та інші об'єкти критичної інформаційної інфраструктури;

б) права та обов'язки власників автоматизованих систем управління критично важливими об’єктами та іншими об'єктами критичної інформаційної інфраструктури, а також експлуатуючих організацій у галузі забезпечення безпеки;

в) порядок розробки, введення в дію, експлуатації та модернізації автоматизованих систем управління критично важливими об’єктами;

г) регламент функціонування єдиної державної системи виявлення та запобігання комп'ютерних атак на критичну інформаційну інфраструктуру та оцінки захищеності її елементів;

д) порядок усунення наслідків комп’ютерних інцидентів критичної інформаційної інфраструктури;

е) дії посадових осіб, персоналу та власників автоматизованих систем управління критично важливими об’єктами та іншими об'єктами критичної інформаційної інфраструктури при виявленні несанкціонованого доступу до оброблюваної інформації та інших комп'ютерних інцидентів;

є) відповідальність за порушення встановленого порядку розробки, введення в дію, експлуатації та модернізації автоматизованих систем управління критично важливими об’єктами й іншими об'єктами критичної інформаційної інфраструктури;

ж) правові підстави і порядок застосування заходів примусової зміни інформаційного обміну з об'єктами інформатизації, які є джерелами комп'ютерних атак, аж до повного його припинення;

- проведення паспортизації автоматизованих систем управління критично важливими об’єктами;

- розробку системи грантів для приватних осіб і організацій, покликаних стимулювати дослідження у сфері виявлення вразливостей програмного забезпечення та обладнання автоматизованих систем управління критично важливими об’єктами й іншими об'єктами критичної інформаційної інфраструктури;

- розробку комплексних систем захисту та забезпечення безпеки автоматизованих систем управління критично важливими об’єктами та іншими об'єктами критичної інформаційної інфраструктури, що відповідають сучасному рівню розвитку інформаційно-комунікаційних технологій, та мінімізують участь обслуговуючого персоналу в налаштуванні та експлуатації програмно-апаратних засобів, що входять до їх складу;

- визначення необхідних обсягів та джерел фінансових ресурсів (бюджетних та позабюджетних) для реалізації програм та планів заходів у галузі забезпечення безпеки автоматизованих систем управління критично важливими об’єктами та критичної інформаційної інфраструктури загалом на наступних етапах реалізації цих основних механізмів;

- введення в експлуатацію першого етапу Ситуаційного центру єдиної державної системи виявлення та попередження комп’ютерних атак на критичну інформаційну інфраструктуру та оцінювання рівня реальної безпеки її елементів;

- створення сил та засобів ліквідації наслідків комп'ютерних інцидентів критичної інформаційної інфраструктури [23; 82].

На третьому етапі (2025−2030 роки) необхідно здійснити:

- впровадження комплексних систем захисту та забезпечення безпеки автоматизованих систем управління критично важливими об’єктами та іншими об'єктами критичної інформаційної інфраструктури, що відповідають сучасному рівню розвитку інформаційних технологій, та мінімізують участь обслуговуючого персоналу в налаштуванні та роботі програмного та апаратного забезпечення, що входить до їх складу;

- введення в дію першого етапу сховища еталонного програмного забезпечення, що використовується в автоматизованих системах управління критично важливими об'єктами та іншими об'єктами критичної інформаційної інфраструктури;

- впровадження системи грантів для приватних осіб та організацій для стимулювання досліджень у галузі виявлення вразливостей програмного забезпечення та обладнання автоматизованих систем управління критично важливими об’єктами та іншими об'єктами критичної інформаційної інфраструктури;

- введення в експлуатацію ситуаційного центру єдиної державної системи виявлення та попередження комп'ютерних атак на критичну інформаційну інфраструктуру України та оцінки рівня реальної захищеності її елементів та ситуаційних центрів регіонального та відомчого рівнів;

- створення автоматизованих систем управління критично важливими об’єктами, а також спеціалізованих економічно доцільних інформаційних технологій, що виключають або в максимальному ступені знижують на технологічному рівні обмін інформацією, що підлягає обов'язковому захисту;

- введення в експлуатацію в цілому єдиної державної системи виявлення та попередження комп'ютерних атак на критичну інформаційну інфраструктуру та оцінки рівня реальної захищеності її елементів [72; 137; 193].

В період після 2030 року має здійснюватися комплекс заходів з підтримки організаційної, економічної, науково-технічної і технологічної готовності України до запобігання загроз безпеки її критичній інформаційній інфраструктурі.

Відповідно, у дисертаційній роботі пропонується створення єдиної державної системи безпеки значущих об'єктів критичної інформаційної інфраструктури, що являє собою комплекс взаємопов'язаних методологічних, організаційних та технічних рішень для управління процесами захисту об'єктів критичної інформаційної інфраструктури та підвищення ефективності захисту значущих об'єктів критичної інформаційної інфраструктури на всіх етапах їх життєвого циклу [219; 221].

В рамках проекту створення єдиної державної системи безпеки важливих об'єктів критичної інформаційної інфраструктури необхідно виконати такі основні блоки робіт:

- категоріювання об'єктів критичної інформаційної інфраструктури;

- розробка технічного завдання та технічне проектування систем захисту інформації значущих об'єктів критичної інфраструктури;

- впровадження систем захисту інформації значущих об'єктів критичної інфраструктури;

- створення центру моніторингу та управління інцидентами інформаційної безпеки критично важливих інфраструктурних об'єктів.

Зокрема, в рамках створення центру моніторингу і управління інцидентами інформаційної безпеки об’єктів критичної інфраструктури пропонується:

- впровадження (зокрема, постачання програмно-апаратних рішень) і розвиток системи аналізу та моніторингу подій безпеки, включаючи:

а) розробку кореляційних правил;

б) підключення джерел подій, в тому числі таких, що не підтримуються штатно;

в) розробку звітності технічної, експлуатаційної й організаційної документації системи;

- постачання, інтеграцію та впровадження засобів сегмента органів державного регулювання;

- розробку та впровадження процесів і регламентів функціонування центру моніторингу і управління інцидентами об’єктів критичної інфраструктури, включаючи регламенти взаємодії з органами державного регулювання;

- навчання відповідального персоналу служб інформаційної безпеки й інформаційних технологій, включаючи проведення кібернавчання [29; 172].

Створення єдиної інформаційної платформи для консолідації даних про об’єкти критичної інфраструктури, засоби та системи захисту інформації важливих об'єктів критичної інфраструктури, включаючи системи захисту інформації та їх відповідність діючій нормативно-правовій базі України, а також українським та міжнародним стандартам у галузі захисту інформації значно підвищить рівень державного управління критичною інфраструктурою загалом [137; 193].

Так, впровадження єдиної системи безпеки значущих об'єктів критичної інформаційної інфраструктури дозволить:

- забезпечити відповідність вимогам нормативно-правової бази, здійснити необхідні заходи щодо підключення до державної системи виявлення, запобігання та ліквідації наслідків комп'ютерних атак на інформаційні ресурси України;

- мінімізувати ризики штрафних санкцій та приписів з боку регулюючих органів, а також виникнення адміністративної та кримінальної відповідальності працівників організації, які виникають при виявленні порушень вимог законодавства;

- регламентувати процеси захисту інформації об'єктів критичної інфраструктури, а також процеси реагування на інциденти інформаційної безпеки, персоналізувати відповідальність за порушення в галузі обробки та захисту інформації об'єктів критичної інфраструктури;

- підвищити рівень обізнаності персоналу у сфері інформаційної безпеки критичної інфраструктури;

- підвищити ефективність системи забезпечення інформаційної безпеки за рахунок модернізації застарілих засобів захисту інформації та створення центру моніторингу та управління інцидентами інформаційної безпеки об’єктів критичної інфраструктури;

- оптимізувати витрати на забезпечення дотримання законодавчих вимог та підтримку необхідного рівня захисту інформаційної інфраструктури, що входить до найважливіших об'єктів, шляхом створення інструментів контролю та управління безпекою на всіх етапах життєвого циклу критичної інфраструктури;

- знизити технологічні, репутаційні, економічні та соціальні ризики, пов'язані з інформаційною безпекою об'єктів критичної інфраструктури.

Висновки до третього розділу

1. Обгрунтовано, що для практичної реалізації заходів державного управління стосовно стратегічних ризиків для критичної інфраструктури повинні застосовуватися системно-правовий, політичний, інформаційний, економічний й організаційно-адміністративний механізми у межах комплексного механізму державного управління забезпеченням безпеки критичної інфраструктури.

Зокрема, щодо системно-правового механізмі вимагається розробка на загальнодержавному та регіональному рівнях нового та розвиток чинного законодавства, яке охоплюватиме найважливіші, значущі та пріоритетні з точки зору національної безпеки держави види стратегічних ризиків для критичної інфраструктури й обумовлені ними загрози.

Обґрунтовано, що основним способом удосконалення нормативно-правового механізму забезпечення безпеки критично важливих об'єктів є прийняття в даній галузі базового закону , який би визначив основні поняття, види та категорії критично важливих об'єктів, а також встановив би вимоги щодо забезпечення безпеки окремих категорій таких об'єктів.

У межах політичного механізму, насамперед, необхідно офіційне визнання на вищому рівні концепції державного управління стратегічними ризиками для критичної інфраструктури як методологічної основи вирішення завдання забезпечення сталого розвитку України.

Інформаційний механізм повинен забезпечувати координацію компетентним органом, починаючи від введення складу і показників стратегічних ризиків для критичної інфраструктури, оцінки очікуваного збитку від їх реалізації, до їх подання органам державного регулювання, засобам масової інформації та громадськості в зручному і зрозумілому вигляді.

Економічний механізм зниження стратегічних ризиків для критичної інфраструктури повинен включати як пряме державне регулювання на основі цільових витрат державних бюджетів, так і непряме державне регулювання за рахунок вдосконалення податкового та кредитного механізмів щодо зниження податкового навантаження.

Щодо удосконалення організаційно-адміністративних механізмів потрібно створення в рамках проведеної в державі адміністративної реформи державного компетентного органу − «стратегічного ризик-менеджера» − з усім необхідним для його функціонування і повноцінною координацією інфраструктури. Реформа органів державної влади потребуватиме залучення висококваліфікованих ризик-менеджерів в структурах управління на загальнодержавному, регіональному і місцевому рівнях.

При цьому важливу роль у справі становлення організаційних важелів управління стратегічними ризиками для критичної інфраструктури буде відігравати:

- вдосконалення державних систем нагляду та контролю;

- оптимальний розподіл виконавчих і контрольних функцій між рівнями державного та муніципального управління;

- оптимізація діяльності всіх органів державної влади, які беруть участь у процесі управління критичною інфраструктурою.

2. Підкреслено роль державно-приватного партнерства для захисту об’єктів критичної інфраструктури. Показано, що приватні оператори знаходяться в авангарді інвестицій та головних зусиль у розробці нових технологій виробництва і захисту. Ці обставини в поєднанні з тим фактом, що основна відповідальність за захист активів та систем об’єктів критичної інфраструктури покладається на їх власників та операторів, підкреслює важливість створення ефективного державно-приватного партнерства для досягнення належного рівня стійкості критично важливих об’єктів.

3. Доведено, що система державного управління стосовно захисту критичної інфраструктури має включати два рівня прийняття рішень:

- загальнодержавний;

- регіональний, а також відповідні механізми: політичні, правові, інституційні, адміністративні, економічні, науково-технічні та ін.

Зазначено, що для кожного з рівнів повинні бути визначені відповідні повноваження та визначена ступінь відповідальності за прийняті рішення: на загальнодержавному − по управлінню зовнішніми та внутрішніми стратегічними ризиками для критичної інфраструктури, на регіональному − внутрішніми ризиками для критичної інфраструктури.

4. Запропоновано склад компонентів комплексної державної політики, які суттєво впливають на забезпечення безпеки об’єктів критичної інфраструктури, але можуть бути не обов'язково або повністю присвячені цілям захисту об’єктів критичної інфраструктури: політика щодо «легких мішеней», політика національної безпеки, антитерористична політика та політика кібербезпеки.

5. Запропоновано комплекс заходів для забезпечення реалізації основних механізмів та етапів впровадження державної політики у сфері забезпечення безпеки автоматизованих систем управління критичної інфраструктури шляхом

консолідації зусиль органів державної влади та інститутів громадянського суспільства, спрямованих на захист інтересів України: правові, організаційні, технічні, соціально-економічні та спеціальні.

Матеріали даного розділу оприлюднені в наступних публікаціях автора: [62; 64; 70].

ВИСНОВКИ

У дисертації вирішено важливе наукове завдання щодо обґрунтування теоретичних засад та розроблення науково-практичних рекомендацій відносно вдосконалення процесів державного управління забезпеченням безпеки критичної інфраструктури. Основні висновки за результатами проведеного дослідження такі.

1. Розкрито сутність державного управління забезпеченням безпеки об'єктів критичної інфраструктури. Обґрунтовано, що у процесі державного управління об'єктами критичної інфраструктури слід виділяти два рівні, для кожного з яких характерним є певний зміст.

Зокрема, перший рівень включає управлінську діяльність аналітичного, науково-прогностичного й організаційного характеру. Її результатом, насамперед, є визначення стратегій управління під зовнішніми впливами, а також організація механізму їх реалізації з урахуванням соціальних, економічних та інших факторів.

Другий рівень процесу державного управління функціонуванням об'єктів критичної інфраструктури стосується організаційно-технічних систем. Базовими елементами системи державного управління на цьому рівні є такі:

- 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.

2. Визначено особливості формування державної системи захисту критичної інфраструктури. Показано, що формування державної системи захисту критичної інфраструктури України при надзвичайних ситуаціях і

терористичних актах підпорядковане дії великого і тісно пов'язаного між собою кола закономірностей. Їх доцільно об'єднати в дві великі групи, що відображають соціально-економічний і організаційний характер будівництва системи.

Зокрема, група закономірностей соціально-економічного характеру відображає зв'язок формування системи забезпечення безпеки населення та захисту критично важливих об'єктів України при надзвичайних ситуаціях та терористичних актах із зовнішніми та внутрішніми умовами розвитку суспільства та держави.

Інша група закономірностей носить організаційний характер і виражає ті внутрішні складові, які притаманні тільки даній системі, та становлять особливості її формування в порівнянні з іншими державними системами та характеризує взаємозв'язок між складовими елементами системи, а також внутрішню логіку формування кожної з них.

3. Проаналізовано досвід зарубіжних країн щодо державного управління забезпеченням безпеки критичної інфраструктури. Зокрема, виділено такі основні риси цієї діяльності: системи управління з дій у кризових ситуаціях мають державний статус; діяльність з попередження та ліквідації кризових ситуаціях є важливою соціальною функцією кожної держави і реалізується більшістю державних структур; право введення особливого режиму діяльності органів управління та населення в зоні лиха надано не тільки главі держави, але й главам суб'єктів держави (наприклад, губернаторам штатів у США); фінансування діяльності щодо захисту критичної інфраструктури в кризових ситуаціях здійснюється переважно шляхом реалізації державних програм; акценти в правовому регулюванні ризику все більше зміщуються у бік превентивних заходів.

Зазначено, що деякі країни не мають спеціального регулятора у сфері кібербезпеки критичної інфраструктури, але натомість наділяють офіційне представництво широкими повноваженнями з підтримки безпеки в національному кіберпросторі.

Підкреслено, що інформований вибір стратегії управління кібербезпекою критичної інфраструктури можливий лише для тих держав, які знаходяться в самому початку цього шляху. Згідно з даними Міжнародного союзу електрозв'язку, офіційний департамент із захисту критичної інфраструктури так чи інакше працює в більшості країн світу. Цей орган, через брак державного регулятора, може офіційно або неофіційно виступати також у ролі відомства відповідального за всі аспекти національної кібербезпеки.

4. Окреслено специфіку державного управління забезпеченням безпеки критичної інфраструктури в Україні. Відзначено, що в сучасний період перед державним управлінням, зокрема, стосовно забезпечення безпеки критичної інфраструктури в Україні об'єктивно стоять наступні цілі: формування нових інститутів державної влади та оптимізація діяльності існуючої системи виконавчої влади (адміністративна реформа); розгортання та зміцнення суспільних інститутів, які забезпечують стійку демократію суспільства та держави; створення та впровадження в життя соціальних та адміністративно - правових регуляторів, які гарантують конституційно проголошений набір прав, свобод та обов'язків громадян України; формування та практична реалізація державної політики, спрямованої на забезпечення безпеки населення та захисту об'єктів критичної інфраструктури; забезпечення внутрішньої та зовнішньої безпеки регіонів України та сприятливих мирних умов для їх життєдіяльності; досягнення гармонійного, збалансованого та взаємопов'язаного розвитку

регіонів у взаємодії з центром на основі поглиблення процесів формування та функціонування всеукраїнського ринку.

5. Здійснено оцінку вітчизняного нормативного й адміністративного забезпечення державного управління критичною інфраструктурою. Відмічено, що в Україні існує декілька нормативно-правових актів, що регулюють інформаційну безпеку об'єктів критичної інфраструктури. Зокрема, Постанова Кабінету Міністрів «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19 червня 2019 р. № 518.

Щодо безпосередніх правових норм державного управління критичною інфраструктурою в Україні, то присутній лише законопроект «Про критичну інфраструктуру та її захист», який, зокрема, передбачає розмежування органів державної влади щодо визначених секторів захисту критично важливих об'єктів.

Вищезазначене дозволяє стверджувати, що в сучасних умовах адміністративно-правове забезпечення захисту критичної інфраструктури в Україні потребує суттєвого вдосконалення враховуючи відсутність специфічних нормативно-правових актів у цієї галузі, а також функціонального розгалуження органів державної влади та місцевого самоврядування, оскільки ключовим органом державної виконавчої влади щодо захисту критично важливих об'єктів є Державна служба України з надзвичайних ситуацій з урахуванням ймовірності виникнення на цих об'єктах аварій природного та техногенного характеру.

6. Вдосконалено державні механізми забезпечення безпеки та підвищення ефективності захисту критичної інфраструктури. Обґрунтовано, що для практичної реалізації заходів державного управління стосовно стратегічних ризиків для критичної інфраструктури повинні застосовуватися системно-правовий, політичний, інформаційний, економічний й організаційно-

адміністративний механізми у межах комплексного механізму державного управління критичною інфраструктурою.

Зокрема, щодо системно-правового механізму вимагається розробка на загальнодержавному та регіональному рівнях нового та розвиток чинного законодавства, яке дозволить охопити найбільш важливі, значущі та пріоритетні з точки зору національної безпеки держави види стратегічних ризиків для критичної інфраструктури й обумовлені ними загрози.

Обґрунтовано, що основним способом удосконалення нормативно-правового механізму забезпечення безпеки критично важливих об'єктів є прийняття базового закону в цій галузі, який би визначив основні поняття, види та категорії критично важливих об'єктів, а також встановив би вимоги щодо забезпечення безпеки окремих категорій таких об'єктів.

У межах політичного механізму, насамперед, необхідно офіційне визнання на вищому рівні концепції державного управління стратегічними ризиками для критичної інфраструктури як методологічної основи вирішення завдання забезпечення сталого розвитку України.

Інформаційний механізм повинен забезпечувати координацію з боку компетентного органу, починаючи з введення складу та показників стратегічних ризиків для критичної інфраструктури, оцінки очікуваного збитку від їх реалізації, до їх подання органам державного управління, засобам масової інформації та громадськості у зручній та зрозумілій формі.

Економічний механізм зниження стратегічних ризиків для критичної інфраструктури повинен включати як пряме державне регулювання на основі цільових витрат державних бюджетів, так і непряме державне регулювання за рахунок вдосконалення податкового та кредитного механізмів щодо зниження податкового навантаження.

Щодо удосконалення організаційно-адміністративних механізмів потрібно створення в рамках проведеної в державі адміністративної реформи державного компетентного органу − «стратегічного ризик-менеджера» − з усім необхідним для його функціонування і повноцінною координацією інфраструктури. Реформа органів державної влади потребуватиме залучення висококваліфікованих ризик-менеджерів в структурах управління на загальнодержавному, регіональному і місцевому рівнях.

7. Виокремлено напрями розвитку системи державного управління забезпеченням захисту критичної інфраструктури. Доведено, що система державного управління щодо захисту критичної інфраструктури повинна включати два рівні прийняття рішень:

- загальнодержавний;

- регіональний, а також відповідні механізми: політичні, правові, інституційні, адміністративні, економічні, науково-технічні та ін.

Зазначено, що для кожного з рівнів повинні бути визначені відповідні повноваження та визначена ступінь відповідальності за прийняті рішення: на загальнодержавному − по управлінню зовнішніми та внутрішніми стратегічними ризиками для критичної інфраструктури, на регіональному − внутрішніми ризиками для критичної інфраструктури.

8. Запропоновано шляхи вдосконалення державної політики захисту критичної інфраструктури в Україні. Запропоновано склад компонентів комплексної державної політики, які чинять значний вплив на забезпечення безпеки об’єктів критичної інфраструктури, але можуть бути не обов'язково або повністю присвячені цілям захисту об’єктів критичної інфраструктури: політика щодо «легких мішеней», політика національної безпеки, антитерористична політика та політика кібербезпеки.

Запропоновано комплекс заходів, що забезпечують реалізацію основних механізмів та етапів впровадження державної політики у сфері забезпечення безпеки автоматизованих систем управління критичної інфраструктури через консолідацію зусиль органів державної влади та інститутів громадянського суспільства, спрямованих на захист інтересів України: правові, організаційні, технічні, соціально-економічні та спеціальні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абрамов Ю. А. Взаимосвязь инициирующих и поражающих факторов чрезвычайных ситуаций природного характера на территории Украины / Ю.А. Абрамов, В.В. Тютюник, Р.И. Шевченко // Проблеми надзвичайних ситуацій. – 2007. – С. 8−17.

2. Акимов В.А. Основы анализа и управления риском в природной и техногенной сферах / В. А. Акимов, В. В. Лесных, Н. Н. Радаев. – М. : Деловой экспресс, 2004. – 352 с.

3. Андреєв С. О. Формування інституціональних засад діяльності органів місцевого самоврядування в Україні як суб’єктів забезпечення цивільного захисту / С. О. Андреєв // Вісник Національного університету цивільного захисту України. Серія. Державне управління. – 2016. – Вип. 1 (4). – С. 223–235.

4. Андронов В. А. Державні механізми забезпечення екологічної оцінки у сфері запобігання і ліквідації наслідків надзвичайних ситуацій / В. А. Андронов, Є.О. Варивода // Теорія та практика державного управління : зб. наук. пр. – Х. : Вид-во ХарРІ НАДУ «Магістр», 2013. – № 4. – С. 236–244.

5. Андрусяк Т. Г. Теорія держави і права : навч. посіб. / Т. Г. Андрусяк. – Львів, 1997. – 198 с.

6. Антонов В. О. Суспільство як об'єкт національної безпеки Української держави / В. О. Антонов // Держава і право. Юридичні і політичні науки. – 2013. – Вип. 60. – С. 79–84.

7. Атаманчук Г. В. Теория государственного управления : курс лекций / Г. В. Атаманчук. – М. : Юрид. лит-ра, 1997. – 400 с.

8. Аудит пожежної і техногенної безпеки [Електронний ресурс]. –

Режим доступу: http://audit.nuczu.edu.ua/

9. Бабков Ю. П. Запобігання та ліквідація надзвичайних ситуацій / Ю. П. Бабков, М. М. Адамчук // Збірник наукових праць Харківського університету Повітряних Сил. – 2015. – Вип. 4 (45). – С. 153– 157.

10. Бакуменко В. Д. Державне управління : основи теорії, історія і практика : навч. посіб. / В. Д. Бакуменко, П. І. Надолішній, М. М. Їжа, Г. І. Арабаджи ; за заг. ред. П. І. Надолішнього, В. Д. Бакуменка. – Одеса : ОРІДУ НАДУ, 2009. – 394 с.

11. Барило О. Г. Удосконалення організаційного механізму державного управління у надзвичайних ситуаціях / О. Г. Барило, С. П. Потеряйко // Вісник Національного університету цивільного захисту України. Серія. Державне управління. – 2016. – Вип. 2 (5). – С. 264–272.

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

13. Бєлоусов А. В. Наукові підходи до визначення ризику надзвичайних ситуацій як об’єкту управління / А.В. Бєлоусов // Наукові розвідки з державного та муніципального управління. – 2015. – №1. – С. 224–235.

14. 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.

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

16. Безпека людини у надзвичайних ситуаціях : навч. посіб. / За ред. В. І. Голінька. – Д. : Національний гірничий університет, 2011. – 161 с.

17. Безпека як категорія і функція державного управління / Г. П. Ситнік

// Вісн. Нац. академії держ. управління. – 2004. – № 1. – С. 350–357.

18. Бек У. Общество риска: На пути к другому модерну. / У. Бек; пер. с нем. В. Седельника. – М. : Прогресс-Традиция, 2000. – 383 с.

19. Білоусов А. В. Сутність, складові та зміст комплексного механізму державного управління ризиками надзвичайних ситуацій [Електронний ресурс] / А. В. Білоусов // Державне будівництво. – 2014. – № 2. – Режим доступу: http://www.kbuapa.kharkov.ua/e-book/db/2014-2/doc/2/10.pdf

20. Білявська О. Міжнародні стандарти управління ризиками / О. Білявська // Управління сучасним містом. – 2008. − № 1–4/1–12 (29−32). – С. 50–56.

21. 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.

22. 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.

23. 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

24. Бойко-Бойчук О. В. Механізми державного управління: узагальнена модель [Електронний ресурс] / О. В. Бойко-Бойчук. – Режим доступу : concept.at.ua/load/0-0-0-34-20

25. Болотських М. В. Державна політика у сфері цивільного захисту: аналіз базових (ключових) законодавчих термінів та понять / М. В. Болотських,

С. О. Андреєв // Актуальні проблеми державного управління. − 2008. − Вип. 1 (33). − С. 16−22.

26. Бурков В. Н. Разработка механизмов управления риском чрезвычайных ситуаций / В. Н. Бурков, Б. П. Титаренко // Вестник МГСУ/ − 2017. – Т. 12. – Вып. 5 (104). – С. 559-563.

27. Бурков В. Н. Теория активных систем: состояние и перспективы / В. Н. Бурков, Д. А. Новиков. М.: Синтег, 1999. – 128 с.

28. 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. − С. 12.

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

30. Ведунг Е. Оцінювання державної політики та програм / Е. Ведунг. – К. : ВСЕУВИТО, 2003. – 350 с.

31. Вітлінський В. В. Ризикологія в економіці та підприємництві : монографія / В. В. Вітлінський, П. І. Великоіваненко. — К. : КНЕУ, 2004. — 480 с.

32. 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.

33. Вовченко С. Д. Розвиток теоретичних основ функціонування системи захисту населення і територій від надзвичайних ситуацій / С. Д. Вовченко // Економіка та держава. – 2013. – № 10. – С. 141–144.

34. Волошин С. М. Нормативно-правове забезпечення техногенно–природної безпеки / С. М. Волошин // Надзвичайна ситуація. – 2013. – № 1. – С. 33–35.

35. Волянський П. Б. Методологічні підходи до управління ризиками в

процесі ліквідації наслідків надзвичайних ситуацій / П. Б. Волянський // Інвестиції: практика та досвід. – 2013. – № 13. – С. 134–136.

36. Гиденс Э. Понятие риска / Э. Гиденс // THESIS. – 1994. – №5. – С. 40–102.

37. Глазунова Н. И. Система государственного управления : учеб. для вузов / Н. И. Глазунова. – М. : ЮНИТИ-ДАНА, 2003. – 551 с.

38. Глобальный индекс кибербезопасности [Электронный ресурс]. – Режим доступа : http://www.tadviser.ru/index.php

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

40. Головач Т. В. Ризик-менеджмент: зміст і організація на підприємстві / Т.В. Головач, А.Б. Грушевицька, В.В. Швид // Вісник Хмельницького національного університету. – 2010. - № 3. – Т.1. – С. 157-163.

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

42. Горбунов С. Анализ технологий прогнозирования чрезвычайных ситуаций / С. Горбунов, Ю. Макиев, В. Малышев // Стратегія цивільного захисту: проблеми та дослідження. – 2011. – № 1. – С. 43–47.

43. Гортенко І. О. Економічні райони України : посіб. / І. О. Гортенко, Л. Л. Тарангул. – К. : Вища школа, 1999. – 205 с.

44. Грачов В. Класифікація ризиків та управління ними / В. Грачов // Фінанси України. – 2002. – № 10. – С. 56–60.

45. Гур’єв С. Завдання кризового менеджменту й управління надзвичайними ситуаціями в державному управлінні / С. Гур’єв, Я. Радиш, А. Терент’єва // Університетські наукові записки : наук. зб. пр. – № 2 (30). –

2012. – С. 285–290.

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

47. Данилишин Б. В. Наукові основи прогнозування природно-техногенної безпеки / Б. В. Данилишин, В. В. Ковтун, А. В. Степаненко. – К. : ЛексДім, 2004. – 520 с.

48. Дєгтяр О. А. Державне та регіональне управління в соціальній сфері : монографія / за заг. ред. А. О. Дєгтяра. – Х. : С.А.М., 2015. – 552 с.

49. Державне управління : навч. посіб. / А. Ф. Мельник, Ю. О. Оболенський, А. Ю. Васіна, Л. Ю. Годієнко. – К. : Знання-Прес, 2003. – 343 с.

50. Державне управління : словник-довідник / заг. ред. В. М. Князєва, В. Д. Бакуменка. – К. : Видавництво УАДУ, 2002. – 228 с.

51. Державне управління в Україні : навч. посібн. / за заг. ред. В. Б. Авер'янова. – К. : Юрінком Інтер, 1998. – 432 с.

52. 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.

53. Державне управління: теорія і практика: навч. посіб. / за ред. В. Авер’янова. – К. : Юрінком-Інтер, 1998. – 431 с.

54. Державне управління і менеджмент : навч. посіб. у таблиця і схемах / Г. С. Одінцова, Г. І. Мостовий, О. Ю. Амосов та ін. – Х. : ХарРІДУ УАДУ, 2002. – 492 с.

55. Державне регулювання інноваційного розвитку економіки України: стратегічні пріоритети : монографія / М. А. Латинін, С. В. Майстро,

В. Ю. Бабаєв та ін. ; за заг. ред. д.держ.упр., проф. М. А. Латиніна. – Х. : Вид-во ХаРІДУ НАДУ «Магістр», 2014. – 320 с.

56. Джигирей В. С. Безпека життєдіяльності : навч. посіб. / В. С. Джигирей, В. Ц. Шидецький. – Львів: Афіша, 2000. – 256 с.

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

58. Дзюндзюк В. Б. Вплив надзвичайних ситуацій на соціально-економічний розвиток територій [Електронний ресурс] / В. Б. Дзюндзюк, Д. Ю. Полковниченко // Державне будівництво. − 2013. − № 2. – Режим доступу : http://www.kbuapa.kharkov.ua/e-book/db/2013-2/doc/2/01.pdf

59. Додонов О. Г. Інформаційно-аналітична підтримка прийняття управлінських рішень у кризових ситуаціях / О. Г. Додонов, В. Г. Путятін, В. О. Валетчик // Реєстрація, зберігання і обробка даних. – 2006. – Т. 8. – № 1. – С. 37–54.

60. Домарацький М. Б. Актуальні проблеми державного управління захистом критичної інфраструктури в Україні / М. Б. Домарацький // IV Всеукраїнська науково-практична конференція «Публічне управління та адміністрування у процесах економічних реформ»: збірник тез. –Херсон : Херсонський державний аграрно-економічний університет, 2020. – С. 159–161.

61. Домарацький М.Б. Аналіз загроз у процесі категоріювання об’єктів критичної інформаційної інфраструктури на державному рівні / М. Б. Домарацький // Інноваційне підприємництво, менеджмент, фінанси: стан, аналіз тенденцій та науково-економічний розвиток : матеріали міжнародної науково-практичної конференції. – Львів: ЛЕФ, 2019. – Ч. 2. – С. 104–105.

62. Домарацький М. Б. Впровадження державних заходів щодо антикризової діяльності відносно захисту регіональної критичної інфраструктури / М. Б. Домарацький // Інноваційний розвиток і підвищення рівня спроможності об'єднаних територіальних громад: матеріали науково-практичної конференції за міжнародною. − Дніпро : ДРІДУ НАДУ, 2019. – С. 74–75.

63. Домарацкий М. Б. Научные основы государственного управления критической инфраструктурой в Украине [Электронный ресурс] / М. Б. Домарацкий // East Journal of Security Studies. – 2018. – Вып. 1 (3). – Режим доступа : http://repositsc.nuczu.edu.ua/bitstream/123456789/10664/1/domaratskyejss.pdf

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

65. Домарацький М. Б. Методика державного категорування критично важливих об’єктів / М. Б. Домарацький // Держава та регіони. – 2019. − № 4(68). – С. 278 – 281. – (Серія «Державне управління»).

66. 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. – (Серія «Державне управління»).

67. Домарацький М. Б. Особливості імплементації міжнародного досвіду забезпечення безпеки критичної інфраструктури в українську практику державного управління / М. Б. Домарацький // Державне управління у сфері цивільного захисту: наука, освіта, практика: матеріали міжнародної науково-практичної інтернет-конференції. – Х. : НУЦЗУ, 2020. – С. 54–56.

68. 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.

69. Домарацький М. Б. Особливості формування та функціонування державної системи моніторингу стану об’єктів критичної інфраструктури / М. Б. Домарацький // Право та державне управління. – 2019. − № 4. – С. 170–174.

70. Домарацький М. Б. Реформування процесів державного управління критичною інфраструктурою / М. Б. Домарацький // Інформаційні технології: наука, техніка, технологія, здоров’я: тези доповідей XXVII науково-практичної конференції MicroCAD-2020. – Ч. IV. – Х. : НТУ «ХПІ», 2020. – (Здано до друку).

71. Домарацький М. Б. Специфіка державного регулювання критичної інфраструктури в Україні / М. Б. Домарацький // Публічне управління та митне адміністрування. – 2020. − № 2(25). – С. 74–75.

72. 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.

73. Домбровска С. М. Забезпечення ефективного державного управління підготовкою фахівців у сфері цивільного захисту: створення професійних стандартів / С. М. Домбровська // Теорія та практика державного управління. − 2012. – Вип. 4 (39). – С. 386–390.

74. Домбровська С. М. Механізми формування безпеки держави

[Електронний ресурс] / С. М. Домбровська, С. Т. Полторак // Теорія та практика державного управління і місцевого самоврядування. – 2015. – № 1. – Режим доступу: http://el-zbirn-du.at.ua/

75. Домбровська С. М. Проблеми та перспективи розвитку державного управління : монографія / С. М. Домбровська, О. О. Гусаров, Ю. Е. Дуднєва. – Х. : УІПА, 2014. – 172 с.

76. Дометрична допомога в умовах надзвичайних ситуацій : практичний посібник / П. Б. Волянський, С. О. Гур'єв, М. Л. Долгий та ін. − Х. : ФОП Панов А. М., 2016. – 136 с.

77. 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.

78. 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.

79. Енциклопедія державного управління: у 8 т. / Нац. акад. держ. упр. при Президентові України ; наук.-ред. колегія : Ю. В. Ковбасюк (голова) та ін. – К. : НАДУ, 2011. Т. 2 : Методологія державного управління / наук.-ред. колегія : Ю. П. Сурмін (співголова), П. І. Надолішній (співголова) та ін. – 2011. – 692 с.

80. Ефективність державного управління / Ю. Бажал, О. Кілієвич, О. Мертенс та ін. ; за заг. ред. І. Розпутенка. – К. : К.І.С., 2002. – 420 с.

81. Європейський цивільний захист [Електронний ресурс]. – Режим доступу : http://ec.europa.eu/ environment/civil/prote/cp10_en.htm

82. 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.

83. Жукова Л. А. Основні стратегічні напрямки державного управління ризиками // Зб. наук. праць УАДУ / За заг. ред. В. І. Лугового, В. М. Князева. – К. : Вид-во УАДУ. – 2002. – Вип. 2. – С. 120–129.

84. Зарубежный опыт и перспективы аудита безопасности [Електронний ресурс] // Бібліотека Експерта 112. – Режим доступу: http://expert112.com.ua/zarubezhnyij-opyit-i-rossijskie-perspektivyi-audita-bezopasnosti/index.html

85. 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

86. 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

87. 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

88. 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

89. 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

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

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

91. 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

92. 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

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

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

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

96. Зеркалов Д. В. Наукові основи цивільного захисту : монографія / Д. В. Зеркалов, М. Д. Кацман, А. І. Ковтун / за редакцією Д. В. Зеркалова. – К. : Основа. 2014. – 1117 с.

97. Іванець Г. В. Алгоритм прогнозування надзвичайних ситуацій соціального характеру за видами та рівнями, можливих завданих збитків внаслідок них / Г. В. Іванець // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2016. – № 4 (49). – С. 173–176.

98. Іванюта С.П. Запровадження сучасних підходів для зниження ризику природних катастроф в Україні // Стратегічні пріоритети. – 2016. – №1 (38). – С.110–117.

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

100. Карамишев Д. В. Публічне управління як специфічний вид управлінської діяльності в умовах суспільних трансформацій / Д. В. Карамишев, В. П. Прасол // Інвестиції: практика та досвід. – 2014. – № 24. – С. 156-160.

101. Капля А. М. Удосконалення державного управління систем запобігання й реагування на надзвичайні ситуації в Україні з використанням досвіду зарубіжних країн: проблеми та перспективи / А. М. Капля, В. С. Чубань, О. Г. Снісар // Пожежна безпека: теорія і практика. – 2013. – № 14. – С. 39–46.

102. Класифікатор надзвичайних ситуацій ДК 019:2010 : Наказ Державного комітету з питань технічного регулювання та споживчої політики від 11.10.2010 р. № 457 [Електронний ресурс]. – Режим доступу: http://www.lnu.edu.ua/faculty/bzh/ZO/DK_019–2010.pdf

103. Коваль О. П. Соціальна безпека: сутність та вимір : наук. доп. / О. П. Коваль. – К. : НІСД, 2016. – 34 с.

104. Кодекс цивільного захисту України : Закон України від 02.10.2012 р. № 5403–VI [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/5403–17

105. Козьменко О. В. Фінансові методи управління катастрофічними ризиками / О. В. Козьменко, О. М. Пахненко // Актуальні проблеми економіки. – 2011. – № 4. – С. 217–224.

106. Колодій А. М. Теорія держави і права : навч. посіб. / А. М. Колодій, В. В. Копєйчиков, С. Л. Лисенков та ін. ; за заг. ред. С. Л. Лисенкова, В. В. Копєйчикова. – К. : Юрінком Інтер, 2002. – 368 с.

107. Корченко А. О. Метод оцінки рівня критичності для систем

управління кризовими ситуаціями. Захист інформації / А. О. Корченко, В. А. Козачок, А. І. Гізун. – 2015. – № 1. − Т. 17. – С. 86–98.

108. Костин А. Эффективность мер по снижению опасности при чрезвычайных ситуаціях / А. Костин // Проблеми безпеки при надзвичайних ситуаціях, 1997. – Вип. 10. – С. 34-37.

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

110. Коротич О.Б. Державне управління регіональним розвитком України : монограф. / О.Б. Коротич. – Х. : Вид-во ХарРІ НАДУ «Магістр», 2006. – 220 с.

111. Костенко В. Модернізація державної системи цивільного захисту в контексті європейської інтеграції України / В. Костенко // Державне управління та місцеве самоврядування. – 2013. – Вип. 4 (19). – С. 107–115.

112. Костенко В. О. Характеризація державного управління захистом населення у надзвичайних ситуаціях : автореф. дис.… канд.. держ. упр. : 25.00.01 / В. О. Костенко ; ДРІДУ НАДУ при Президентові України, Дніпропетровськ, 2016. – 20 с.

113. Косяченко С. А. Модели, методы и автоматизация управления в условиях чрезвычайных ситуаций / С. А. Косяченко, Н. А. Кузнецов, В. В. Кульба, А. Б. Шелков // Автоматика и телемеханіка. – 1998, № 6, С. 3−6.

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

115. Кризовий менеджмент та принципи управління ризиками в процесі ліквідації надзвичайних ситуацій : монографія / С. О. Гур’єв, А. В. Терент’єва, П. Б. Волянський. – К. : б. в., 2008. – 148 с.

116. Кравчук М. В. Теорія держави і права (опорні конспекти) : навч. посіб. для студ. вищ. навч. закл. / М. В. Кравчук. – К. : Атіка, 2003. – 288 с.

117. Кравців С. Я. Ризик-орієнтований підхід у державному регулюванні у сфері техногенної та пожежної безпеки / С. Я. Кравців, О. М. Соболь, А. Г. Коссе // Вісник Національного університету цивільного захисту України. Серія. Державне управління. – 2017. – Вип. 1 (6). – С. 336–341.

118. 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.

119. Криштанович М. Ф. Реалізація механізмів публічного управління у сфері цивільного захисту України щодо національної безпеки / М. Ф. Криштанович // Вісник Національного університету цивільного захисту України. Серія. Державне управління. – 2017. – Вип. 1 (6). – С. 341–347.

120. Кузніченко С. О. Державне управління у надзвичайних ситуаціях: проблеми правового забезпечення / С. О. Кузніченко // Юридичний вісник. – 2010. – № 3. – С. 52–56.

121. Кулєшов М. М. Система реагування на надзвичайні ситуації та механізми управління / М. М. Кулєшов // Вісник Національного університету цивільного захисту України. – 2017. – Вип. 1 (6). – С. 314–322. – (Серія: Державне управління)

122. Курашвили Б. П. Очерк теории государственного управления / Б. П. Курашвили. – М. : Наука, 1987. – 294 с.

123. Кутинов О. Гражданская оборона в странах НАТО / О. Кутинов // Зарубежное военное обозрение. – 2012. – №5. – С.12–19.

124. Лазор О. Д. Основи державного управління та місцевого

самоврядування : навч. посіб. / О. Д. Лазор, О. Я. Лазор, І. Г. Лазор. – К. : Дакор, 2007. – 312 с.

125. Лапін В. Безпека життєдіяльності людини : навч. посіб. / В. Лапін. – К. : Знання, 2007, – 332 с.

126. 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.

127. Ліпкан В. А. Національна безпека та національні інтереси України / В. А. Ліпкан. – К. : КНТ, 2006. – 68 с.

128. Ліхачов С. Національна безпека України як об'єкт державного управління / С. Ліхачов // Право України. – 2009. – № 10. – С. 182–189.

129. 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.

130. Лопанов А. Н. Мониторинг и экспертиза безопасности жизнедеятельности / А. Н. Тимофеев, Е. В. Климова. – Белгород : Изд-во БГТУ, 2009. – 201 с.

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

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

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

134. Майстро С. В. Теоретичні засади механізму державного управління системою цивільного захисту / С. В. Майстро // Теорія та практика державного управління. – 2014. – Вип. 3. – С. 3−10.

135. Малеван О. Ю. Напрями удосконалення сфери цивільного захисту держави Тищенко [Електронний ресурс] / О. Ю. Малеван, Ю. П. Переверзін // Державне управління: удосконалення та розвиток. − 2012. − № 11. − Режим доступу: http://www.dy.nayka.com.ua

136. Малинецкий Г. Г. Теория риска и технологии обеспечения безопасности. Подход с позиций нелинейной динамики / Ю. Л. Воробьев, Г. Г. Малинецкий, Н. А. Махутов // Проблемы безопасности при чрезвычайных ситуаціях, 1999. – Вып. 1. – С. 19−24.

137. Малиновський В. Я. Державне управління: навч. посіб. / В. Я. Малиновський. – К. : Атіка, 2003. – 576 с.

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

139. Марцинковский Д. Обзор основных аспектов риск-менеджмента / Д. Марцинковский // Das Management. – 2009. – № 1/11– 12. – С. 54–59.

140. Маслов Є. П. Державна політика у сфері цивільного захисту України в умовах надзвичайних ситуацій [Електронний ресурс] / Є. П. Маслов. – Режим доступу : www.zerkalov.kiev.ua

141. 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.

142. Медичний та біологічний захист за умов надзвичайних ситуацій : навч. посіб. / М. Д. Близнюк, П. Б. Волянський, М. Т. Гафарова та ін. – Х. : ФОП Панов А.М., 2016. – 324 с.

143. Мезенцева О. М. Аналіз надзвичайних ситуацій в Україні за характером та наслідками / О. М. Мезенцева // Наукові записки. – 2014. – Вип. 15. – С. 130–133.

144. 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.

145. 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.

146. Мельтюхова Н. М. Технологія державного управління : навч. посіб. / За заг. ред. Г. І. Мостового, О. Ф. Мельникова. – Х. : Вид-во ХарРІ НАДУ «Магістр», 2005. – 152 с.

147. Методичні рекомендації з питань організації та реалізації заходів цивільного захисту в органах виконавчої влади на підприємствах, в установах і організаціях [Електронний ресурс]. – К. : ДСНС України, 2015. – Режим доступу: http://undicz.dsns.gov.ua/files/2015/8/11/Metod_rekomendaciyi.pdf

148. 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....

149. Михайлов С. Состояние и перспективы развития гражданской обороны Франции / С. Михайлов // Зарубежное военное обозрение. – 2013. – № 6. – С. 15–21.

150. Михайлюк О. В. Цивільний захист : навчальний посібник. Ч.1. Соціальна, техногенна та природна безпеке / О. В. Михайлюк. – Миколаїв : НУК, 2005. – 136 с.

151. Мишин В. Исследование систем управления : учеб. для вузов / В. Мишин. – М. : ЮНИТИ-ДАНА, 2003. – 162 с.

152. Могил С. Держава як суб’єкт попередження і ліквідації наслідків аварій і катастроф / С. Могил // Актуальні проблеми держави та права. – Вип. 6. – Ч. II, 2009. – С. 107–114.

153. Моделі ефективності державного управління : монографія / В. С. Загорський, М. Д. Лесечко, Р. М. Рудніцька та ін. – Львів : ЛРІДУ НАДУ, 2010. – 100 с.

154. Мороз В. М. Розвиток громадянського суспільства: взаємозобов'язання і взаємовідповідальність між основними учасниками соціального діалогу / В. М. Мороз // Вісник Національного університету цивільного захисту України. − 2014. − Вип. 2. − С. 14−22. – (Серія: Державне управління).

155. Надолішній П. Організаційно-функціональна структура державного управління: поняття і соціальна практика / П. Надолішній // Вісн. НАДУ. – 2003. – № 3. – С. 31–43.

156. 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.

157. 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.

158. Нікітін Ю. В. Теоретико-правовий підхід до визначення загроз як детермінуючих чинників впливу на національну безпеку України / Ю. В. Нікітін // Держава і право. Юридичні і політичні науки. – 2008. – Вип. 41. – С. 502–508.

159. Нижник Н. Р. До проблеми ефективності державного управління в Україні / Н. Р. Нижник // Підвищення ефективності державного управління: стан, перспективи та світовий досвід : зб. наук. пр. К. : Вид-во УАДУ, 2000. – С. 6–11.

160. Нижник Н. Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку) / Н. Р. Нижник, Г. П. Ситник, В. Т. Білоус. – Ірпінь : Акад. ДПС України, 2000. – 304 с.

161. Нормативно-правова база у галузі безпеки і оборони України / заг. ред.: А. Гриценко, А. Єрмолаєв, Ф. Флурі. – К. : Центр дослідж. армії, коверсії та роззброєння, 2012. – 800 с.

162. Оболонский А.В. Человек и государственное управление / А.В. Оболонский, М.И. Пискотин. – М. : Наука, 1987. – 252 с.

163. Одінцова Г. С. Теорія і історія державного управління : опорний конспект лекцій і методичні вказівки до проведення практичних занять / Г. С. Одінцова, Н. М. Мельтюхова. – Х. : УАДУ, 2001. – 136 с.

164. Одокієнко С. М. Аналіз виникнення надзвичайних ситуацій техногенного та природного характеру в Україні / С. М. Одокієнко, Л. А. Тарандушка, І. А. Жирякова // Пожежна безпека: теорія і практика. – 2013. – №15. – С. 115−123.

165. Олійник А.Ю. Теорія держави і права : навч. посіб. / А.Ю. Олійник, С.Д. Гусарєв, О.Л. Слісаренко. – К. : Юрінком Інтер, 2001. – 176 с.

166. Організація цивільного захисту під час реформування місцевого самоврядування та територіальної організації влади в Україні : практичний порадник / О. Я. Лещенко, В. М. Михайлов, Н. М. Романюк, В. О. Скакун ; за заг. редакцією М. О. Маюрова, П. Б. Волянського. − К. : ІДУЦЗ, 2017. − 127 с.

167. Осипов Е. А. Правовое обеспечение безопасности в чрезвычайных

ситуациях : учеб. пособ. / Е. А. Осипов. – М. : МГИУ, 2012. – 199 с.

168. Основы национальной безопасности / М. И. Абдурахманов, В. А. Баришполец, В. Л. Манилов, В. С. Пирумов. – М. : Друда, 1998. – 327 с.

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

170. Пал Л. А. Аналіз державної політики / Л. А. Пал. – К. : Основи, 1999. – 422 с.

171. Панфилова Э.А. Понятие риска: многообразие подходов и определений / Э.А. Панфилова // Теория и практика общественного развития. – 2010. – № 4. – С. 30–34.

172. 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.

173. Полковниченко Д. Державна політика у сфері попередження надзвичайних ситуацій на основі концепції ризиків [Електронний ресурс] / Д. Полковниченко // Теорія та практика державного управління. – 2013. – № 4. – Режим доступу: http://www.kbuapa.kharkov.ua/e–book/conf/2013–4/doc/3.pdf

174. Полковниченко Д. Ю. Особливості формування системи державного управління в умовах безпеки та надзвичайних ситуаціях / Д. Ю. Полковниченко // Теорія та практика державного управління і місцевого самоврядування. – 2016. – № 2. – Режим доступу: http://nbuv.gov.ua/UJRN/Ttpdu_2016_2_23

175. Пономаренко Г. О. Управління у сфері забезпечення внутрішньої безпеки держави: адміністративно-правові засади : монографія / Г. О. Пономаренко. – Х. : Вид. СПД ФО Вапнярчук Н. М., 2007. – 448 с.

176. Пономаренко С. С. Науково-теоретичний аналіз впливу НС на соціально-економічний розвиток: загальнодержавний і локально-територіальний рівні / С. С. Пономаренко, А. В. Максимов // Вісник Національного університету цивільного захисту України. Серія. Державне управління. – 2017. – Вип. 1 (6). – С. 322–328.

177. Порфирьев Б. Н. Управление безопасностью в природно-техногенной сфере на основе концепции риска / Б. Н. Порфирьев // Управление риском. – 2002. – № 2. – С. 36–42.

178. Порфілов О. Підходи до розроблення та прийняття управлінських рішень в умовах невизначеності та ризику // Вісник Нац. ун-ту «Львівська. політехніка». – 2016. – № 855. – С. 218–224. – (Серія: Юридичні науки).

179. Порядочний Л. В. Безпека в надзвичайних ситуаціях та цивільна оборона : навч. посіб. / Л. В. Порядочний, В. М. Заплатинський. – К. : Київ. нац. торгов.-екон. ун-т, 2003. – 301 с.

180. Практичний порадник з реалізації основних заходів цивільного захисту в умовах реформування місцевого самоврядування та територіальної організації влади в Україні / М. В. Білошицький, О. Я. Лещенко, В. І. Мазуренко, та ін. ; за заг. ред. П. Б. Волянського. К. : ІДУЦЗ, 2016. – 64 с.

181. Приходченко Л. Л. Забезпечення ефективності державного управління: теоретико-методологічні засади : монографія / Л. Л. Приходченко. – Одеса : Вид-во Оптимум, 2009. – 299 с.

182. Природні та техногенні загрози, оцінювання небезпек : навч. посіб. / В. А. Андронов, А. С. Рогозін, О. М. Соболь та ін. – Х. : Вид-во НУЦЗУ, 2011. – 264 с.

183. Приходько В. М. Потенційно небезпечні об'єкти – як фактор дестабілізації / В. М. Приходько // Системи обробки інформації. – 2014. – № 7. –

С.45–47.

184. 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.

185. Про Основні засади (стратегію) державної екологічної політики України на період до 2020 року [Електронний ресурс] : Закон України від 21.12.2010 № 2818-VI. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2818-17

186. Про Стратегію сталого розвитку «Україна – 2020» [Електронний ресурс] : Указ Президента України від 12.01.2015 р. № 5/2015. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/5/2015

187. Про схвалення Концепції національної екологічної політики України на період до 2020 року [Електронний ресурс] : Розпорядження Кабінету Міністрів України від 17.10.2007 р. № 880-р. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/880-2007-%D1%80

188. Про схвалення Концепції управління ризиками виникнення надзвичайних ситуацій техногенного та природного характеру [Електронний ресурс] : Розпорядження Кабінету Міністрів України від 22.01.2014 р. № 37-р. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/37-2014-%D1%80

189. 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

190. Проневич О. С. Державне управління у надзвичайних ситуаціях: концептуально-правовий базис та інституційна надбудова / О. С. Проневич // Форум права. – 2015. – № 5. – С. 186–193.

191. Публічне адміністрування в Україні : навч. посіб./ В. Б. Дзюндзюк, О. Б. Коротич, Н. М. Мельтюхова та ін.. – Х. : Вид-во ХарРІ НАДУ «Магістр», 2012. – 256 с.

192. Радиш Я. Ф. Досвід взаємодії міжнародних цивільно-військових сил при ліквідації наслідків надзвичайних ситуацій / Я. Ф. Радиш, А. В. Терентьєва // Держава та регіони. – 2009. – № 2. – С. 157–160.

193. Райт Г. Державне управління / Г. Райт. – К. : Основи, 1994. – 432 с.

194. Рейтинг стран по уровню кибербезопасности [Электронный ресурс]. – Режим доступа : https://nonews.co/directory/lists/countries/cybersecurity-index

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

196. Романюк О. Д. Методи економіко-статистичного аналізу : навч. посіб. / О. Д. Романюк. – К. : УАДУ, 1997. – 144 с.

197. Ромін А. Методологічні засади державного управління сферою захисту населення і територій від надзвичайних ситуацій / А. Ромін, Р. Приходько // Публічне управління: теорія та практика : зб. наук. пр. – Х. : Вид-во ДокНаукДержУпр., 2013. – № 4. – С. 41–47.

198. Рудніцька Р. М. Механізми державного управління: сутність і зміст / Р. М. Рудницька, О. Г. Сидорчук, О. М. Стельмах ; за наук. ред. д.е.н., проф. М. Д. Лесечка, к.е.н., доц. А. О. Чемериса. – Львів : ЛРІДУ НАДУ, 2005. – 28 с.

199. Русецький А. А. Аналіз стану загроз критичній інфраструктурі в Харківській області / А. А. Русецький // Актуальні проблеми вітчизняної юриспуденції. – 2017. – 2017. - № 1. – Т. 2. – С. 18–20.

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

201. Садковий В. П. Державне управління у сфері цивільного захисту в Україні: нормативно-правовий аспект : монографія / В. П. Садковий, А. В. Ромін, О. О. Островерх, С. М. Домбровська. – Х. : ТОВ «Оберіг», 2013. – 190 с.

202. Садковий В. П. Уніфікація механізмів державного управління професійною підготовкою кадрів цивільного захисту в Україні : автореф. дис. ... д-ра наук з держ. упр. : 25.00.02 / В. П. Садковий. – Чорномор. держ. ун-т ім. Петра Могили. – Миколаїв, 2014. – 36 с.

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

204. Семенченко А. І. Механізм стратегічного управління забезпеченням національної безпеки у кризових та надзвичайних ситуаціях [Електронний ресурс] / А. І. Семенченко. – Режим доступу: http://old.niss.gov.ua/book/StrPryor/2/6-3-Semenchenko.pdf

205. Скакун О. Ф. Теория права и государства : учеб. / О. Ф. Скакун, Н. К. Подберезский. – Харків : Юринком Інтер, 1997. – 500 с.

206. Ситник Г. П. Національна безпека України: теорія і практика / Г. П. Ситник, В. М. Олуйко, М. П. Вавринчук. – К. : Кондор, 2007. – 616 с.

207. Скрипник О. А. Сучасні тенденції формування системи державного управління у сфері цивільного захисту населення від надзвичайних ситуацій в Україні [Електронний ресурс] / О. А. Скрипник // Державне управління та місцеве самоврядування. − 2015. – № 2 (14). – Режим доступу: http://www.dridu.dp.ua/zbirnik/2015-02(14)/14.pdf.

208. Служба безпеки України (офіційний сайт) [Електронний ресурс]. – Режим доступу : https://www.ssu.gov.ua/

209. Смірнова О. Виробничий ризик: сутність і управління /

О. Смірнова // Управління ризиком. – 2001. – № 2. – С. 20–23.

210. Сморгунов Л. Государственная политика и управление : учебник : в 2 ч. / Л. Сморгунов, А. Альгин, И. Барыгин и др. ; под ред. Л. Сморгунова. – Ч. 1: Концепции и проблемы государственной политики. – М. : РОССПЭН, 2006. – 381 с.

211. Соболь О. М. Організаційно-правовий механізм державного управління у сфері захисту населення і територій від надзвичайних ситуацій [Електронний ресурс] / О. М. Соболь, Р. В. Приходько. – Режим доступу: http://www.kbuapa.kharkov.ua/e-book/db/20122/doc/2/13.pdf

212. Соха Ю. І. Організаційно-економічні механізми управління природо-техногенною безпекою : автореф. дис.… к. держ. упр. : 25.00.02 / Ю. І. Соха ; ЛРІ НАДУ при Президентові України, Львів, 2017. – 20 с.

213. Соціально-економічний аналіз надзвичайних ситуацій природного та техногенного характеру / С. М. Волошин, Л. В. Жарова, Є. В. Хлобистов та ін.; за науковою редакцією д.е.н. проф. Є. В. Хлобистова. – Сімферополь : НДІ СРП, 2010. – 258 с.

214. 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.

215. Старостіна А. О. Ризик-менеджмент: теорія та практика : навч. посіб. / А. О. Старостіна, В. А. Кравченко. – К. : Видавництво «Політехніка», 2004. – 200 с.

216. Стеблюк М. І. Цивільна оборона та цивільний захист : підручник / М. І. Стеблюк. – К. : Знання, 2010. – 487 с.

217. Стратегія і тактика національної безпеки: зарубіжний досвід, проблеми та перспективи України / за заг. ред. В. П. Горбуліна. – К. : Нац. центр з питань євроатлант. інтеграції, 2006. – 304 с.

218. Стрельцов В. Ю. Розвиток публічної служби України в умовах біпатризму / В. Ю. Стрельцов // Теорія та практика державного управління. Збірник наукових праць. – Х.: Вид-во ХарРІ НАДУ "Магістр", 2010. – Вип. 4 (31). – С. 394−398.

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

220. Суходоля О. М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України / О. М. Суходоля // Стратегічні пріоритети. – 2016. − № 3(40). – С. 62–76.

221. Теоретико-методологічні засади державного управління: формування понятійного апарату : метод. рек. / В. В. Корженко, В. В. Говоруха, О. Ю. Амосов та ін. ; за заг.ред. В. В. Корженка. – К. : НАДУ, 2009. – 56 с.

222. Теоретичні та організаційно-методичні засади проектування освітньої діяльності навчально-методичних установ цивільного захисту : монографія / Є. Ю. Литвиновський, В. В. Бегун, С. В. Гелдаш та ін. – Львів : Кругозір, 2017. – 230 с.

223. Теорія держави і права : навч. посіб. / А. М. Колодій, В. В. Копєйчиков, С. Л. Лисенков та ін. ; за заг. ред. С. Л. Лисенкова, В. В. Копєйчикова. – К. : Юрінком Інтер, 2002. – 368 с.

224. Теорія держави і права. Академічний курс : підруч. / ред. О. В. Зайчук, Н. М. Оніщенко. – К. : ЮрІнтер, 2006. – 688 с.

225. Терехов Л. Экономико-математические методы / Л. Терехов. – М. : Статистика, 1972. – 342 с.

226. Титаренко А. В. Методологічні засади державного управління сферою захисту населення і територій від надзвичайних ситуацій / А. В. Титаренко // Вісник Національного університету цивільного захисту України. – 2016. – Вип. 1 (4). – С. 216–222. – (Серія : Серія. Державне управління).

227. Тренды кибербезопасности [Электронный ресурс]. – Режим доступа : http://www.tadviser.ru/index.php

228. Труш О. О. Досвід побудови та функціонування систем цивільного захисту країн-членів європейського союзу Південної Європи / О. О. Труш // Теорія та практика державного управління. – 2010. – № 1. – С. 112–123.

229. Український соціум: загрози екстремальних ситуацій : монографія / Г. В. Рева, В. К. Врублевський, В. П. Ксьонзенко ; за ред. В. К. Врублевського. – К. : Інтелект, 2003. – 432 с.

230. Усаченко Л. М. Історія державного управління в Україні : навч. посіб. / Л. М. Усаченко, В. І. Тимцуник. – К. : ТОВ «НВП «Інтерсервіс», 2013. – 292 с.

231. Хохлов Н. В. Управление риском : учеб. пособ. для вузов / Н. В. Хохлов. – М. : ЮНИТИ-ДАНА, 1999. – 239 с.

232. Федоренко В. Н. Гражданская оборона зарубежных государств. Международная организация гражданской обороны / В. Н. Федоренко. − М. : ООО “ИПП “КУНА”, 2003. − С. 275−294.

233. Федулов Г. В. Зарубежный опыт создания и обеспечения функционирования систем предупреждения и ликвидации чрезвычайных ситуаций / Г. В. Федулов // Проблемы безопасности при чрезвычайных

ситуациях. − 1998. − Вып. 8. − С. 63−100.

234. Фещур Р. В. Статистика: теоретичні засади і прикладні аспекти : навч. посіб. / Р. В. Фещур, А. Ф. Барвінський. – Львів : Інтелект-Захід, 2003. – 576 с.

235. 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.

236. Харламов В. В. Теоретичні засади державного управління вищою освітою у сфері цивільного захисту / В. В. Харламов // Вісник Національного університету цивільного захисту України. Серія. Державне управління. – 2017. – Вип. 1 (6). – С. 69–75.

237. Харченко С. Некоторые аспекты подготовки специалистов и руководителей в области анализа риска / С. Харченко, А. Прохожев // Управление риском. – 1997. – № 4. – С. 15–22.

238. Харчук А. І. Організація управління у надзвичайних ситуаціях [Електронний ресурс] / А. І. Харчук, Р. Ю. Сукач, М. Я. Колісник. – Режим доступу:http://ubgd.lviv.ua

239. 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.

240. Чечель А. О. Передумови удосконалення економічного механізму природокористування в Україні / А. О. Чечель // Збірник наукових праць Донецького державного університету управління. – Том XI. – Випуск 149 «Управління економічним розвитком промислових підприємств». – 2010. – С.80−87. – (Серія «Економіка»).

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

242. Човушян Э. Управление риском и устойчивое развитие : учеб. пособ. для экон. вузов / Э. Човушян, М. Сидоров. – М. : Изд-во РЭА имени Г. В. Плеханова, 1999. – 63 с.

243. Чуб И. А. Моделирование системы мониторинга техногенной безопасности региона / И. А. Чуб, В. М. Попов // Открытые информационные и компьютерные интегрированные технологии : сб. научн. тр. – 2012. – Вып. 56. – С. 157–161.

244. Шаптала В. Г. Основы моделирования чрезвычайных ситуаций : учебное пособие / В. Г. Шаптала, В. Ю. Радоуцкий, В. В. Шаптала. – Белгород, 2010. – 166 с.

245. Шахов В. Національний інтерес і національна безпека в геостратегії України / В. Шахов, В. Мадіссон // Вісник Національної академії державного управління при Президентові України. – 2013. – № 2. – С. 44–56.

246. Шевцов А. Реформування системи цивільного захисту населення відповідно до завдань європейської та євроатлантичної інтеграції / А. Шевцов, О. Їжак. – Режим доступу : http://www.niss.gov.ua/Monitor/mart2009/3.htm

247. Шоботов В. М. Цивільна оборона : навчальний посібник / В. М. Шоботов. – Київ : Центр навчальної літератури, 2006. – 438 с.

248. 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.

249. Якимчук А. Ю. Публічне адміністрування : навч. пособ. / А. Ю. Якимчук, О. М. Корецький. – Донецьк : Юго-Восток, 2014. – 224 с.

250. Яковлев С. Ю. Методологические проблемы анализа риска в

сложных системах / С. Ю. Яковлев, А. Я. Фридман // Информационные технологии в региональном развитии. – 2008. – Вып. VIII. – С. 69–72.

251. International Telecommunication Union [Електронний ресурс]. – Режим доступу : https://www.itu.int/ru/Pages/default.aspx

ДОДАТКИ

ВОЛИНСЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ
ДЕПАРТАМЕНТ ІНФРАСТРУКТУРИ
м-н Київський,9, м. Луцьк, 43027, тел. (0332) 778255, e-mail: ukb@gukb.voladm.gov.ua код ЄДРПОУ 42304390

14.05.2019р. № 294/01-17/2-19 на № _____ від _____

ДОВІДКА
про використання результатів дисертаційного дослідження Домарацького Михайла Богдановича «Державна безпека критичної інфраструктури в Україні»

У дисертації Домарацького М.Б. вирішується соціально значуще науково-практичне завдання щодо вдосконалення процесів державного регулювання критичної інфраструктури.

Дисертаційне дослідження Домарацького М.Б. має суттєву значущість стосовно теоретичного підходу до державної протидії стратегічним ризикам і загрозам для критичної інфраструктури, який, на відміну від існуючих, передбачає пріоритетну реалізацію системного комплексу організаційних, технічних, фінансових та інших заходів попереджувального та реагувального характеру, які виробляються на основі експертно- аналітичних методів вирішення ряду взаємопов'язаних завдань щодо ідентифікації, оцінки та ранжування часткових та інтегральних стратегічних загроз критичній інфраструктурі на загальнодержавному та регіональному рівнях за наявності політичного, правового, інституційного, адміністративного, економічного, науково- технічного та техніко-технологічного забезпечення.

На особливу увагу заслуговують запропонована послідовність етапів забезпечення функціональності системи раннього попередження прояву кризових ситуацій в якості аналітичного процесу.

Перспективність застосування висновків і пропозицій автора дисертаційного дослідження у практичній діяльності не викликає сумнівів враховуючи їх актуальність і змістовність.

Т.в.о. директора Віктор Довгополюк

ДЕРЖАВНА АУДИТОРСЬКА СЛУЖБА УКРАЇНИ
ЗАХІДНИЙ ОФІС ДЕРЖАУДИТСЛУЖБИ
УПРАВЛІННЯ ЗАХІДНОГО ОФІСУ ДЕРЖАУДИТСЛУЖБИ У ВОЛИНСЬКІЙ ОБЛАСТІ
пр-т Президента Грушевського, 3-А, м. Луцьк, 43005, тел. (0332) 77 09 20,
E-mail:volyn@dkrs.gov.ua Код ЄДРПОУ ВП № 40913671

14.05.2020 №13-03-09-14/1592-2020

ДОВІДКА
про використання результатів дисертаційного дослідження Домарацького Михайла Богдановича «Державна безпека критичної інфраструктури в Україні»

У дисертації Домарацького М.Б. вирішується соціально значуще науково-практичне завдання щодо вдосконалення процесів державного регулювання критичної інфраструктури.

Дисертаційне дослідження Домарацького М.Б. має суттєву значущість стосовно теоретичного підходу до державної протидії стратегічним ризикам і загрозам для критичної інфраструктури, який, на відміну від існуючих, передбачає пріоритетну реалізацію системного комплексу організаційних, технічних, фінансових та інших заходів попереджувального та реагувального характеру, які виробляються на основі експертно-аналітичних методів вирішення ряду взаємопов'язаних завдань щодо ідентифікації, оцінки та ранжування часткових та інтегральних стратегічних загроз критичній інфраструктурі на загальнодержавному та регіональному рівнях за наявності політичного, правового, інституційного, адміністративного, економічного, науково- технічного та техніко-технологічного забезпечення.

На особливу увагу заслуговують запропонована послідовність етапів забезпечення функціональності системи раннього попередження прояву кризових ситуацій в якості аналітичного процесу.

Перспективність застосування висновків і пропозицій автора дисертаційного дослідження у практичній діяльності не викликає сумнівів враховуючи їх актуальність і змістовність.

Начальник Управління
Західного офісу Держаудитслужби
у Волинській області,
кандидат економічних наук Анатолій ОМЕЛЬЧУК

Дата: 21.11.2019 р.

ЗАТВЕРДЖУЮ

Проректор з навчальної та методичної роботи
Національного університету
цивільного захисту України
_____ О.О. Назаров
«__» _____ 2019 р.

АКТ

про впровадження результатів дисертаційного дослідження здобувача Навчально-науково-виробничого центру Національного університету цивільного захисту України Домарацького Михайла Богдановича на тему: «Державне управління забезпеченням безпеки критичної інфраструктури в Україні» на здобуття наукового ступеня кандидата наук за державного управління за спеціальністю 25.00.05 – державне управління у сфері державної безпеки та охорони громадського порядку.

Комісія у складі:

Голова – начальник навчально-науково-виробничого центру, доктор наук з державного управління, професор Домбровська С.М.

Члени комісії – завідувач кафедри публічного адміністрування у сфері цивільного захисту, д.держ.упр., проф. Майстро С.В.; провідний науковий співробітник наукового відділу з проблем управління у сфері цивільного захисту, д.держ.упр., проф. Стрельцов В.Ю.; професор кафедри публічного адміністрування у сфері цивільного захисту, д.держ.упр., проф. Крюков О.І.

цим актом засвідчують, що результати дисертаційного дослідження Домарацького М.Б. на тему: «Державне управління забезпеченням безпеки критичної інфраструктури в Україні» (поглиблення категоріально-понятійного апарату, розроблення принципово нового підходу до вдосконалення державної системи захисту критичної інфраструктури) використовуються при викладанні навчальних дисциплін: «Управління соціальним і гуманітарним розвитком» та «Державна політика у сфері екологічної безпеки» за програмою підготовки магістрів публічного управління та адміністрування у Національному університеті цивільного захисту України.

Голова комісії
д.держ.упр., професор С.М. Домбровська

Члени комісії
д.держ.упр., професор С.В. Майстро
д.держ.упр., професор В.Ю. Стрельцов
д.держ.упр., професор О.І. Крюков