НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

УДК 351.862.4

Домбровська С.М., Шведун В.О.

МОНОГРАФІЯ

БЕЗПЕКА КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ: ТЕОРЕТИКО-ПРИКЛАДНІ ЗАСАДИ ДЕРЖАВНОГО УПРАВЛІННЯ

Харків – 2024

Монографію розглянуто та рекомендовано до друку Вченою Радою
Національного університету цивільного захисту України
Протокол № 7 від 07.03.2024

Рецензенти:

Драган І.О. - завідувач кафедри права та правоохоронної діяльності Державного університету «Житомирська політехніка», доктор наук держ.упр, професор;

Белай. С.В. – заступник начальника навчально-методичного центру-начальник відділу методичного забезпечення навчального процесу Національної академії Національної гвардії України, доктор наук з державного управління, професор

Безпека критичної інфраструктури в Україні: теоретико-прикладні засади державного управління: монографія / С. М. Домбровська, В.О. Шведун. Харків, НУЦЗУ. 2024. 227 с.

У монографії вирішено наукове завдання, обґрунтовано теоретичні засади та розроблено науково-практичні рекомендації щодо вдосконалення процесів державного управління забезпеченням безпеки критичної інфраструктури, зокрема, під час повномасштабного російського вторгнення та протягом перспективного періоду післявоєнного відновлення.

Інформаційну базу 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.

Домбровська С.М.
Шведун В.О.

УДК 351.862.4

ЗМІСТ

ВСТУП

Актуальність теми. Наразі існує необхідність переосмислити спектр та характер загроз, що проявляються як стосовно 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, насамперед на важливих об’єктах критичної інфраструктури. Через це постійно підвищується значущість питань, що стосуються подолання різноманітних кризових явищ та забезпеченням особистої, соціальної чи національної безпеки в разі надзвичайних ситуацій. Особливо це стало актуальним для України в період повномасштабної російської агресії, починаючи з 24 лютого 2022 року, протягом якого відбулися масштабні руйнування численних об’єктів критичної інфраструктури України.

Нині здатність держави та суспільства своєчасно розпізнавати передумови криз і катастроф, здатних заподіяти шкоду згаданій критичній інфраструктурі, й ефективно їм протистояти, стала мало не найголовнішим завданням національної безпеки.

Цю ситуацію спричинило те, що аварії, катастрофи та стихійні лиха з їх наслідками стають дедалі масштабнішими і вже починають становити реальну небезпеку для держави, зокрема для стабільності її економіки, та життя, здоров’я і добробуту її громадян. Аналіз масштабних (і не тільки) надзвичайних ситуацій (далі – НС) і їх наслідків демонструє, що загрозу нацбезпеці здатні становити як деякі надзвичайні ситуацій регіонального чи навіть вседержавного масштабу, так і постійні НС, що стаються на територіальному, місцевому та локальному рівнях. Крім того, кризові явища, з якими стискається наше суспільство, показують, що необхідно кардинально змінити систему захисту

людей і критично важливих об’єктів під час НС, а також розробити та впровадити ефективні механізми її функціонування.

Необхідно також узяти до уваги, що питання змісту управлінських функцій, організаційної структури, основ функціонування і варіантів подальшої розбудови системи державного управління забезпеченням безпеки критичної інфраструктури зумовлюють необхідність виведення на новий якісний рівень політики держави у сфері забезпечення безпеки населення і територій під час НС у мирний і воєнний час з урахуванням і використанням нових теоретичних напрацювань у галузі державного будівництва.

Останніми роками в нашій країні суттєво розвинулися процеси створення та розвитку державних механізмів захисту людей, об’єктів і територій від НС будь-яких форм і масштабів. Зокрема, у Стратегії забезпечення державної безпеки України, введеної в дію Указом Президента України від 16 лютого 2022 року № 56/2022. Загалом можемо визнати, що в Україні сформувалася та діє дуже ефективна та соціально затребувана система захисту населення і територій від НС. Водночас масштабні зміни в багатьох виявах життєдіяльності держави та збільшення кількості й масштабів російських терористичних актів призвели до необхідності формування ефективної національної політики із захисту критично важливих об’єктів у разі виникнення та поширення НС. Ураховуючи викладене вище, необхідно вдосконалити процеси забезпечення державної безпеки критичної інфраструктури саме відповідно до наявних умов.

Значний внесок у дослідження проблем державного управління зробили такі науковці, В. Д. Бакуменко, О. В. Бойко-Бойчук, В. М. Вакуленко, Н. М. Гринчук, А. О. Дєгтяр, С. М. Домбровська, О. Д. Лазор, М. А. Латинін, В. Я. Малиновський, Н. М. Мельтюхова, В. М. Мороз, В. М. Нижник, Р. М. Рудніцька, О. О. Труш, А. О. Чечель та ін.

Аналіз наукових джерел із проблематики державного управління у сфері нацбезпеки, зокрема і щодо захисту людей, певних обєктів і територій, свідчить,

що тут чсимало зроблено як українськими, так і зарубіжними ученим. Зокрема, вказані питання розглянуто у наукових працях таких авторів, як В. А. Андронов, С. В. Бєлай, А. В. Бєлоусов, М. В. Болотських, Б. Е. Братко, П. Б. Волянський, М. Б. Домарацький, А. Б. Качинський, В. В. Коврегін, В. А. Ліпкан, Є. П. Маслов, О. В. Михайлюк, 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. Саме тому обрана тема дослідження наразі є досить актуальною.

Мета й завдання дослідження. Мета роботи полягає в обґрунтуванні теоретичних засад і 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 критичної інфраструктури як об’єкту державного управління;

− визначити особливості формування та функціонування державної системи захисту критичної інфраструктури;

− проаналізувати закордонний досвід державного управління забезпеченням безпеки критичної інфраструктури;

− окреслити особливості державного управління забезпеченням безпеки критичної інфраструктури в Україні;

− здійснити аналіз вітчизняного нормативно-організаційного механізму державного управління забезпеченням безпеки критичної інфраструктури;

− запропонувати напрями трансформації державних механізмів забезпечення безпеки та підвищення ефективності захисту критичної інфраструктури;

− виокремити шляхи удосконалення системи державного управління захистом критичної інфраструктури;

− визначити орієнтири модернізації 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 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.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ДЕРЖАВНОГО УПРАВЛІННЯ ЗАБЕЗПЕЧЕННЯМ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Критична інфраструктура як об’єкт державного управління

Важливими пріоритетами людей незалежно від періоду їхнього життя завжди є прагнення забезпечити власне існування, зберегти життя та здоров’я, уникати агресії, досягти якісних умов існування та захищати довкілля. Більшість із цих пріоритетів безпосередньо належить 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 у цьому світі небезпек, що загрожують всім і кожному, обумовлює необхідність докладати зусилля для забезпечення особистої, громадської, державної та інших різновидів безпеки. У найзагальнішому вигляді небезпека − це потенційна можливість викликати шкоду, принести нещастя. Небезпеку також можна охарактеризувати як можливий результат впливу якихось негативних факторів на відповідні 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.

Осмислюючи поняття небезпеки, варто усвідомлювати, що тут мається на увазі лише потенційна можливість нещастя, а не саме нещастя. Це нагадування є необхідним, бо 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. У 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 охоплюють захист життя та здоров'я людини, а також захист власності людини від НС у мирний і воєнний час та від терористичних актів [16; 56].

У цьому випадку до життєвих інтересів суспільства слід віднести запобігання надзвичайним та іншим екстремальним ситуаціям, спричиненим аваріями, природними та іншими катастрофами, терористичними актами та в разі ведення військових дій або небезпек, спричинених цими діями.

До життєво важливих інтересів держави слід віднести:

– забезпечити ефективний захист населення та критично важливих об'єктів на території Україні під час НС і терористичних актів;

– забезпечити захист та виживання населення у воєнний час;

– збереження об'єктів, істотно необхідних для стійкого функціонування економіки та виживання людей.

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

Головними завданнями держуправління в плані забезпечення безпеки населення та зазначених об'єктів є такі: створення комплексу правових, організаційних, технологічних, інженерно-технічних та інших заходів

відповідно до потенційних загроз, призначених попереджати аварії та катастрофи на небезпечних об’єктах; підготовка для підтримки необхідних сил і засобів.

У монографії термін «населення» означає громадян України, іноземних громадян та осіб без громадянства, що перебувають на території України. Під «критично важливими об’єктами України» в цій роботі маються на увазі об’єкти, порушення функціонування яких здатне спричинити:

– втрату керованості (управління);

– руйнування інфраструктури;

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

У цьому випадку концепція «забезпечення безпеки населення та захисту критичних об’єктів під час НС і в разі терористичних актів» означатиме набір взаємопов’язаних програмних цілей і ресурсів, спрямованих на запобігання чи зменшення:

– втрат серед населення;

– загроз життю та здоров’ю людей;

– пошкоджень виробничих і соціальних об’єктів та навколишнього середовища від НС природного й техногенного характеру, терактів і сучасних засобів ураження.

Одним із головних 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 не збігається з поняттям рівня безпеки, що відповідає індивідуальним перевагам деяких членів суспільства. Істотно відрізняються також індивідуальні здібності людей оцінювати небезпеку й усвідомлювати обґрунтованість пропонованих суспільством критеріїв, нормативів і заходів із забезпечення безпеки [6; 125].

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

Сучасні уявлення про національну та регіональну безпеку (як її складову) відображає щільний зв'язок і взаємозалежність безпеки особи, суспільства й держави на всіх рівнях − від регіонального до конкретного місцевого. Питання нацбезпеки України наразі врегульовано достатньою кількістю законів, указів Президента України, постанов Уряду, а також багатьох інших підзаконних актів. Але, незважаючи на наявні великі кількісні масштаби, законодавча база в цій галузі має здебільшого фрагментарний характер, перш за все стосовно територіального рівня [88; 115].

Водночас явна недооцінювання діяльності забезпечення нацбезпеки 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 виключно на загальнодержавному рівні. Але це зовсім не так. Люди живуть у конкретній місцевості, в конкретному регіоні і вимагають задоволення власних матеріальних і духовних потреб та захисту своїх інтересів не лише на загальнодержавному рівні, а й у регіонах [94; 125].

Заперечення регіональних інтересів найвиразніше відбито в характеристиці національних економічних інтересів. Таке ставлення до таких актуальних регіональних проблем свідчить про збереження традиційного для України ставлення держави до людини 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 особи 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; 54].

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 погано корелює з ринковим станом. Формування ефективної економіки і вирівнювання процесів розвитку територій відповідають економічним інтересам територіальних спільнот і служать підґрунтям для консолідації населення під ідеєю загальнонаціонального інтересу.

Національні інтереси України в політичній стабільності значною мірою залежать від інтересів особи та регіональної спільноти.

Базовими принципами політичної стабільності є такі:

– розвинене місцеве самоврядування;

– демократичні вибори;

– законність і безпека громадян;

– дієва незалежна судова система.

Водночас 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. При цьому соціальні інтереси формуються безпосередньо в первинних соціальних групах, спільнотах і лише потім стають предметом вивчення і реалізації державних, громадських, політичних структур [17; 229].

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 із забезпечення безпеки регіону. У результаті стабільність положення і безпека регіонів визначають і загальний рівень нацбезпеки.

Ця обставина чітко вказує на те, що стан національної безпеки, насамперед внутрішньої безпеки, слід розглядати не лише за сферами життєдіяльності, а й у територіальному розрізі. Тому велику теоретичну і

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

Під час вивчення проблем регіональної безпеки методологічно найбільш значущим є питання про зміст, який вкладається у термін «регіон». На жаль, у нашій країні до цих пір не вироблено єдиного, загальноприйнятого або якось узаконеного чіткого й однозначного його визначення [110; 154].

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 межах історичних традицій тощо. Тому регіон − це самодостатній соціальний організм, який перебуває в єдності із середовищем, має власні фізико-географічні, культурно-цивілізаційні, еколого-економічні, етноісторичні, політико-адміністративні та правові властивості й виступає засобом формування і функціонування держави.

Регіони, як і держава в цілому, є прив’язаними до географічного середовища і мають політико-адміністративний зміст, пов’язаний з:

– типом і формою державності;

– регіональним заломленням відносин з іншими державами;

– характером кордонів;

– функціонуванням партій, громадських рухів і ЗМІ.

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 відповідно до цих вимог регіональні одиниці можуть перетинатися і піддаватися постійним змінам. Однак політичного значення регіони набувають лише тоді, коли більшість жителів регіонів вважає їх існування необхідним, а суспільство в цілому робить із цього необхідні висновки.

Отже, 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 цього регіону.

Цей факт ще більше підкреслює, що регіональна безпека повинна забезпечуватися силами та засобами цього регіону у тісній співпраці та за підтримки відповідних сил і засобів загальнодержавного рівня й інших регіонів. А для цього потрібна відповідна правова база та механізм її реалізації [29; 78].

Критичні об'єкти – це об'єкти, наслідком порушення чи припинення функціонування яких стає втрата управління економікою України, її регіонів чи муніципалітетів, а також значне погіршення стану безпеки населення, що мешкає в цих районах постійно чи тривалий час.

Категоризацію критично важливих об'єктів слід проводити незалежно від належності, відомства й типу об'єкта. Метою категоріювання є висунення кількісних і якісних вимог до системи фізичного захисту. Ці вимоги висуваються відповідно до рівня втрат і присвоєної у відповідності до них категорії об'єкта. Категорія об'єкта повинна визначатися на підставі оцінювання потенційної небезпеки об'єкта, при цьому повинна враховуватися ймовірність таких видів та масштабів втрат [65; 128].

До видів втрат належать такі:

– 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 НС і 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 таких 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 слід створити комісію з категоріювання, і першою її дією має бути 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, що пов'язуються виключно з

ручною або механізованою працею, потім все одно будуть виключені з розгляду [68; 197].

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. Підкреслимо, що можливість негативних наслідків, які роблять процес критичним, не завжди є очевидною. 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, а через це – до припинення поставок, зупинки 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 зазначені об’єкти, з подальшого розгляду виключаються. Усі визначені у такий спосіб об’єкти критичної інфраструктури включено до єдиного списку, який слід надіслати державним органам [17; 22].

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

Це вже творча робота, аналогічна аналізу загроз, яка повинна проводитися під час створення системи захисту. Складність зумовлюється тим, що:

– кожен об’єкт може використовуватися в декількох критичних процесах;

– той самий об’єкт можна атакувати в різні способи, і це буде призводитиме до різних наслідків для різних процесів.

У результаті аналізу необхідно оцінити для кожного об’єкта критичної інфраструктури за кожним показником категоризації максимально можливу шкалу негативних наслідків, що відповідають цьому показнику. Нарешті, на підставі цієї оцінки треба для кожного показника категоріювання визначити, якій категорії значущості відповідає цей об’єкт критичної інфраструктури за цим показником.

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

Відомості про результати категоріювання охоплюються 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.

Отже, держуправління 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.

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

Об’єктом держуправління здатні виступати лише ті відносини, які можуть об’єктивно регулюватися законом, тобто мають нормативний характер і

перебувають у сфері соціального простору, в якій право здатне чинити на суспільне життя прогресивний перетворюючий вплив. Крім того, врегулювання цих відносин має бути доцільним та ефективним.

Система всіх правових засобів, методів та способів, що використовуються у державному управлінні суспільними відносинами у галузі охорони критичних об'єктів, формує нормативно-правовий механізм державного регулювання у розглядуваній сфері [23; 110].

Нагадаємо, що серед категорій критичних об'єктів, що підлягають державному управлінню, планується виділити таке:

– об'єкти, що реалізують важливі функції держуправління;

– 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 держуправління, полягає в такому:

– державне управління загалом;

– управління конкретною територією;

– управління окремою групою державних органів.

Серед основних загроз для закладів, які реалізують важливі функції держуправління, виокремимо надзвичайні ситуації. Зауважимо, що характер можливих втрат унаслідок реалізації ключових загроз передбачає:

– втрату контролю над територією;

– паніку;

– людські жертви;

– матеріальні збитки.

Що стосується об’єктів життєзабезпечення населення і транспортних цілей, то їх функції охоплюють таке:

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

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

Надзвичайні ситуації є ключовою загрозою для об’єктів життєзабезпечення населення і транспортного призначення. Стосовно можливих наслідків виникнення та поширення надзвичайних ситуацій на цих об’єктах ми повинні зосередитись на таких питаннях:

– заподіяння шкоди здоров’ю людей та 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 – НС та розкрадання небезпечних речовин, унаслідок чого може ставатись таке:

– 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 такі НС, через 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, здатні породжувати паніку та призводити до заподіяння шкоду життю та здоров’ю людей.

Призначенням об’єктів історії та культури є:

– просвітництво населення;

– збереження пам’ятників історії та культури.

Загрозами у цьому випадку є НС та розкрадання культурно-історичних цінностей. Одним із наслідків, зауважимо, є те, що відвідування цих місць може призвести до заподіяння шкоди здоров’ю та життю людей, а також втрати згаданих пам’ятників.

Однією з особливостей аналізу загроз під час категоріювання об’єктів критичної інфраструктури є те, що суб’єкти категоріювання часто плутають ці два поняття:

1) аналіз загроз, здійснюваний під час формування системи безпеки значимого об’єкта критичної інфраструктури;

2) оцінювання негативних наслідків інциденту з об’єктом критичної інфраструктури, здійснюване під час категоріювання [68; 125].

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

Для оцінювання негативних наслідків порушення роботи об’єкта критичної інфраструктури цей рівень деталізації являється надмірним, у деяких випадках – неможливим, а головне – не потрібним.

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

– 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 ввімкнення аварійного захисту [17; 22; 65].

Усі перелічені компоненти управляються автоматизовано. На стадії категоріювання слід узяти за аксіому, що якщо не забезпечувати захист системи від дій зловмисника, то він зможе впливати на елементи системи управління. Через це 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 оцінювання можливості такого сценарію не потрібно оцінювати, чи можливо впровадити шкідливий код або дані у програмне забезпечення системи управління котельнею чи інші загрози, перелічені в банку даних. Достатньо того, що система управління дозволяє людині, яка отримала до них доступ, виконати такі дії, і це підтверджує фахівець зі служби головного інженера організації. Оцінюючи негативні наслідки суб’єкти критичної інфраструктури, часто намагаються врахувати здійснювані заходи захисту, наприклад:

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

– те що у котельні встановлено два котли, які в штатному режимі працюють із половинним навантаженням.

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

По-друге, у разі категоріювання таких об'єктів загрози визначають категорію значущості, а категорію значущості, в свою чергу, – склад основних заходів захисту, яких необхідно вжити на об'єкті критичної інфраструктури.

На стадії категоріювання ще не визначено категорію значущості об'єкта, тож, відповідно, не визначено, які заходи захисту є необхідними. Тому на цій стадії суб'єкта не має підстав вважати, буцім ужиті ним заходи захисту є достатніми [68; 82; 145].

По-третє, правила категоріювання вимагають під час оцінювання наслідків враховувати також і взаємозв'язок об'єктів, включно з 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 усіх 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.

Головним завданням забезпечення безпеки об’єктів критичної інфраструктури є максимально швидке надходження інформації про такі загрози та її використання для вжиття адекватних заходів безпеки. При цьому найважливішими стають питання обладнання й 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. Ще до того як вирішувати питання, як захищати, необхідно визначитися з тим, що саме слід захищати, від чого і до якої міри. Саме в такій послідовності вирішуються завдання побудови систем безпеки об’єктів критичної інфраструктури.

Якщо взяти усі загрози разом, серед них напрошується виділення таких двох груп:

1) загрози самому критично важливому об’єкту;

2) загрози, що походять від такого об’єкта.

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

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

Запобіганню цих загроз присвячено левову частку повсякденної діяльності правоохоронних органів і внутрішніх структур безпеки об'єктів.

До другої групи належать загрози життєдіяльності населення та навколишніх населених пунктів, які є джерелом найбільш критичних об'єктів.

Виникнення різних НС на цих об'єктах і територіях через природні й 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. Окремо зосередимось на загрозах, спричинених несанкціонованими діями порушників.

Загрози для зазначених об'єктів можна поділити так:

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

– загрози об'єктам і територіям, не оснащеним системами безпеки.

В аспекті можливості здійснення перша категорія загроз володіє такими 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 кількістю 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 у разі реалізації загроз;

– потреба в залученні до реалізації загроз смертників;

– обмеженість у часі для підготовки і проведення акції.

Порівняно із загрозами першої групи, загрози безпеки життєдіяльності міста відрізняють здійсненність за наявності у виконавців професійних навичок, озброєння і оснащення, а також на необхідності ґрунтовної підготовки акції (збирання відомостей про такий об’єкт, наймання виконавців, поетапна доставка необхідних предметів у 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 такими факторами:

– безперешкодність пересування населення і транспорту всередині та / або поблизу таких найважливіших об’єктів (за винятком особливих випадків);

– якщо такі об’єкти перебувають у різних формах власності;

– якщо вони 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 з 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 виникнення НС на критично важливому об’єкті.

Наявність ЗМІ є позитивним фактором забезпечення безпеки на критично важливих об’єктах. Однак у деяких випадках ці засоби навпаки, здатні ненавмисно спровокувати НС – 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) сприяє підвищенню безпеки на критично важливих об’єктах [16; 138].

Зазначені чинники дещо видозмінюють можливості реалізації первинних функцій безпеки, на які слід зважати під час вироблення підходів до вирішення завдань безпеки в місті. Зокрема, їх попередній аналіз показує, що з огляду на особливості міської інфраструктури найскладнішими і 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. Важливим чинником покращення 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, отримуваній від населення [90; 172].

Зважаючи на всі очевидні технічні рішення, що реалізують ці функції, необхідно наперед визначити інформаційні ознаки, які вказують на розгортання НС, оптимізувати обсяги та послідовність переданих фрагментів інформації та встановлення їх споживачів. Це завдання має вирішуватись на основі відповідної інформаційної моделі.

Ефективність вирішення завдання припинення загрози значною мірою 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 (за наявності таких), що розміщуються на кордонах об’єктів. Умова, за якої виявлена загроза буде припинена, залежатиме від двох чинників: часу стримування загрози елементами системи безпеки об’єкта та часу прибуття оперативного підрозділу міста до місця акції. Вважаючи, що другий чинник є фіксованим для конкретного об’єкта внаслідок його віддаленості від оперативного підрозділу, можна визначити мінімально допустимий час стримування загрози службою безпеки об’єкта. Отже, 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, визначатиметься переважно можливостями міських засобів виявлення і близькістю знаходження до місця акції сил оперативних підрозділів.

Чинник раптовості, властивий початку прояви загрози в міських умовах, висуває як одне з головних завдань ідентифікацію передкризової (попередньої

виникненню загрози) ситуації, що дозволить силам реагування впровадити необхідні попереджувальні дії. Ознаками такої ситуації є:

– неадекватна поведінка людей у 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 можна здійснювати автоматичну генерацію гіпотез передкризової ситуації, належить до завдань, що передують вибору технічних рішень і їх реалізації.

Отже, адекватність і достатність проєктних рішень щодо забезпечення безпеки життєдіяльності міста досягаються попередніми обґрунтуванням вимог до функціональних властивостей систем та засобів безпеки, які теж мають обиратися на підставі аналізу загроз потенційно небезпечним і критично важливим об’єктам міста та інших відповідальних елементів його інфраструктури [56; 125; 138].

1.2. Механізми державного управління забезпеченням безпеки об’єктів критичної інфраструктури

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

1) адміністративна реформа, покликана створити нові інститути державної влади в усіх регіонах України та поліпшити діяльність наявної системи виконавчої влади;

2) розгортання та зміцнення соціальних інститутів, що сприяють установленню стійкої демократії в державі;

3) заснування й формування соціальних та адміністративно-правових регуляторних органів, які гарантують конституційний набір прав, свобод та обов'язків громадян України;

4) розроблення державної політики щодо громадської безпеки й захисту критичної інфраструктури та її реалізація;

5) забезпечення внутрішньої та зовнішньої безпеки регіонів України та формування мирних умов, сприятливих для їх життєдіяльності;

6) досягнення гармонійного і взаємопов'язаного розвитку регіонів у взаємодії з державою шляхом прискорення формування та оптимізації 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 зв'язку з побудовою «дерева цілей», в яких стратегічні, оперативні та тактичні цілі, кінцеві та проміжні, державні та приватні, віддалені й тісно узгоджені, є взаємопов'язаними та становлять певну логічну цілісність. [10; 26].

Важливо також з'єднати «дерево цілей» із 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 найблагородніші 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 держуправління у сфері громадської безпеки й захисту критично важливих об'єктів вимагає спочатку встановити місце та роль 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 цій 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, серед іншого на свідомості, поведінці та діяльності людей.

Сьогодні всі питання держуправління зосереджуються як ніколи на проблемі забезпечення нацбезпеки України. Управління безпекою в різних сферах життєдіяльності й пошук ефективних шляхів вирішення актуальних проблем суспільства зачіпають інтереси всіх груп населення, політичних партій, вчених і практиків [88; 241].

Очевидно, що серед найгостріших економічних, продовольчих, енергетичних, соціальних, політичних тощо 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 того, що вони істотно впливають на стан економічної, екологічної та соціальної безпеки [34; 47].

Конкретне сполучення функцій держуправління залежить як від стану та структури керованих процесів − сукупності керованих об'єктів, так і від місця та ролі держави у сферах життєдіяльності.

Держава та суспільство є взаєпов'язаними, її діяльність мимоволі визначається потребами й інтересами суспільного розвитку. Цю взаємозалежність особливо важливо підкреслити, оскільки у багатьох політичних заявах та виступах ЗМІ постійно висувається думка, що державі не

варто намагатись впливати на суспільство, вона не повинна заважати його свободі, натомість має відкрити простір для творчості. Однак вивільнення суспільства та його окремих відносин, процесів і явищ від цілепокладаючих, організуючих і регулюючих впливів держави передбачає, що замість них працюватимуть самоврядні механізми (економічні, соціальні, культурні, інформаційні тощо), що підтримують досягнутий рівень організованості та урегульованості, інакше в суспільстві виникає стан некерованості, свавілля, анархії і хаосу.

У 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 такому:

– 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.

Досліджуючи функції держуправління у галузі громадської безпеки й захисту критичної інфраструктури, в цій роботі ми спиралися на аналіз усієї сукупності чинників, які нині впливають на державні відносини, а також на те, що суспільство наразі не готове взяти на себе функції, які виконуються державними установами. Протистояти впливу надзвичайних ситуацій на сталий розвиток України зараз можна лише завдяки відповідній соціальній організації суспільства, поклавши відповідну стратегічну роль на державу [46; 53; 161].

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

– планування;

– організацію;

– регулювання;

– роботу з персоналом;

– контроль.

Це необхідно врахувати, оптимізуючи функцій органів виконавчої влади регіонів України в межах адміністративної реформи. Відмова від функцій планування та контролю в держуправлінні, де вкрай потрібен перспективний (стратегічний) погляд, навряд чи є виправданою, оскільки соціальні процеси, що підлягають державному управлінню, охоплюють десятки мільйонів людей.

На управлінській практиці позначається ігнорування і недооцінювання 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. У 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 слід 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.

Систему громадської безпеки та захисту об'єктів критичної інфраструктури під час НС і терористичних актів неможливо реформувати без здійснення специфіки функцій управління, особливо тих, які притаманні саме державі й 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:

1) у плані наявності в країні орієнтацій на вікові традиції, зокрема, політичну культуру населення та правлячі групи (претенденти на владу), які певною мірою визначають реалізацію цієї проблеми; не обов'язково, щоб ці традиції визначали процес держуправління, однак немає сумніву, що заперечення їх у нинішній ситуації в кінцевому рахунку створює тупикову ситуацію;

2) узяття до уваги сьогоднішнього соціально-політичного й економічного становища; аналіз цього чинника є необхідним через те, що він надає можливість, з одного боку, розробляти рішення поставленої проблеми на реальній основі, а з іншого − враховувати минуле, характерне лише для сьогоднішнього моменту, а також зосередитися на дійсно ключових проблемах оптимізації механізмів та структур держуправління;

3) узяття до уваги глобального аспекту завдань держуправління, що вирішуються в Україні; світовий досвід дає не лише і не так багато знань про можливі рішення конкретних завдань управління, глобальний контекст дозволяє будувати запропоновані рішення; отже, щоб передбачити світові тенденції,

зберегти українську самобутність і використовувати дійсно оптимальні варіанти рішень проблем держуправління;

4) використання загальнонаукового принципу подвійної герменевтики, тобто подвійної інтерпретації вирішення поточного дослідного завдання: суворо наукового аналізу проблем держуправління, врахування фундаментальних аспектів проблеми, новітніх наукових напрацювань тощо.

Захищеність об'єктів критичної інфраструктури − це стан, за якого цим об'єктам забезпечуються умови для запобігання виникненню потенційних небезпек і подолання чи мінімізації негативних наслідків кризових ситуацій природного чи техногенного характеру або породжених діями терористів [22; 80; 219].

Під час оцінювання захищеності критично важливого об'єкта враховується:

– обсяг впровадження інженерно-технічних заходів для підвищення безпеки;

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

– фактичний стан згаданих вище апаратури та систем;

– забезпеченість захисту персоналу об'єкта та населення, що мешкає в зоні впливу об'єкта як джерела НС;

– підготовленість об'єкта до роботи в умовах НС;

– повнота проведення заходів щодо запобігання та пом'якшення наслідків НС;

– готовність систем управління до роботи під час НС;

– фізична захищеність об'єкта від терактів.

Повна реалізація зазначених вище заходів дозволить виконати такі завдання:

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

– визначення можливості виникнення НС ;

– оцінювання ймовірних наслідків НС ;

– оцінювання можливого впливу НС , що сталися на сусідніх небезпечних об’єктах;

– оцінювання стану робіт із попередження НС та готовності до ліквідації НС на небезпечному об’єкті;

– розроблення заходів зі зменшення ризику та пом’якшення наслідків НС на небезпечному об’єкті.

Необхідно по всій території нашої держави проводити моніторинг небезпечних хімічних та біологічних речовин і розробляти пропозиції щодо впровадження першочергових заходів небезпечних хімічних та біологічних об’єктів, територій їх розміщення під час здійснення заходів [130; 172].

– з розроблення моделі управління та взаємодії, а також алгоритмів ухвалення 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 і процесів і попередженні появі та розвитку НС. Його мета – інформаційне забезпечення процесу ухвалення управлінських рішень про вплив у правильному напрямку на стан системи, явища чи процесу. По-друге, метою моніторингу є вироблення аналітичної інформації, потрібної для проведення досліджень у тій предметній галузі, 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, доцільно організовувати три основні види моніторингу:

1) моніторинг техногенних небезпек і впливів;

2) моніторинг небезпечних явищ і процесів;

3) екологічний моніторинг.

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

Екологічний моніторинг як один з основних перелічених 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 ДСНС, необхідною екологічною інформацією [104; 130].

Включення до єдиної системи сил і засобів великої кількості відомств обумовлює наявність широких можливостей у цій системи стосовно рішення задач комплексного моніторингу. Усі згадані системи, як і десятки інших систем спостереження та контролю, покликаних вирішувати ті чи інші приватні завдання, складають той базис, на якому можна побудувати систему 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, оцінювання та контроль за станом небезпечних в техногенному відношенні об’єктів, ідентифікації загроз; прогнозування розвитку ситуації з урахуванням можливих сценаріїв виникнення аварій, катастроф і НС на об’єктах критичної інфраструктури;

– оцінювання та прогнозування характеру та масштабів наслідків техногенного впливу на такі об’єкти;

– спостереження, оцінювання та прогнозування стану навколишнього середовища;

– інформаційну та інтелектуальну підтримку всього процесу ухвалення управлінських рішень у відповідній сфері, зокрема і щодо розглядуваних об’єктів [34; 145; 214].

Аналогічним чином система моніторингу небезпечних природних явищ і процесів повинна містити в собі комплекс джерел інформації, який дозволятиме вирішувати завдань щодо:

– спостереження, оцінювання та прогнозування стану навколишнього середовища, своєчасного виявлення симптомів (ознак), що вказують на виникнення небезпечних природних явищ і процесів, прогнозування їх можливого розвитку та переростання у НС, особливо на об’єктах критичної інфраструктури;

– спостереження, оцінювання та прогнозування поточного стану, характеру та ступеня ураження, що завдається розглядуваним об’єктам;

– інформаційної та інтелектуальної підтримки повного процесу ухвалення управлінських рішень у сфері забезпечення природної безпеки.

Система екологічного моніторингу покликана здійснювати:

– спостереження, оцінювання та прогнозування стану навколишнього середовища за програмами геофізичного, біологічного моніторингів та моніторингу джерел антропогенного впливу;

– інформаційно-інтелектуальну підтримку процесу ухвалення управлінських рішень і наукових досліджень у сфері екологічної безпеки.

Аналіз розглянутих видів моніторингу показує їх глибокий зв’язок із цільовими функціями, особливо щодо спостереження, оцінювання та прогнозування стану навколишнього середовища. Однак не можна не помічати і

явні особливості, і деякі відмінності в цих цільових функціях. Вони обумовлюються характером завдань, які повинні вирішуватися структурами управління, в інтересах яких здійснюється відповідний вид моніторингу [145; 164].

Цільова функція моніторингу техногенних небезпек і впливів як спостереження, а також оцінювання 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. Водночас інформація про стан довкілля, отримувана в межах такого моніторингу, потрібна для виявлення тенденцій і прораховування розвитку ситуації та ознак небезпеки й перетворення її на НС. Аналогічні судження можна зробити і щодо цільових функцій моніторингу, оцінці та прогнозування стану довкілля в процесі моніторингу небезпечних природних явищ та ознак небезпеки їх перетворення на НС. Однак розглянута цільова функція значно розширюється в напрямку прогнозування та оцінювання динаміки розвитку стану навколишнього середовища й виявлення ознак виникнення небезпечних природних явищ і процесів. Найбільш широко представлена цільова функція моніторингу, оцінювання та прогнозування стану довкілля в екологічному моніторингу.

Отже, екологічний моніторинг належить до заходів, спрямованих зрештою на інформаційну підтримку виконання головних завдань із забезпечення екологічної безпеки. Тому мету проведення екологічного моніторингу в загальному випадку можна сформулювати як ідентифікацію та оцінювання екологічних небезпек, а також інформаційну підтримку підготовки й ухвалення управлінських рішень стосовно:

– охорони природи та здоров'я людей;

– регулювання та відновлення якості довкілля;

– нормалізації екологічної обстановки в екстремальних випадках.

Моніторинг навколишнього середовища охоплює спостереження, оцінювання та прогнозування антропогенних змін абіотичної складової біосфери та відповідну реакцію біологічних систем на ці зміни, тому для його здійснення використовується принцип інтегрованого поєднання різних типів такого моніторингу. Зокрема, залежно від реакції основних складових біосфери на антропогенний вплив, розрізняють геофізичний і біологічний моніторинги.

Геофізичний моніторинг містить у собі елементи спостереження, оцінювання і прогнозування стану та змін геофізичного середовища (сукупність фізичних процесів і властивостей певної земельної ділянки), тобто зміни абіотичного компонента біосфери як в мікро-, так і макромасштабі, включно із забрудненням навколишнього середовища радіоактивними, шкідливими хімічними речовинами, іншими небажаними інгредієнтами тощо, а також реакціями великих систем – погоди та клімату [69; 72].

Головним завданням біологічного моніторингу є встановлення й оцінювання:

– стану 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.

Біологічним моніторингом охоплюються спостереження, оцінювання та прогнозування стану здоров’я людей і найважливіших популяцій як в аспекті існування тієї чи іншої екосистеми, так і з погляду високої господарської цінності (наприклад, цінні сорти риб). Також здійснюється спостереження та оцінюється стан найчутливіших до певного виду антропогенного впливу популяцій рослин і тварин, зокрема популяцій-індикаторів [72; 142; 172].

Екологічний моніторинг, по суті, містить у собі в повному обсязі два розглянутих вище види моніторингу в їх взаємозв’язку. До цього моніторингу

відповідно до його функціональних завдань, про які вже згадувалося, належить і моніторинг джерел та 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 шкідливо впливають на навколишнє середовище.

Моніторинг критично важливих об'єктів інфраструктури проводиться або на постійній основі, регулярно, або з певною заздалегідь визначеною періодичністю й охоплює спостереження, вимірювання та фіксацію даних, поєднуючи контроль та аналізу узагальнених параметрів стану охорони згаданих об'єктів, що дозволяє як чинити на них вплив, так і наперед розробляти рішення, потрібні для запобігання кризовим ситуаціям природного й техногенного походження та/або максимального зменшення їх негативних наслідків [102; 130].

До цілей запровадження моніторингової системи належить поетапна мінімізація рівня ризику впливу на об'єкти критичної інфраструктури різноманітних зовнішніх чинників (від природних до пов'язаних із тероризмом) та шкоди, яку можуть завдати населенню держави та навколишньому середовищу такі ситуацій [22; 86; 145].

До завдань такого моніторингу належать надання інформаційної підтримки, необхідної для визначення й реалізації відповідних заходів із завчасного прогнозування, встановлення потенційних загроз об'єктам критичної інфраструктури і небезпек та запобігання виникненню кризових ситуацій на згаданих об'єктах.

Об'єктом цієї системи моніторингу вважається захищеність таких об'єктів. Ця система покликана забезпечити виконання цілої низки функцій, до

яких, зокрема, належать збирання, аналізування, обробка, зберігання та передання інформації про:

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

– маршрути транспортування вантажів та інші необхідні дані;

– інформаційне забезпечення дій, що здійснюються у межах підготовки та реалізації заходів із забезпечення безпечного функціонування зазначених вище об’єктів, запобігання появі кризових ситуацій, їх локалізації і ліквідації їх наслідків;

– підготовка інтегрованих оцінок (моделей) кризових ситуацій щодо критично важливих об’єктів інфраструктури та оцінювання їх імовірних наслідків;

– прогнозування можливих загроз згаданим об’єктам і динаміки змін стану їх захисту в разі впливу на них різних природних, техногенних тощо чинників;

– створення і ведення баз даних з інформацією, потрібною для обґрунтування необхідності певних управлінських рішень щодо захисту таких об’єктів;

– використання інформаційних ресурсів системи моніторингу відповідно до передбаченого порядку; вжиття заходів для їх захисту від несанкціонованого впливу;

– подальша розбудова єдиного інформаційного простору системи моніторингу шляхом уніфікування інформаційного, програмного й апаратного забезпечення та досягнення їх сумісності;

– інформаційна підтримка реалізації міжнародних договорів та угод, що стосуються моніторингу згаданих об’єктів.

У цій системі можна виділити національний, міжрегіональний, регіональний, міський і місцевий рівні. Крім них, системи моніторингу має ще такі складові:

– центри системного моніторингу й оперативного управління (далі − центри моніторингу);

– системи, комплекси та засоби отримання інформації про узагальнені параметри стану охорони розглядуваних інфраструктурних об’єктів;

– системи та засоби телекомунікацій, збору й передання даних та оповіщення.

В Україні головними структурними складовими цієї системи, що мають забезпечувати вирішення покладених на неї завдань, повинні бути центри моніторингу органів державної влади та місцевого самоврядування.

Вирішуючи завдання, покладені на систему моніторингу, слід налагодити інформаційну взаємодію між його центрами різного рівня та іншими державними й недержавними інформаційними системами України загального та спеціального призначення, а також з міжнародними інформаційними системами [69; 70].

Під час формування та використання цієї системи необхідно спиратися на такі базові принципи:

1) відповідність завданню, що стоїть перед системою моніторингу, а також його структурі та особливостям загрози об’єктам критичної інфраструктурі;

2) урахування структури та завдань органів державної влади та місцевого самоврядування України, до відання яких належать забезпечення захисту згаданих вище інфраструктурних об’єктів і навколишнього середовища;

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

а) спільна система класифікації та кодифікації загроз згаданим об’єктам;

б) показники та критерії оцінювання стану захищеності таких об’єктів;

в) базові (типові) протоколи й алгоритми (програми) збирання, обробки та обміну інформацією, підготовки та автоматизованої підтримки ухвалення та реалізації управлінських рішень на підставі даних моніторингу стану згаданих об’єктів;

4) спільна геоінформаційна система;

5) ієрархічність будови системи моніторингу, можливість використовувати ресурси системи моніторингу критично важливих інфраструктурних об’єктів як централізовано, так і санкціоновано децентралізовано;

6) досягнення раціональної функціональної сумісності центрів моніторингу критичної інфраструктури різнорівневих об’єктів;

7) уніфікація програмних, інформаційних і технічних засобів, досягнення сумісності елементів цього моніторингу, забезпечення можливості її модульного розширення та модернізації;

– забезпечення можливості структурного та функціонального розвитку, оптимізації складу користувачів системи цього моніторингу та спектра відповідних наданих послуг;

– багатофункціональність, яка забезпечує вирішення завдань в інтересах водночас і національної безпеки, і соціально-економічного розвитку країни;

– наступність, що ґрунтується на інтеграції та вдосконаленні інших систем моніторингу критичної інфраструктури об’єктів;

– гарантування захисту інформації від несанкціонованого доступу, включно з обмеженням доступу до інформації про критичні об’єкти інфраструктури, що циркулюють у системі моніторингу;

– запобігання залежності системи моніторингу від зарубіжних технологій.

Головними завданнями механізмів державного регулювання захисту об’єктів критичної інфраструктури як складових механізмів держуправління у сфері цивільного захисту є такі:

– втілення в життя державної політики у сфері цивільного захисту, захисту населення й територій від НС, забезпечення пожежної безпеки та безпеки людей на водних об’єктах (у межах компетенції відповідних інституцій);

– контрольна функція у згаданій вище сфері;

– розроблення і вжиття заходів з організації та здійснення цивільного захисту, захисту населення і територій від НС і пожеж, забезпечення безпеки людей на водних об’єктах та екстреного реагування на НС на національному рівні (у межах компетенції відповідних інституцій) [93; 145; 148].

При цьому кожний суб’єкт зазначених механізмів:

– організовує прогнозування НС у межах системи моніторингу та відповідного прогнозування, роботу з попередження НС національного рівня та їх ліквідації, порятунку та життєзабезпечення людей під час таких ситуацій, сприяє ліквідації НС регіонального та міжмуніципального характеру, а також забезпечує вчасне ухвалення управлінських рішень у разі переходу цих НС на національний рівень;

– організовує в передбаченому нормативними актами порядку роботу із запобігання пожежам і контроль за організацією їх гасіння на критично важливих для безпеки країни об’єктах та інших особливо важливих пожежонебезпечних об’єктах, особливо цінних об’єктах культурної спадщини України й під час проведення заходів загальнодержавного рівня з масовим скупченням людей, перелік яких затверджується Урядом України [8; 86; 164];

– відповідно до законодавства організовує пошук та порятунок людей на водних об’єктах;

– організовує разом із зацікавленими регіональними органами виконавчої влади в установленому порядку формування та доставку вантажів гуманітарної допомоги населенню, постраждалому внаслідок НС, зокрема і населенню зарубіжних країн;

– організовує облік атестованих аварійно-рятувальних служб, пожежників, пожежно-рятувальних, пошуково-рятувальних та аварійно-рятувальних формувань і громадських об'єднань, у яких до статутних завдань належить здійснення аварійно-рятувальних робіт і гасіння пожеж;

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

– організовує взаємодію сил і засобів, задіюваних в аварійно-рятувальних операціях під час НС і гасіння пожеж;

– організовує атестування аварійно-рятувальних служб, пожежно-рятувальних, аварійно-рятувальних формувань і рятувальників органів державної виконавчої влади, органів виконавчої влади регіонів України, органів місцевого самоврядування та інших організацій;

– контролює створення та забезпечення готовності сил і засобів цивільного захисту в усіх регіонах України, муніципальних утвореннях та організаціях;

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

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

– у межах власної компетенції вживає в передбаченому нормативними актами порядку заходів із запобігання, виявлення та припинення терористичної діяльності на об’єктах, підвідомчих ДСНС України, а також з усунення чи мінімізації наслідків терактів;

– бере участь у межах своєї компетенції в інформуванні населення через ЗМІ та інші канали про прогнозовані НС і пожежі й ті, що виникають, заходи із забезпечення безпеки населення і територій та методи захисту, а також займається пропагандою у сфері цивільного захисту, захисту населення та територій від НС, забезпечення пожежної безпеки та безпеки людей на водних об’єктах;

– бере в межах своєї компетенції участь в управлінні єдиною державною системою цивільного захисту;

– бере участь у розробленні пропозицій стосовно надання державної допомоги населенню та територіям, що постраждали від НС регіонального, національного і транскордонного характеру, та щодо координації діяльності всіх видів протипожежного захисту [91; 157; 248].

Отже, суб’єкти забезпечення охорони об’єктів критичної інфраструктури для реалізації покладених на них завдань наділяються такими основними повноваженнями:

– готувати проєкти нормативно-правових актів та інших документів щодо цивільного захисту загалом, захисту населення та територій від НС, забезпечення пожежної безпеки тощо;

– проводити в передбаченому законодавством вигляді контроль за організацією наглядової діяльності головними управліннями ДСНС України за дотриманням встановлених вимог у сфері цивільного захисту, захист населення та територій від НС, забезпечення пожежної безпеки тощо органами місцевого самоврядування, відповідними організаціями, їх посадовими особами, громадянами України, іноземними громадянами та особами без громадянства;

– реалізовувати функції з управління закріпленим за ними державним майном в установленому порядку;

– здійснювати повноваження розподільника коштів із Держбюджету України щодо головних управлінь ДСНС України та підпорядкованих підрозділів відповідно до законодавчих та інших нормативно-правових актів;

– створювати координаційні та дорадчі органи (зокрема, комісії чи групи), що формуються на представницькій основі, а також інші колегіальні органи для обговорення актуальних питань діяльності ДСНС України тощо [104; 216].

1.3. Особливості формування та функціонування державної системи захисту критичної інфраструктури

Ураховуючи 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 стосовно особливо значущих для держави та суспільства елементів інфраструктури, пошкодження 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, треба передбачити та сформувати заходи з мінімізації та усуненню шкоди, але, перш за все, профілактичні заходи, здатні заздалегідь запобігти серйозним аваріям або хоча б мінімізувати їх наслідки.

Загроза пошкодження критично важливого інфраструктурного об’єкта залежить від взаємного розташування у просторі та часі (для стаціонарних об’єктів – лише у просторі) джерела небезпеки й того об’єкта, на який воно

впливає. Водночас небезпеки становлять загрозу лише тоді, коли вони мають можливість заподіяти шкоду конкретним об’єктам. Відповідно, небезпека (і так само кілька різних небезпек) становитиме загрозу для зазначеного об’єкта інфраструктури, лише в тому разі, якщо її (їх) небезпечні чинники мають можливість на цей об’єкт впливати. Наприклад, для людей загроза виникає за умови, що вони працюють на об’єкті підвищеної небезпеки чи в зоні забруднення, а для рухомих об’єктів – якщо вони під час небезпечної події перебувають у зоні впливу небезпечних чинників [91; 241].

Ступінь загрози життю населення в певній місцевості й, відповідно, критичній інфраструктурі зумовлюється ступенем її небезпечності, а також географічними та часовими чинниками. Якщо перенести такий об’єкт за межі небезпечної території, загроза для нього зникне, хоча небезпечність території не зміниться. Загроза життєдіяльності змінюється з часом – виникає взагалі, збільшується чи зменшується. Безпека населення, навколишнього середовища та різних об’єктів, зокрема й об’єктів критичної інфраструктури, у разі настання можливих техногенних аварій і стихійних лих у НС установлюється шляхом оцінювання 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 наслідками в часі та просторі.

Кількість різновидів ризику є великою, але в контексті надзвичайних ситуацій зазвичай розглядаються так звані «чисті ризики», які передбачають тільки небажаний (негативний) ефект. До них можна віднести, зокрема, ризики можливих втрат: популяційний, індивідуальний, природний, екологічний, диференційований, інтегральний (сумарний, сукупний), фізичний, економічний, соціальний (колективний, груповий) тощо.

Крім того, для умов надзвичайних ситуацій необхідно отримати оцінки індивідуального і соціального ризиків. У деяких окремих випадках, наприклад для небезпечних технологічних процесів, виконують оцінювання регламентованих параметрів небезпек.

Індивідуальний ризик (розподіл ризику) − це ймовірність (частота) виникнення небезпечних чинників під час НС у певному місці простору [35; 148].

Соціальний ризик (характерний для масштабу небезпеки) – залежність від ймовірності травмування певної кількості людей від загальної кількості людей, постраждалих від чинників 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, прогноз наслідків НС для об’єктів критичної інфраструктури розробляється в кілька етапів.

На І етапі встановлюють параметри впливів − значущих уражальних чинників, що спричинюють основні руйнування й ураження, з характеристиками, що зазвичай обираються з використанням існуючих методик.

На ІІ етапі встановлюють закони ураження − опору елементів ризику впливів, під якими розуміють залежності ймовірності ураження від інтенсивності прояву уражальних чинників, застосовуючи для їх формалізації ті чи інші функції, що відповідні цій надзвичайній ситуації.

На ІІІ етапі прогнозування дається оцінювання наслідків сполучення моделей впливу і законів ураження (руйнування / пошкодження). З використанням цього методологічного підходу оцінюються наслідки майже всіх стихійних лих і техногенних аварій, що необхідно для обґрунтованого ухвалення рішень про організацію екстреної евакуації населення з районів НС і забезпечення його життєдіяльності у безпечних районах, а також залучення для

ліквідації НС сил і засобів ДСНС України різного рівня. Конкретний вплив різних чинників на об’єкти критичної інфраструктури та людей під час аварій і катастроф з можливими їх наслідками описується за допомогою відповідних моделей. Моделі впливу − це залежності, що визначають розміри потенційної небезпеки (негативного впливу), а також розподіл інтенсивності уражальних чинників. При цьому потенційну небезпеку можна описати у вигляді аналітичних, табличних або графічних залежностей [23; 79; 169].

Параметри уражальних чинників 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 і співпраця між державою та інфраструктурними організаціями: якщо держава залишається гарантом внутрішньої безпеки й виступає посередником в межах інформаційно-комунікаційних процесів, то інфраструктурні організації мають значно детальну інформацію про відповідні елементи інфраструктури, й завдяки цьому лише вони здатні вжити ефективних конкретних заходів захисту.

Розробники основних заходів захисту повинні зосередитись, по-перше, на відповідних положеннях закону, а по-друге, на загальновизнаних принципах бізнесу далекоглядного управління ризиками та стратегічного планування господарської діяльності підприємства, спрямованих на досягнення успіху та послідовності, наприклад у межах так званого управління для забезпечення безперервності бізнесу.

Так, зазвичай органи правління низки інфраструктурних організацій зобов’язані вживати належних заходів і створювати системи контролю, наприклад системи ризик-менеджменту, що дозволяють на ранній стадії помітити тенденції і факти, що становлять загрозу для подальшого існування суспільства [99; 133; 195].

До таких тенденцій і фактів поряд із ризикованими операціями та порушеннями положень нормативно-правових актів належать також загрози стихійних лих чи терактів, здатних відчутно вплинути на подальше існування підприємства. Відповідно, керівники за оцінкою достатності капіталу й узвичаєними стандартами кредитування останнім часом почали приділяти посилену увагу питанням аналізу й оцінюванню підприємницьких ризиків.

Інший орієнтир визначення критичних заходів щодо захисту інфраструктури випливає з відповідальності інфраструктурних організацій за захист своїх об'єктів від потенційних загроз і вжиття необхідних заходів. Ці обов'язки інфраструктурних організацій частково закріплено 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].

У плані безпеки важливим є внесок у захист критично важливих елементів інфраструктури заходів з припинення несанкціонованих дій, що вчиняються сторонніми особами. Необхідно забезпечити рівень захисту об'єктів від порушень, спричинених навмисно, а також унаслідок стихійних явищ чи аварій, які по змозі виключали б виникнення серйозної небезпеки, наприклад унаслідок вибуху чи шляхом поширення небезпечних речовин. Слід також уникати перебоїв у постачанні продукції та наданні послуг, якщо існує серйозний ризик для діяльності критичної інфраструктури.

Тож, головним завданням розроблення концепції основних заходів захисту є захист життя людини за рахунок зниження рівня уразливості критичних елементів інфраструктури до впливу природних явищ і подій, спричинених технічними поломками або людськими прорахунками, а також зменшення рівня уразливості до актів тероризму чи злочинних дій. Отже,

концепція основних заходів захисту повинна враховувати стандартизовані будівельні, організаційні, кадрові й технічні заходи безпеки [93; 95; 156].

Попри те, що небезпека для навколишнього середовища теж здатна становити серйозну загрозу, в цій концепції самі лише екологічні наслідки розглядати окремо не слід. Однак і в цій сфері можна застосувати аналогічний підхід. Також залишаються без уваги злочинні посягання на підприємства, що завдають шкоди, перш за все, їх конкурентоспроможності, такі як, наприклад, промислове шпигунство.

Вчені та практики різних сферах і галузей одностайні в тому, що наявна система національної та регіональної безпеки, насамперед у природно-техногенній, екологічній і військовій сферах, недостатньо ефективно вирішує проблеми захисту життєво важливих інтересів як людей, так і держави, оскільки вона не є цілісною, достатньою, раціонально організованою та ефективно керованою [52; 72].

Крім того, цей компонент системи забезпечення нацбезпеки працює головним чином на оперативній основі. По суті, всі органи, що її забезпечують, працюють в одному режимі реагування. Розуміння змісту поняття «регіональна безпека» та його внутрішньої структури дозволяють визначити раціональну структуру системи громадської безпеки та захисту критично важливих об’єктів під час НС і терористичних актів.

Треба враховувати також те, 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 нацбезпеки свідчить, що в цій галузі слід використовувати

напрацювання як теорії ухвалення рішень, так і теорії організації державних органів [88; 219].

Теорія ухвалення рішень у державній політиці характеризується дослідженням щонайменше шести змінних:

1) дійові особи процесу держуправління (організації та громадяни), їх цінності та сприйняття;

2) ситуації (звичайні, кризові й їх комбінації);

3) організаційна система (фіксований набір функцій та відносин основних установ, причетних до у ухвалення рішень);

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

5) громадські особи, які ухвалюють рішення (вивчаючи специфіку взаємовідносин між особами, які ухвалюють рішення);

6) власне рішення (вибір одного варіантів з кількох).

Водночас політика нацбезпеки є результатом ланцюга дій у межах організаційної структури, тобто результатом певного процесу.

Процес ухвалення та реалізації рішень складається із серії дій у межах організаційних структур, які в сукупності формують курс держуправління. Етапами цього процесу можуть бути:

– ідентифікація проблеми;

– планування її вирішення;

– ухвалення рішення;

– реалізація політики;

– оцінювання результату.

Структуру і процес ухвалення рішень у сфері нацбезпеки та їх реалізації передбачають Конституція України та державні закони [88; 91]. При цьому теорія організації державних органів надає важливого значення такій характеристиці, як сутність організації, або організаційна сутність.

Сутність організації − це точка зору самої організації, що виражається домінуючою в ній групою, на те, якими повинні бути завдання і можливості організації.

Сутність організації визначальним чином впливає на формування інтересів цієї організації. Важливими при цьому вважаються такі 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, що вважаються необхідними для їх існування; звідси тенденція до отримання максимального автономії організації;

– організації чинять опір у разі спроб позбавити їх функцій, які розглядаються як частина їх сутності;

– організація намагається вивести за свої межі функцію, яка наново з'явилася, оскільки новий персонал з новими знаннями, вміннями й інтересами може спробувати змінити сутність організації.

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

Формування системи безпеки під час НС, як з теоретичної, так і практичної точки зору, – це багатогранний, об'ємний процес, який містить у собі цілий комплекс взаємозалежних заходів. Відповідно, у цьому процесі необхідно виділити організаційні та функціональні компонент.

Зокрема, організаційна складова процесу формування згаданої системи охоплює встановлення і вдосконалення організаційної структури. Це статичний (структурний) «зріз» системи, покликаний забезпечити взаємодії елементів системи, а також її стійкість, визначеність і послідовність.

Створення системи постійних органів управління на всіх щаблях державної влади та місцевого самоврядування, спеціально уповноважених

захищати населення і території від НС, а також визначення їхніх завдань і функцій варто визнати пріоритетною сферою [174; 204].

Функціональна складова процесу формування системи забезпечення безпеки під час НС або її динамічний (функціональний) «зріз» пов'язуються з реальною практичною взаємодією, в результаті якої виникає сукупний результат всієї управлінської діяльності у сфері захисту від НС. Зазначена складова формування системи постійно потребує уваги, коригування, стимулювання та контролю, оскільки у функціонуванні системи не виникає автоматизму, раз і назавжди заданої визначеності. Зазначене зумовлюється, перш за все, об'єктом управління, який розвивається і постійно видозмінюється. Тому без сильного зовнішнього організуючого впливу система буде постійно дисфункціонувати.

Через це найважливішою складовою методології побудови системи забезпечення безпеки населення і захисту критично важливих об'єктів України у разі НС і терористичних актів є обґрунтування концепції управління цією системою [35; 129; 197].

Ґрунтуючись на положеннях загальної теорії управління складними системами, управління безпекою під час НС слід розглядати в межах певної соціально-економічної системи, яка об'єднує:

– стабільні внутрішні зв'язки населення;

– об'єкти економіки, інфраструктури, території;

– управлінські структури.

У процесі держуправління об'єктами критичної інфраструктури доречно виокремити два рівні, чи то дві ієрархічно пов'язані складові, кожна з яких характеризується певним змістом.

Перший з них (перша складова управління) охоплює управлінську діяльність аналітичного, науково-прогностичного й організаційного характеру, покликану визначати стратегії управління зовнішніми, наприклад

техногенними, впливами, й організовувати механізм їх реалізації, враховуючи соціальні, економічні та інші чинники [23; 145].

Другий рівень держуправління вказаними об’єктами стосується організаційно-технічних систем. Головними елементами системи управління на ньому є такі:

– функціональний контур і інформаційні технології;

– методи й засоби розроблення та ухвалення управлінських рішень;

– методичне забезпечення аналізу й оцінювання ризику з урахуванням соціальних, економічних тощо особливостей.

Чинники формування системи мають тісній зв’язок із виробленням основних напрямів регіональної політики у сфері забезпечення безпеки населення та захисту критично важливих об’єктів України під час НС і терористичних актів. Орієнтовну структуру цього процесу показано на рисунку. Ця схема свідчить, що вироблення регіональної політики − це широкомасштабний і багаторівневий процес. Тут необхідно враховувати величезну кількість чинників і явищ [29; 94].

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

На рівні вищого керівництва регіону на підставі аналізу загроз найважливішим інтересам в економічній, соціальній, екологічній і природно-техногенній сферах, а також оцінювання наявних для усунення цих загроз людських, фінансових, інформаційних, сировинних, енергетичних тощо ресурсів виробляються провідні напрямки забезпечення нацбезпеки в цій галузі.

Отже, на розбудову системи забезпечення безпеки населення та захисту зазначених об’єктів України під час НС і терористичних актів впливає велике коло тісно пов’язаних між собою закономірностей. Серед них доцільно виділити дві основні групи, що відбивають соціально-економічний та організаційний характер формування цієї системи [12; 72].

Так, група соціально-економічних закономірностей відбиває зв'язок між розбудовою розглядуваної системи й загальними умовами розвитку суспільства й держави (як зовнішніми, так і внутрішніми). Найважливішими з них є такі:

– відповідність організації системи рівню розвитку України, її економічному потенціалу;

– відповідність напрямів формування системи захисту від реальних небезпек в економічній, соціальній, екологічній, природній та техногенній сферах цілям державної політики сталого розвитку;

– єдність інтересів усіх груп населення стосовно захисту від НС [94; 213].

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

– пряма залежність ефективності функціонування розглядуваної системи від розвитку економічних і правових механізмів діяльності стосовно забезпечення безпеки населення та захисту критично важливих об'єктів України під час НС і терористичних актів;

– залежність організаційної структури сил системи від виконуваних нею завдань і рівня їх технічного оснащення;

– залежність ефективності управління заходами із запобігання НС та їх ліквідації від організації системи на всіх рівнях;

– відповідність організації, засобів, сил, а також фінансових і матеріальних ресурсів ступеню небезпечності та наслідкам аварій, катастроф, стихійних лих і терактів.

Закономірності формування системи реалізуються на практиці через відповідні принципи. При цьому доцільно розглядати суспільно-економічні та організаційні засади у цьому контексті. Усі вони перебувають у діалектичній єдності, доповнюються та уточнюються в міру розвитку української державності й науково-технічного прогресу, а також змін у характері та ступені загроз. Творче застосування цих принципів на практиці забезпечується науковим підходом до використання закономірностей формування системи в конкретних умовах.

Перша група − суспільно-економічні принципи. Ця група враховує реалії, що склалися на поточний момент, такі як:

– державна перебудова України;

– перебіг економічних реформ;

– загальний характер заходів із захисту від НС.

Одним із провідних соціально-економічних принципів є єдність заходів із забезпечення безпеки населення та захисту зазначених об’єктів під час НС і терактів та заходів із забезпечення регіональної безпеки. Найбільш значущими принципами у цьому контексті є такі:

– забезпечення єдності державного будівництва та формування системи;

– загального характеру заходів із захисту від НС.

Друга група − організаційні принципи створення в Україні та вдосконалення системи забезпечення безпеки населення та захисту критично важливих об’єктів під час НС і терактів, що відображають закономірність її функціонування та розвитку як особливого різновиду 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 має будуватися на єдиних принципах, за якими згадані суб'єкти повинні мати рівні повноваження.

Отже, сформульовано основні концептуальні принципи, які дозволяють розробити конкретні заходи для формування реалістичного та доступного для практичного використання регіональної політики у цій галузі [29; 145].

Забезпечення регіональної безпеки, насамперед населення та критично важливих об'єктів, − це цілеспрямована діяльність державних і громадських установ і громадян України з виявлення, запобігання загрозам безпеці та протидії їм як обов'язкова та неодмінна умова захисту інтересів регіонів нашої держави. При цьому провідними напрямами забезпечення регіональної безпеки у конкретних сферах життєдіяльності є такі.

В економічній сфері:

– забезпечення стійкого зростання економічного потенціалу України та підвищення рівня соціальної захищеності населення;

– обмеження концентрації виробництва в певних промислових зонах;

– перехід від трудомістких, енерго- та ресурсоємних галузей діяльності до передових і високотехнологічних, ураховуючи світовий досвід;

– організація сприяння товаровиробникам;

– здійснення приватизації та акціонування з огляду на інтереси регіону та населення;

– забезпечення конкурентоспроможності підприємств, підтримка їх реформування;

– сприяння фінансовому забезпеченню програм розвитку промислових підприємств;

– посилення виробничих та економічних зв’язків між різними регіонами нашої держави та країнами ближнього зарубіжжя;

– подальший розвиток транспортної мережі, насамперед магістралей.

У соціальній сфері:

– стабілізація життя населення та покращення його рівня, соціальний захист населення;

– охорона здоров’я;

– розбудова системи первинної та іншої професійної освіти та перепідготовки; організація громадських робіт для забезпечення максимальної зайнятості трудових ресурсів;

– реалізація заходів з поліпшення санітарно-епідеміологічної обстановки в регіоні;

– оптимізація співвідношення державної, муніципальної та приватної власності під час створення актуальних запасів та організації торгівлі продовольством і предметами першої необхідності;

– виконання комплексної програми заходів соціального захисту для мешканців регіону.

В екологічній сфері:

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

– зменшення техногенного впливу на навколишнє природне середовище та здоров’я населення;

– забезпечення участі громадськості в ухваленні та реалізації рішень щодо довкілля;

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

– удосконалення 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 нема відомостей про:

– об’єкт, його технічні характеристики, терміни будівництва;

– відповідальних (контактних) осіб;

– процедури або порядок ознайомлення з проєктом

а також, не ведеться реєстрація й облік висловлених думок.

Цю діяльність пропонується розвивати на основі системного підходу. Його складовими є такі:

– економічна;

– адміністративно-кримінальна (штрафи, судові розгляди);

– соціально-психологічна.

Для успішного вирішення проблеми доцільно:

– сприяти впровадженню стану показників у систему оцінювання ефективності діяльності місцевих (насамперед регіональних) органів виконавчої влади;

– поступово запровадити систему технічних регламентів та привести її у відповідність до міжнародних стандартів;

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

Наразі функції із забезпечення безпеки і контролю розосереджені серед низки міністерств і відомств. Єдиним органом, який цим займається безпосередньо (серед іншого і забезпеченням безпеки критично важливих об'єктів) має стати ДСНС України. Сьогодні на цю службу покладено ведення реєстру критично важливих об'єктів. Головними складовими системи моніторингу, від яких залежатиме вирішення покладеного на ДСНС завдання, мають бути центри моніторингу державних органів виконавчої влади та місцевого самоврядування [138; 172].

Організації, що експлуатують потенційно небезпечні об'єкти, необхідно обов'язково оцінювати на предмет готовності до запобігання та ліквідації НС (надалі − оцінювання готовності об'єктів).

Оцінювання готовності об'єктів слід проводити, враховуючи клас небезпечності об'єкта. У випадку оцінювання готовності об'єкта його слід оцінювати 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 НС. Для оцінювання допускається залучення спеціалізованих науково-дослідних, проєктних та інших організацій із відповідними ліцензіями.

В Україні здійснюється паспортизація територій та небезпечних об'єктів. Вона, звісно, стала підґрунтям для обліку та контролю над територією та особливо небезпечними об'єктами для запобігання НС та їх ліквідації. При цьому типовий паспорт безпеки небезпечного об'єкта і території має враховувати таку категорію, як критично важливі об'єкти.

Технічні регламенти висувають низку вимог до об'єктів технічного регулювання (продукція, включно з будівлями та спорудами, виробничі

процеси, експлуатація, зберігання, транспортування, продаж та утилізація). Необхідно розробити єдину національну нормативну базу відповідних проблем для оцінювання ризику критично важливих об'єктів, і цьому може допомогти їх категоріювання. Відповідно, перелік таких об'єктів, на які поширюється вимога заповнити цей паспорт, буде розширено [9; 68].

Водночас необхідно відзначити таку обставину – критично важливі об'єкти потребують насамперед запобігання НС. Через це першочерговими стають заходи фізичного захисту від зовнішніх і внутрішніх впливів. Крім того в самому забезпеченні безпеки зазначених об'єктів можна виокремити два провідні напрями:

1) захист об'єктів від зовнішніх впливів, щоб відвернути їх знищення та виникнення аварійних ситуацій;

2) захист людей та навколишнього середовища від негативних чинників, які утворюються у випадку, якщо аварія все ж таки стається.

Загалом виділяють такі основні принципи забезпечення державою безпеки та захисту критичної інфраструктури:

– захист населення і територій від різних типів НС;

– наукові дослідження і здійснення дослідно-конструкторських робіт щодо виявлення закономірностей виникнення НС згаданого вище характеру, залежності рівнів ризику та зменшення збитків від дій органів виконавчої влади, керівників підприємств та організацій різних форм власності;

– формування регіональної системи виявлення, оцінювання, прогнозування та моніторингу НС природного характеру і техногенних ситуацій;

– удосконалення заходів з ліквідації природних і техногенних НС і терористичних актів;

– підвищення рівня підготовки населення та фахівців територіальної підсистеми ДСНС України до дій із запобігання та ліквідації НС;

– розроблення та застосування економічних механізмів управління безпекою (ліцензування, декларування, страхування, визначення пільг і диференційованих ставок платежів тощо) на потенційно небезпечних об’єктах та регулювання їх діяльності для вирішення безпекових питань;

– розроблення компенсаційних заходів (відшкодування збитків за рахунок виплат за страховими полісами з благодійних, стабілізаційних тощо спеціальних фондів, державна допомога) в разі настання НС;

– ухвалення та впровадження регіональних цільових програм у розглядуваній сфері;

– управління безпекою на основі узгодженої діяльності органів державної влади на загальнодержавному, регіональному та промисловому рівнях. [138; 145].

Висновки до першого розділу

1. Установлено, що об’єктами критичної інфраструктури є об’єкти, порушення чи припинення функціонування яких здатне призвести до втрати керованості економікою України, її регіонів чи муніципалітетів, та до значного зниження рівня безпечності життєдіяльності населення, що мешкає в цих районах тривалий час.

2. Доведено, що в процесі держуправління громадськістю критичну інфраструктуру слід поділити на два рівні з певним власним змістом.

До першого рівня належить управлінська діяльність аналітичного, науково-прогностичного й організаційного характеру, завдяки якій визначаються стратегії управління зовнішніми впливами й організація механізму їх реалізації, враховуючи соціальні, економічні тощо чинники.

Другий рівень процесу громадського управління критично важливими інфраструктурними об’єктами стосується організаційно-технічних систем. На ньому рівні базовими елементами розглядуваної системи є такі:

– функціональний контур та інформаційні технології;

– методи, способи й засоби підготовки та ухвалення управлінських рішень;

– методичне забезпечення аналізування та оцінювання ризиків, враховуючи соціальні, економічні тощо особливості.

3. Визначено, що головним завданням забезпечення безпеки об’єктів критичної інфраструктури є якомога швидше отримання інформації про загрози та її використання для вжиття адекватних заходів безпеки. При цьому найважливішими стають питання обладнання й 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.

4. Зазначається, що розбудова системи забезпечення безпеки населення та захисту критично важливих об’єктів України під час НС і терористичних актів піддається впливу великого кола взаємопов’язаних закономірностей. Доцільно поділити їх на дві великі групи, що відображають соціально-економічний та організаційний характер формування цієї системи.

Так, група соціально-економічних закономірностей відбиває зв’язок між розбудовою розглядуваної системи й загальними умовами розвитку суспільства й держави (як зовнішніми, так і внутрішніми), тоді як друга група охоплює закономірності організаційного характеру, до неї належать внутрішні компоненти, притаманні лише цій системі, що є наслідком особливостей її формування порівняно з іншими державними системами та характеризує

зв’язок між її складовими та внутрішньою логікою формування кожного з її компонентів.

5. Показано, що прогноз наслідків НС для об’єктів критичної інфраструктури бажано здійснювати в декілька етапів.

На І етапі встановлюють параметри впливів − значущих уражальних чинників, що спричинюють основні руйнування й ураження, з характеристиками, що зазвичай обираються з використанням існуючих методик.

На ІІ етапі встановлюють закони ураження − опору елементів ризику впливів, під якими розуміють залежності ймовірності ураження від інтенсивності прояву уражальних чинників, застосовуючи для їх формалізації ті чи інші функції, що відповідні цій надзвичайній ситуації.

На ІІІ етапі прогнозування дається оцінювання наслідків сполучення моделей впливу і законів ураження (руйнування / пошкодження). З використанням цього методологічного підходу оцінюються наслідки майже всіх стихійних лих і техногенних аварій, що необхідно для обґрунтованого ухвалення рішень про організацію екстреної евакуації населення з районів НС і забезпечення його життєдіяльності у безпечних районах, а також залучення для ліквідації НС сил і засобів ДСНС України різного рівня. Конкретний вплив різних чинників на об’єкти критичної інфраструктури та людей під час аварій і катастроф з можливими їх наслідками описується за допомогою відповідних моделей.

РОЗДІЛ 2
ОЦІНКА ПОТОЧНОГО СТАНУ ТА ВИКЛИКІВ ДЕРЖАВНОГО УПРАВЛІННЯ ЗАБЕЗПЕЧЕННЯМ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1. Закордонний досвід державного управління забезпеченням безпеки критичної інфраструктури

Сама теми цього дослідження вимагає розглянути досвід діяльності державних органів різних країн світу щодо захисту критичної інфраструктури, зокрема і в кризових умовах [21; 184].

Насамперед у цьому контексті варто розглянути досвід формування системи антикризового управління в США, особливо її територіальної складової. Серія терористичних актів, що сталися в різних країнах, об'єктивно вимагали від керівництва США перегляду підходів до організації антикризового управління. Заява Адміністрації США від 1 березня 2003 року про заснування Єдиної національної системи управління в умовах надзвичайних ситуацій та відповідний комплекс організаційних заходів стали дуже серйозною частиною підготовчої роботи 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 негайного реагування на існуючу загрозу.

Під час навчань з відбиття терористичних атак із застосуванням хімічних та біологічних уражальних речовин, було виявлено такі недоліки:

– 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 представників 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 уражальних чинників;

– неефективність наявних профілактичних заходів щодо запобігання виникненню та нейтралізації паніки серед населення [126; 154].

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 змогу швидко і точно визначити патоген або токсикант, що використовується;

– персонал служб протидії актів технологічного тероризму повинен володіти відповідними знаннями й оснащенням 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, що ґрунтується на списку найбільш імовірних патогенів і хімічних отруйних речовин;

– ураховуючи, що біотехнологія надає найширші можливості для зниження наслідків терактів, здійснити дослідження і розроблення медикаментів, вакцин і діагностичних засобів нового покоління [15; 21; 129].

Ці дані свідчать про те, що захист населення та критичної інфраструктури від терактів, здійснюваний спецслужбами і правоохоронними органами, не відіграє головної ролі в загальному комплексі заходів, покликаних підвищити безпеку. У США були актуальними:

– попередження незаконного втручання в роботу критичної інфраструктури;

– пом’якшення можливих негативних наслідків;

– загальне підвищення життєздатності та стійкості функціонування критичної інфраструктури в різноманітних надзвичайних і кризових ситуаціях.

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

Уже 21 вересня 2001 р., виступаючи перед конгресом, президент Буш заявив про необхідність створення нового федерального відомства − Міністерства внутрішньої безпеки, яке координувало б роботу багатьох органів, що займаються питаннями безпеки. Створення Міністерства ознаменувало 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.

У межах 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 і професійну підготовку [131; 200; 232].

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

Конгресом США вжиті безпрецедентні для США юридичні заходи зі зміцнення внутрішньої безпеки. Одразу після вчинення терактів і до кінця 2001 року він ухвалив десять законопроєктів і резолюцій щодо міжнародних та внутрішніх юридичних аспектів боротьби з тероризмом.

Крім того, на розгляді палат конгресу тоді 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, серед іншого із собаками і міношукачами, в будь-яку пору доби.

Закон розширив визначення тероризму, а також дозволив притягати до судової відповідальності не лише за вчинення терактів, 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 НС, в яких повинні відображати основні заходи всіх органів державного та військового управління на території США та щодо підготовки до дій у разі настання кризи.

Усе це було спрямовано на підвищення готовності федеральних та місцевих органів влади і приватного сектору реагувати на широкий спектр різних загроз критичній інфраструктурі. Очікується помітна активізація роботи над формуванням єдиної національної системи антикризового управління через посилення терористичної загрози та проблеми, що стосуються реконструкції повоєнного Іраку [15; 239].

Водночас говорити про ефективність єдиної національної системи управління в умовах кризових ситуацій, що досі формується, зараз ще зарано, як попередня діяльність федеральних відомств США свідчила про значний ступінь децентралізації організації кризового управління, а також превалювання у розглянутій сфері економічних механізмів над організаційними.

Характерною особливістю законодавства США є надання права губернаторам штатів оголошувати особливий режим в разі виникнення надзвичайної або іншій кризової ситуації.

Згідно із законами штату, які є різними в кожному зі штатів США, губернатор оголошує стан надзвичайної ситуації або надзвичайний стан або виданням спеціального указу, або шляхом повідомлення про це через ЗМІ (декларацію). Указ або декларація зазвичай містить опис причин такої НС, її розташування всередині штату і повноважень, відповідно до чого губернатор оголошує надзвичайну ситуацію або надзвичайний стан.

Звичайно, реагування часто починається до офіційного оголошення і без декларації про надзвичайну ситуацію (надзвичайний стан). Частіше за все губернатори користуються цим правом тільки якщо їм потрібні особливі екстрені повноваження або вони хочуть запросити президентську декларацію про НС. Хоча закони в різних штатах варіюють, така декларація зазвичай надає губернатору особливі, 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).

Водночас, 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 необхідність може бути логічним

обґрунтуванням для оголошення НС, навіть якщо реально реагування об'єктивно не потрібне. Це також може забезпечити політичний тиск, потрібний для оголошення надзвичайного стану (надзвичайної ситуації) у ситуації, коли немає інших гарантій для офіційного оголошення такої ситуації [184, 212].

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.

Варто розглянути досвід організації управління охороною населення та об'єктів економіки на територіальному та місцевому рівнях в умовах НС і в інших країнах.

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

Перший – це ухвалення нових законів і запровадження нових керівних органів чи підрозділів в існуючих структурах держуправління (як-то Міністерство оборони чи Міністерство внутрішніх справ).

Інший шлях полягає в узгодженні, приведення у відповідність до вже наявних нормативних актів і посилення координації роботи державних, приватних і громадських організацій щодо запобігання та ліквідації НС [102; 145].

Так, цивільна оборона Великобританії структурно входила до Міністерства внутрішніх справ і вирішувала обмежене коло питань, що стосувалися усунення наслідків повітряних нападів противника. Тому новий закон про цивільну оборону Великобританії, ухвалений у 2003 році, замість того, що діяв з 1948 року, мав за мету встановити права й обов'язки громадян, державних структур і недержавних установ у сфері цивільної оборони, а також порядок дії під час ліквідації наслідків стихійних лих і терактів.

Ухвалення у Великобританії нового закону, який розширив традиційні завдання цивільної оборони, з ухилом у вирішення проблем мирного часу, свідчить про реакцію уряду на загальносвітове посилення загрози тероризму, серед іншого у зв'язку з подіями в Іраку.

Екологічна експертиза та ліцензування підприємств були законодавчо закріплені в більшості західноєвропейських держав, зокрема в Ірландії, Франції, Швейцарії тощо.

Так, у Швеції нове законодавство про управління під час НС передбачає забезпечення зменшення наслідків аварій і катастроф за рахунок превентивних заходів та заходів реагування на НС відповідними службами підприємств і муніципалітету. У 1986 році в цій країні почало працювати Національне управління рятувальних служб, яке координує діяльність 284 органів місцевого самоврядування та служб.

Також у Західній Європі діє регіональна система підготовки та оповіщення про великі аварії на промислових підприємствах, що охоплює всі держави-члени ЄС [184; 216].

Водночас у більшості країн між першими двома групами нормативно-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, зорієнтовані на роботу у воєнному стані.

Загалом аналіз організаційно-правових баз держуправління захистом критичної інфраструктури під час надзвичайних та/або кризових ситуацій у США і країнах Західної Європи дозволив виокремити такі основні його риси:

– системи управління діями у згаданих ситуаціях мають державний статус;

– діяльність з попередження та ліквідації кризових ситуацій вважається важливою соціальною функцією держави і реалізується більшістю її структур;

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

– заходи захисту критичної інфраструктури під час НС фінансуються головним чином за рахунок державних програм;

– акценти в правовому регулюванні ризику дедалі сильніше зсуваються у бік превентивних заходів.

Загалом зарубіжний досвід є значущим для формування перспективної системи громадської безпеки та захисту критично важливих об'єктів під час НС. Політичні й економічні умови в Україні та продовження реформування системи управління на національному та регіональному рівнях об'єктивно зумовлюють необхідність пошуку оптимального варіанту для подальшої розбудови цієї системи [29; 144].

Межі використання зарубіжного досвіду для розробки системи громадської безпеки та захисту зазначених об'єктів під час НС і терористичних актів на згаданих вище рівнях визначатимуться перебігом адміністративної реформи в Україні й особливостями державної влади в найближчі роки.

Окремо варто зупинитися на забезпеченні кібербезпеки критичної інфраструктури в різних країнах. Специфіка різних сфер, віднесених до критичної інфраструктури, вимагає особливої уваги під забезпечення безпеки. Для кожної конкретної сфери заходи захисту, що застосовуються, повинні відповідати цілям безпеки, що часто суперечать принципам конфіденційності або доступності інформаційних ресурсів тощо [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 заходи захисту, та представників конкретних підприємств.

Особливо актуальною проблема організації такої взаємодії є для приватних підприємств. Програми партнерства державного та приватного секторів у розглядуваній сфері зазвичай спрямовано на вирішення саме цієї проблеми [28; 203].

Наявність зрілих механізмів 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. Тому цікаво простежити та порівняти показники зрілості управління кібербезпекою на державному рівні, наприклад, використовуючи дослідження досвіду зарубіжних країн.

Так, доцільно проаналізувати профіль з кіберблагополуччя Міжнародного союзу електрозв'язку для 196 країн. Для орієнтовного оцінювання зрілості механізмів управління кібербезпекою критичної інфраструктури розглядали такі заходи, які реалізуються на державному рівні:

– чи є офіційно ухвалена стратегія або політика кібербезпеки критичної інфраструктури;

– чи створено офіційне відомство, відповідальне за забезпечення такої безпеки;

– чи створено офіційне відомство, відповідальне за повідомлення і обробку інцидентів кібербезпеки у критичній інфраструктурі;

– чи існує офіційно ухвалена програма міжвідомчого співробітництва у розглядуваній сфері;

– чи існує офіційно ухвалена програма державно-приватного співробітництва у розглядуваній сфері (рис. 2.1).

Поєднання цих параметрів визначає рівень зрілості управління кібербезпекою критичної інфраструктури.

Тим не менш, тип стратегії управління кібербезпекою зазначеної інфраструктури визначають не один чи декілька з цих параметрів, а роль відомства, офіційно відповідального за національну кібербезпеку цієї інфраструктури, в процесі реалізації заходів захисту критичних ресурсів від кібератак [38; 194].

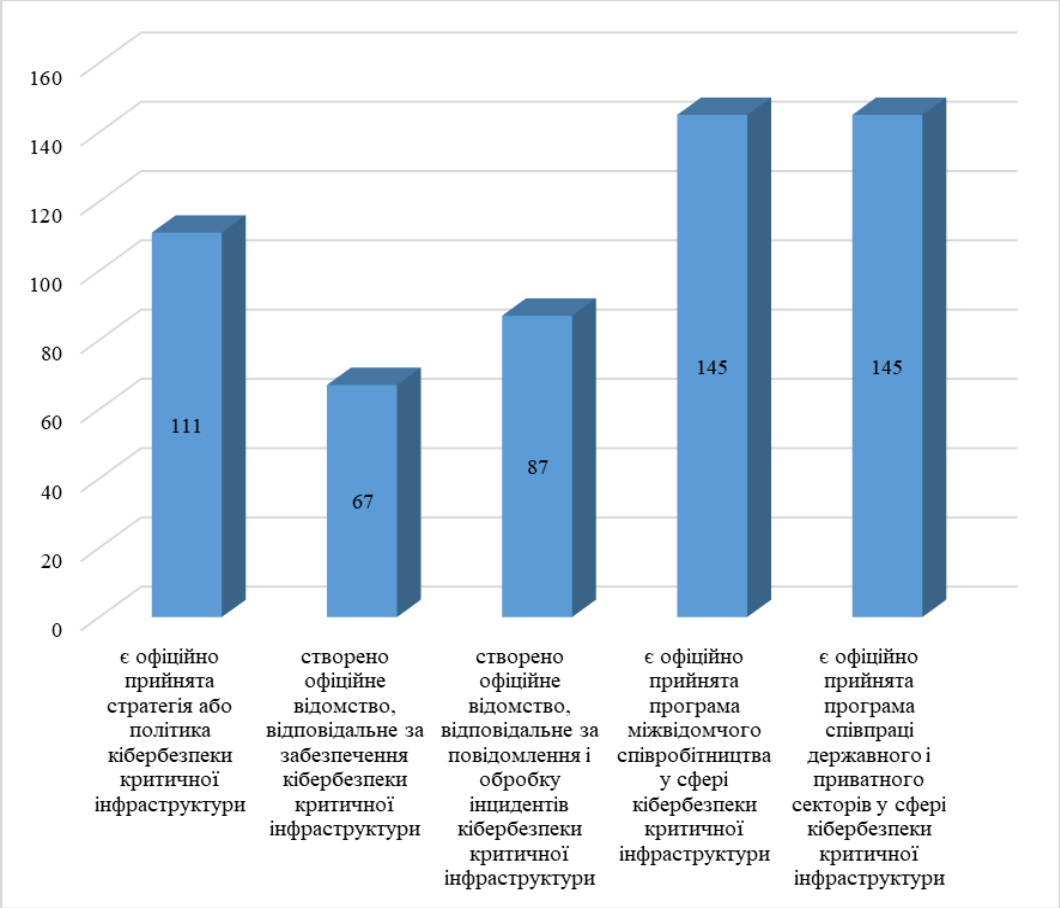

Рис. 2.1. Профіль з кіберблагополуччя Міжнародного союзу електрозв’язку для 196 країн, кількість країн

До компетенції вказаного відомства, як правило, належать такі обов’язки:

– здійснювати управління діяльністю із забезпечення кібербезпеки критичної інфраструктури на державному рівні;

– забезпечувати взаємодію між відомствами, інтереси яких зачіпаються питаннями такої кібербезпеки;

– ухвалювати підзаконні нормативно-правові акти, що регулюють заходи кіберзахисту критичної інфраструктури;

– визначати критерії ідентифікації та ідентифікувати життєво важливі системи;

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

– описувати і по змозі підтримувати процеси кібербезпеки цієї інфраструктури (такі, як повідомлення про інциденти);

– оцінювати кібербезпеку систем і сертифікувати продукти кіберзахисту згідно з установленими критеріями;

– сприяти співпраці між державним та приватним сектором у розглядуваній сфері.

Аналіз практики управління кібербезпекою критичної інфраструктури з погляду взаємодії між державою і приватним сектором дозволив визначити три основні типи стратегій цього управління, розглянуті нижче. Як правило, вибір конкретної стратегії визначається спільною розробкою регулюючих і виконавчих органів у галузі нацбезпеки, 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. Решта установ може консультувати цей департамент або брати участь у заходах, дотичних до забезпечення такої кібербезпеки, але не чинять вирішального впливу на регулювання цієї діяльності. Цей підхід реалізується, наприклад, у Німеччині, Італії, Чехії та Естонії.

Заходи щодо забезпечення безпеки зазвичай добре документуються і, як правило, застосовуються до всіх галузей відповідальності керівництва, крім прямо визначених у законодавстві випадків.

Головне управління займається питаннями кібербезпеки критичної інфраструктури на державному рівні і, як правило, також відповідає за її захист від кібератак. Для цього воно на підзаконному рівні формулює директиви та рекомендації, встановлює вимоги до сертифікації, розробляє відповідні керівні документи та підтримує довгострокові державні програми (такі, як програма UP Kritis у Німеччині) [21; 77; 82].

Цей централізований підхід закріплено 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, що відповідає за захист найважливіших інформаційних інфраструктур на федеральному рівні. Його діяльність контролюється Федеральним міністерством внутрішніх справ. Оскільки захист критичної інфраструктури розглядається як мережеве завдання з участю різних органів на різних рівнях, усі відповідні програми та ініціативи кібербезпеки координує Федеральне відомство з питань інформаційної безпеки Німеччини.

У Чехії основним органом є Управління Національної Безпеки, яке відповідає за кібербезпеку критичної інфраструктури, захист класифікованої інформації, управління допусками безпеки та управління криптографічним захистом. Власне захист цієї інфраструктури здійснює Національний центр кібербезпеки, що є структурною частиною цього ж управління. У разі значного інциденту, що стосується кібербезпеки, Управління виступає провідним повноважним органом, який координує роботу інших відомств з вирішення цього інциденту (включно з різними державними та приватними установами). При цьому діяльність різнохарактерних суб'єктів залежить від рішень Управління національної безпеки у разі оголошення надзвичайного стану і може здійснюватися у процесі усунення загрози кібербезпеки або її наслідків. Управління підтримує операторів критичної інфраструктури під час настання НС і в разі потреби забезпечує розслідування інцидентів [21; 22; 168].

У деяких державах спеціального регулятора у сфері кібербезпеки критичної інфраструктури не існує, натомість у них офіційні представництва наділяються широкими повноваженнями з підтримки безпеки в національному кіберпросторі. Одним з прикладів є Латвія. Її національний орган із захисту критичної інфраструктури (Інститут реагування на інциденти безпеки інформаційної технології Латвійської Республіки) поділяє координуючу роль зі Службою державної безпеки й Бюро із захисту Конституції в межах Міністерства оборони. Ці органи співпрацюють стосовно оцінювання і управління поточними інформаційними ризиками для критичної інфраструктури. Бюро із захисту Конституції 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 уразливості та пов'язаних з цим ризиків та давати рекомендації зацікавленим сторонам щодо усунення виявлених

недоліків, а також може давати рекомендації державним установам, які контролюють власників об’єктів критичної інфраструктури. Бюро спільно з Інститутом реагування на інциденти безпеки інформаційної технології Латвійської Республіки періодично інформує Національну Раду Безпеки Інформаційних Технологій про актуальні загрози критично важливій інфраструктурі.

У принципі, активна співпраця регулятора і національного органу із забезпечення кібербезпеки такої інфраструктури є показником відкритості регулятора, його обізнаності про короткострокові галузеві потреби у заходах безпеки та готовності будувати відносини із 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. В 11 з цих 90 країн він і є згаданим вище уповноваженим органом (це досить непоганий показник розподілу обов’язків у більшості країн). Якщо розглянути лише ті країни, що мають офіційно ухвалену стратегію або політику кібербезпеки критичної інфраструктури, то залишиться тільки 64 із 196 країн, для яких складено профілі кіберблагополуччя. Серед цих 64 лише 7 країн не розрізняють спеціалізований і основний орган, відповідальний за питання кібербезпеки такої інфраструктури.

Отже, 64 держави із 196 демонструють зрілий підхід до управління кібербезпекою критичної інфраструктури (рис. 2.2).

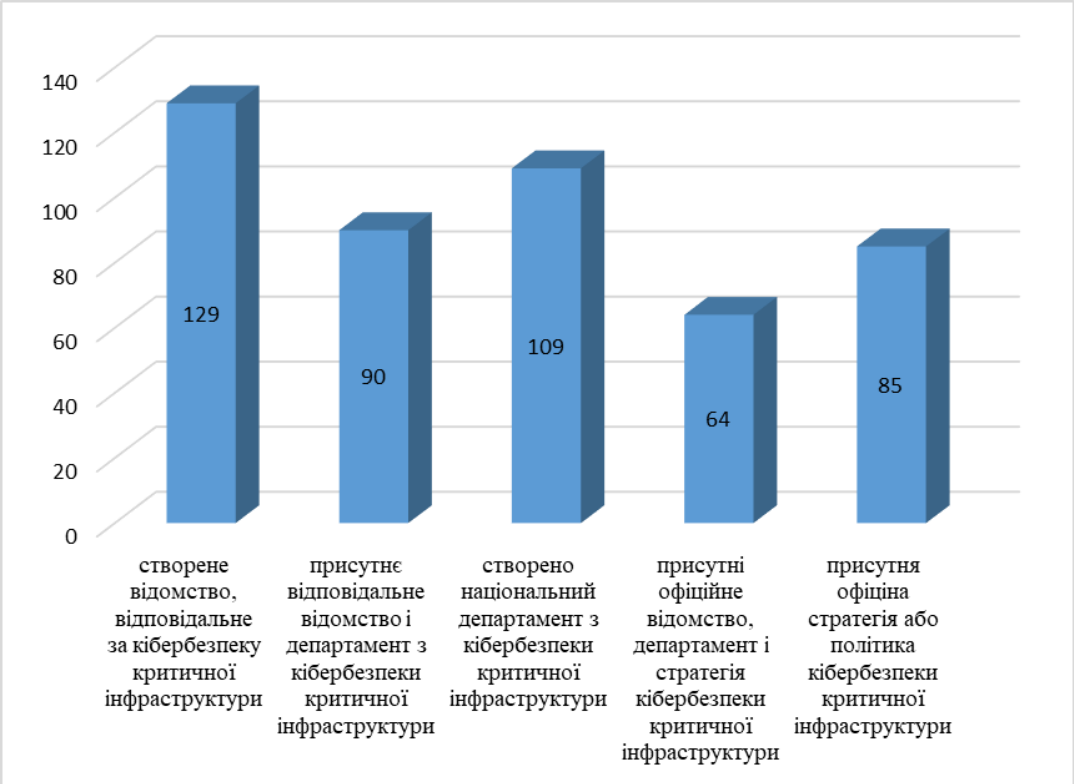

Рис. 2.2. Розподіл індикаторів зрілості управління кібербезпекою критичною інфраструктурою у країнах світу, кількість країн

Якою б не була організаційна форма головного управління, ця стратегія часто стикається з проблемами побудови відносин із приватним сектором, що найчастіше пояснюється єдиними вимогами до впровадження і реалізації процедур та заходів з кібербезпеки незалежно від специфіки конкретної галузі критичної інфраструктури. Представники сфери цієї інфраструктури можуть сумніватися в тому, що фахівці з кібербезпеки є достатньо компетентними в їхній галузі для використання будь-яких механізмів, або побоюються, що ті можуть не побачити зв'язку між кібератаками та можливими фізичними збитками. Власники приватних об'єктів, класифікованих як критична для забезпечення кібербезпеки інфраструктура, можуть неохоче ділитися інформацією про випадки порушення кібербезпеки [15; 23; 194].

Без залучення представників кожної конкретної сфери критичної інфраструктури розроблення заходів захисту такої інфраструктури може почати орієнтуватися на хибні цілі безпеки та ігнорувати практичний досвід, установлюючи вимоги, які важко виконати через наявні обмеження. Щоб вирішити це питання деякі країни диверсифікують методи захисту критичної інфраструктури, залучаючи в процес захисту її зацікавлені сторони такої інфраструктури.

Наприклад, німецький регулятор Federal Office for Information Security реалізує згадану раніше програму UP Kritis. Зазначена програма UP Kritis також оперує поняттями, які виходять за межі сфери інформаційних технологій для підтримання доступності і зміцнення надійності критично важливої інфраструктури. Для забезпечення всебічного захисту такої інфраструктури слід спільно розробляти та впроваджувати заходи щодо фізичного захисту та забезпечення безпеки інформаційних технологій. У межах UP Kritis успішно реалізується співпраця між галузями промисловості та державою. Організації-учасниці програми співпрацюють за принципом взаємної довіри. Вони обмінюються ідеями та досвідом і навчаються одна в одної забезпеченню захисту цієї інфраструктури, діють разом і завдяки цьому знаходять найкращі рішення. У межах UP Kritis також розробляються нові концепції, встановлюються контакти, робляться вправи, розробляється і використовується спільний підхід до антикризового управління інформаційними технологіями [21; 227].

За даними Міжнародного союзу електрозв’язку, в 51 країні зі 196 була реалізована офіційна програма або ініціатива щодо міжвідомчої співпраці з питань кібербезпеки критичної інфраструктури. Водночас у 51 країні певною мірою було реалізовано програму обміну інформацією між державою та приватним сектором, що стосується кібербезпеки такої інфраструктури. В обох випадках майже в третині країн ці ініціативи підтримуються спеціальними

управліннями захисту цієї 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

У цьому випадку захист критичної інфраструктури перебуває в компетенції декількох відділів і груп, що співпрацюють, або міжвідомчого комітету. 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

У цьому випадку відповідальність за безпеку критичної інфраструктури лежить на одному відомстві або розподіляється між декількома. Саме так функціонує система захисту такої інфраструктури в Австрії, Франції, Польщі, Фінляндії, Австралії, Канаді та багатьох інших країнах.

Зокрема, в Австрії на стратегічному рівні відповідальність за захист критичної інфраструктури розподіляють Федеральна канцелярія Австрії та Федеральне міністерство внутрішніх справ. За управління та координацію роботи різних відомств відповідає 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 містить у собі кілька державних установ, найважливішими з яких є:

– 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 охоплює приватні організації та національні департаменти, специфічні для сфери критичної інфраструктури [23; 189].

Відомством, що координує захист найважливіших складових такої 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, а керує нею прем'єр-міністр Франції. Ще одне утворення − ANSSI (франц. «Agence nationale de la securite des systemes d information») − міжвідомче агентство, яким керує Стратегічний комітет SGDSN. Ці два основні агентства відповідають за всі форми захисту критичної інфраструктури. Офіційно у них немає інших форм

співпраці з іншими державними установами. ANSSI співпрацює з приватним сектором у вісімнадцяти різних робочих групах з таких питань:

– 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 за захист критичної інфраструктури відповідає насамперед Центр державної безпеки (RCB), і всі відповідні заходи підтримуються через форуми співпраці між державними органами й операторами критичної інфраструктури. Засідання представників відповідних міністерств для обговорення питань захисту такої інфраструктури проводяться кожні кілька місяців. Крім того, експертна група представників урядових установ збирається кожні два тижні для підготовки рекомендацій для Державного секретаря. Офіційно ухвалена Політика захисту кіберпростору Республіки Польща передбачає дії, що стосуються безпеки інфраструктури інформаційних критичних технологій і власне захисту критичної інфраструктури (норми регулювання останніх містяться в Національній програмі захисту критичної інфраструктури). У Стратегії національної безпеки Республіки Польща, зокрема, зазначається, що захист критичної інфраструктури належить до обов'язків операторів і власників, і їх відповідальність підтримується державною та адміністративними можливостями.

У Фінляндії єдиного органу, відповідального за захист всіх секторів критичної інфраструктури, немає. Більша частина цієї інфраструктури цієї держави перебуває в суспільстві у приватній власності бізнесу, що відображено у Стратегії кібербезпеки Фінляндії. Ноу-хау та експертиза у сфері кіберсистем, а також послуги та засоби захисту значною мірою належать приватним компаніям. Національне законодавство у сфері кібербезпеки такої інфраструктури покликано 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, серед іншого за безперервність функціонування національної критичної інфраструктури. Іншими специфічними для сфери цієї інфраструктури органи є 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 більшою мірою орієнтовано на поділ обов'язків, і в деяких випадках – на партнерство відповідального за кібербезпеку критичної інфраструктури органу і відомств, обізнаних про особливості її конкретних складових. Кожне таке відомство несе відповідальність за вибудовування відносин з великими підприємствами регіону, важливими в цьому регіоні [15; 82].

У разі такого підходу визначення цілей безпеки для кожної складової критичної інфраструктури вимагає менше зусиль. Водночас 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 повне передання відповідальності власникам та операторам об'єктів критичної інфраструктури. Цей підхід реалізує, наприклад, Ірландія. Стратегія кібербезпеки Ірландії декларує таке: «внаслідок наявності 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.

Швейцарія також реалізує принцип субсидіарності у кіберзахисті критично важливої інфраструктури. Там 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, а також за вжиття всіх відповідних заходів протидії. Уряд максимально сприяє процесам захисту критичної інфраструктури, а її оператори самостійно несуть відповідальність за власну безпеку, держава ж при цьому реалізує підтримуючі заходи.

Центр обліку та аналізу захисту інформації є національним інформаційним центром для обміну даними про загрози та інциденти між приватним і державним секторами і водночас – головним органом у галузі кіберзахисту критичної інфраструктури Швейцарії, але використовується він здебільшого для підтримки у випадку інциденту.

Єдине відомство, відповідальне за кібербезпеку, здатне встановити межі, в яких кібербезпека критичної інфраструктури покращуватиметься в усіх галузях такої інфраструктури. Головною проблемою при цьому є те, що пропоновані в цих межах заходи захисту можуть не відповідати потребам кожного конкретного сектора [68; 93].

Водночас підхід, що ґрунтується на саморегуляції, ідеально відповідає різноманітності потреб критичної інфраструктури, але в цьому разі неможливо уникнути інцидентів кібербезпеки, багато з яких матимуть серйозні наслідки, якщо критична інфраструктура буде пошкоджена. Метод управління кібербезпекою критичної інфраструктури, за якого до відповідних процесів залучається 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 дотримання вимог до забезпечення кібербезпеки цієї інфраструктури здійснюється лише стосовно найважливіших підприємств та організацій, компрометація яких може мати значні наслідки на національному рівні. Цей підхід використовує, наприклад, уже згаданий французький регулятор ANSSI.

Вимоги до реалізації заходів захисту, рекомендованих для підприємств критичної інфраструктури, встановлюються водночас із пільгами для підприємств середнього рівня критичності, однак у разі нехтування цими вимогами і в разі виникнення інциденту кібербезпеки передбачається 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 такі підприємства та об’єкти повною мірою використовують

інформаційні і комунікаційні технології, включно з 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. Тобто йдеться про незалежне партнерство за участю третьої сторони між державним та приватним сектором у розглядуваній сфері (перший учасник – уповноважене відомство, другий – представники секторів цієї інфраструктури). Взаємодія з експертною стороною забезпечує поінформованість про актуальні загрози і методи захисту від них, що відповідає спеціальним потребам секторів критичної інфраструктури.

Стратегія управління кібербезпекою цієї інфраструктури може вибиратися завдяки такій інформованості лише тими державами, які перебувають на самісінькому початку цього шляху. За даними Міжнародного союзу електрозв'язку, офіційний департамент із захисту критичної інфраструктури у тому чи іншому вигляді працює в більшості держав. Також цей орган через відсутність державного регулятора може офіційно або неофіційно виступати у ролі відомства, відповідального за всі аспекти національної кібербезпеки. 150 країн розпочали діяльність із забезпечення кібербезпеки на національному рівні (принаймні мають або стратегію та офіційний орган, відповідальний за ці питання, або відповідний департамент), із них 64 мають водночас 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 логічно застосувати для своєчасного усунення недоліків цих стратегій. Методи, що застосовуються в межах 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 її кіберзахисту.

Водночас ключові компанії, незалежні дослідники та відділи захисту критичної інфраструктури починають займати ключову позицію у відносинах між державою та приватним сектором у сфері кібербезпеки цієї інфраструктури. Часто саме вони сприяють на глобальному рівні обміну сучасними законодавчими, оперативними й технічними практиками кіберзахисту (наприклад, завдяки стандартизації та адаптації посібників, що документують ці практики), і це врешті-решт посилює кібербезпеку зазначеної інфраструктури в усьому світі [66; 71; 227].

2.2. Особливості 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 на сучасному етапі відповідної системи держуправління та місцевого самоврядування [46; 52].

Однак аналіз та оцінювання стану вітчизняних державного та місцевого управління, а також розроблення пропозицій на тему його розвитку

ускладнюються неоднозначністю низки суспільно-політичних та економічних проблем, які служать об'єктивними підставами безпосередньо для розвитку держуправління 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, серед яких виділяють доіндустріальний, індустріальний, постіндустріальний та інформаційний. Також воно дуже відрізняється за географічною та національною ознаками. У 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].

У 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 є невіддільним від використання певних засобів, ресурсів, форм і методів, і часто останні чинять вирішальний вплив на результати реалізації цілей. Історичних прикладів на цю тему достатньо. Це питання безпосередньо торкається і функцій держуправління, 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 держуправління та місцевого самоврядування формуються 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 нині перед державним управлінням в Україні постали такі цілі (зокрема, стосовно безпеки критичної інфраструктури) [45; 53]:

1) адміністративна реформа – формування нових та вдосконалення вже наявних інститутів державної влади (зокрема, системи виконавчої влади);

2) розгортання та зміцнення громадських інститутів, завдяки яким у державі досягається стійка демократія;

3) створення та втілення в життя соціальних та адміністративно-правових регуляторів, які гарантують задекларований у Конституції комплекс прав, свобод та обов'язків громадян України;

4) розроблення та практична реалізація державної політики щодо забезпечення безпеки населення та захисту об'єктів критичної інфраструктури;

5) захист внутрішньої і зовнішньої безпеки та забезпечення сприятливих мирних умов для життєдіяльності регіонів України;

6) досягнення збалансованого і взаємопов'язаного розвитку регіонів у взаємодії з центром на основі поглиблення процесів формування і функціонування загальноукраїнського ринку.

Проблема встановлення цілей забезпечення безпеки критичної інфраструктури у державному управлінні вбачається не стільки в постановці та формулюванні окремих цілей, які держава покликана реалізовувати, скільки в побудові «дерева цілей», у якому різні стратегічні й тактичні, загальні й окремі, завершальні та проміжні, віддалені та близькі тощо цілі зможуть узгоджуватися, поєднуватися і становити певну логічну цілісність. Також важливо з'єднати

«дерево цілей» з необхідними й 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.

Для відповіді на питання про зміст і структуру функцій держуправління у сфері забезпечення безпеки населення та захисту об'єктів критичної інфраструктури спочатку треба визначити місце та роль регіонів України в конкретній галузі життєдіяльності. Саме місце і роль регіону зумовлюють його зміст і форму, а вже потім – функції управління та інші його прояви [110; 137; 220].

Зокрема, під функціями державного та місцевого 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, включно із свідомістю, поведінкою та діяльністю людей.

Сьогодні всі питання держуправління як ніколи зосереджуються на проблемі забезпечення нацбезпеки України, однією з головних складових якої є забезпечення безпеки критичної інфраструктури. Питання управління безпекою в різних сферах життєдіяльності, пошук ефективних способів вирішення завдань, що постали перед суспільством, відповідають інтересам усього населення та цікавить учених і 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 слід усвідомлювати, що вони чинять суттєвий вплив на стан економічного та соціального забезпечення та екологічний стан.

При цьому набір функцій держуправління залежить від стану та структури керованих процесів – сукупності керованих об'єктів і водночас – від місця та ролі держави у сферах життєдіяльності. Держава є пов'язаною із суспільством, відповідно, напрями її розвитку 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» із 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].

У 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 держуправління у сфері забезпечення безпеки населення та захисту об'єктів критичної інфраструктури, в цій роботі доцільно

виходити з аналізу всіх чинників, які сьогодні впливають на взаємозв'язок держави та суспільства, й на ту обставину, що громадянське суспільство наразі не готове взяти на себе функції, що виконуються державними структурами. Протистояти впливу НС на сталий розвиток України наразі можна лише завдяки стратегічній ролі держави у цьому процесі [46; 49; 52].

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

Це є особливо важливим в контексті оптимізації функцій органів виконавчої влади регіонів України в межах адміністративної реформи. Відмова від функцій планування і контролю в держуправлінні, зокрема стосовно забезпечення безпеки критичної інфраструктури, де довгостроковий (стратегічний) погляд є вкрай необхідним, навряд чи виправдано, тому що десятки мільйонів людей беруть участь у соціальних процесах, якими управляє держава.

На управлінській практиці позначаються ігнорування і недооцінювання 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.

Зауважимо, що держуправління на рівні регіону України в теоретичному плані достатньою мірою не вивчено. У 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 об'єктів під час НС і терористичних актів не може здійснюватися без здійснення специфічних функцій управління, тих, які притаманні саме державі й повинні реалізовуватися за допомогою управлінських функцій спеціальних державних органів.

Наукова методологія потребує врахування особливостей державного управління та місцевого самоврядування в Україні щонайменше в чотирьох аспектах:

1) з урахуванням існування у країні орієнтацій на давні традиції, зокрема щодо політичної культури населення і правлячих груп (претендентів на владу), що певною мірою визначають реалізацію розглянутої проблеми; не обов'язково, щоб ці традиції визначали процес держуправління, однак безсумнівно, що їх заперечення у нинішній ситуації в кінцевому рахунку створює тупикову ситуацію;

2) урахування сьогоднішнього соціально-політичного та економічного становища – аналіз цього чиннику є необхідним, бо він дозволяє, з одного боку, вибудовувати розроблення рішень поставленої проблеми на реальному фундаменті, а з іншого – надає можливість урахувати скороминуще, характерне лише для сьогоднішнього моменту, а також зосередитися на дійсно ключових

проблемах оптимізації механізмів і структур держуправління, зокрема стосовно забезпечення безпеки критичної інфраструктури;

3) урахування глобального аспекту завдань держуправління, що вирішуються в Україні – світовий досвід дає не тільки і не стільки знання про можливі рішення конкретних управлінських завдань, насправді глобальний контекст дозволяє вибудовувати пропоновані рішення так, щоб спрогнозувати світові поточні тенденції, зберегти українську самобутність і використовувати дійсно оптимальні варіанти вирішення проблем держуправління, зокрема стосовно забезпечення безпеки зазначеної інфраструктури;

4) використання загальнонаукового принципу подвійної герменевтики, тобто подвійної інтерпретації вирішення дослідницької проблеми, яка зараз є ключовою: суворо науковий аналіз проблем держуправління з урахуванням фундаментальних аспектів проблеми, новітніх наукових розробок тощо стосовно держуправління у розглядуваній сфері забезпечення безпеки [46; 54; 78].

В умовах загострення загроз природного та техногенного характеру і підвищення ймовірності вчинення терактів першорядного значення набуває питання підвищення охорони критично небезпечних та потенційно небезпечних об’єктів. Аналіз життєвого циклу та чинників небезпеки зазначених об’єктів дозволяє говорити про імовірнісний характер небезпек, що виникають під час поводження з небезпечними речовинами.

Так, дослідження низки робіт показують, що джерело небезпеки може мати природне, космічне, технічне або соціально-економічне походження. До найнебезпечніших джерел виникнення подій надзвичайного характеру належать такі:

– несприятливі природні явища;

– стихійні лиха та природні катастрофи;

– природні ризики, спричинені господарською діяльністю людини та пов’язані з накопиченням екологічних збитків;

– техногенні аварії та катастрофи і терористичні прояви [34; 148; 182].

Загроза пошкодження критично важливого інфраструктурного об’єкта залежить від взаєморозташування у просторі та часі (для стаціонарних об’єктів – лише у просторі) джерела небезпеки й того об’єкта, на який воно впливає. Водночас небезпеки становлять загрозу лише тоді, коли вони можуть заподіяти шкоду конкретним об’єктам. Відповідно, небезпека (і так само кілька різних небезпек) становитиме загрозу для зазначеного об’єкта інфраструктури, лише в тому разі, якщо її (їх) небезпечні чинники мають можливість на цей об’єкт впливати. Наприклад, для людей загроза виникає за умови, що вони працюють на об’єкті підвищеної небезпеки чи в зоні забруднення, а для рухомих об’єктів – якщо вони під час небезпечної події перебувають у зоні впливу небезпечних чинників [91; 179].

Ступінь загрози життю населення в певній місцевості й, відповідно, критичній інфраструктурі зумовлюється ступенем її небезпечності, а також географічними та часовими чинниками. Якщо перенести такий об’єкт за межі небезпечної території, загроза для нього зникне, хоча небезпечність території не зміниться. Загроза життєдіяльності змінюється з часом: вона може виникати, збільшуватися чи зменшуватися. Безпека населення, різних об’єктів, зокрема й об’єктів критичної інфраструктури, і навколишнього середовища в цілому у разі настання можливих техногенних аварій і стихійних лих у НС установлюється шляхом оцінювання 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 наслідками в часі та просторі [18; 20; 231].

Крім того, існує таке визначення терміну «ризик»: це ймовірність заподіяння шкоди життю та здоров'ю людей, майну фізичних чи юридичних осіб, державній чи муніципальній власності, навколишньому середовищу, життю та здоров'ю тварин і рослин з урахуванням тяжкості цієї шкоди. Застосування цього поняття дозволяє перевести небезпеку в категорію вимірюваних категорій. Ризик насправді є мірою небезпечності. При цьому всі практичні заходи з управління ризиками ґрунтуються на концепції прийнятного ризику, головна ідея якої – прагнення звести його до безпечного рівня. Рівень прийнятного ризику задається пороговими значеннями розміру збитку і ймовірності його виникнення [36; 231].

Кількість різновидів ризику є досить великою, але стосовно НС розглядаються лише так звані «чисті ризики», які передбачають тільки небажаний (негативний) ефект. До них належать такі ризики можливих втрат:

– популяційний;

– диференційований;

– індивідуальний;

– інтегральний (сумарний, сукупний);

– природний;

– фізичний;

– екологічний;

– економічний;

– соціальний (колективний, груповий) тощо.

Для умов надзвичайних ситуацій слід оцінювати індивідуальний і соціальний ризики. У деяких окремих випадках, наприклад для небезпечних технологічних процесів, оцінюють і регламентовані параметри небезпек. Зокрема, індивідуальний ризик (розподіл ризику) – це ймовірність (частота) виникнення небезпечних чинників під час НС у певному місці простору [13; 19; 26].

Соціальний ризик (характерний для масштабу небезпеки) визначається ймовірністю ураження певної кількості людей, що порівнюється із загальною кількістю людей, що зазнали впливу небезпечних чинників під час НС. Наявні методи проведення аналізу й оцінювання ризику, викладені в методичних вказівках щодо проведення оцінювання 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 і НС.

Аналіз економічної безпеки для страхових компаній здійснюється на підставі ступеня оцінювання ризику НС 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 трапляється зацікавленість певних осіб виключити або суттєво знизити у ланцюжку «вартість – безпека – вигода» фінансування заходів безпеки на потенційно небезпечних об’єктах і створити ланцюг «ціна – вигода».

Результати аналізу ризику виникнення різних НС використовуються для:

– декларування промислової безпеки небезпечних виробничих об’єктів;

– експертизи промислової безпеки та погодження паспортів безпеки;

– обґрунтування технічних рішень із забезпечення безпеки найважливіших об’єктів;

– страхування;

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

– оцінювання інтегрального впливу на навколишнє природне середовище;

– в інших процедурах, пов’язаних з аналізом безпеки [148; 248].

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

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 під час вантажно-розвантажувальних робіт унаслідок помилки людини або відмови механізмів із 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, у результаті чого стаються 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 такі:

– 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 та/або виникнення пожежі ємності (боєприпасів);

– падіння метеорита в зону зберігання об’єкта;

– терористичний акт, серед іншого 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].

Прогнозування наслідків НС, як уже вказувалося, здійснюється в кілька етапів.

На І етапі встановлюють параметри впливів − значущих уражальних чинників, що спричинюють основні руйнування й ураження, з характеристиками, що зазвичай обираються з використанням існуючих методик.

На ІІ етапі встановлюють закони ураження − опору елементів ризику впливів, під якими розуміють залежності ймовірності ураження від

інтенсивності прояву уражальних чинників, застосовуючи для їх формалізації ті чи інші функції, що відповідні цій надзвичайній ситуації.

На ІІІ етапі прогнозування дається оцінювання наслідків сполучення моделей впливу і законів ураження (руйнування / пошкодження). З використанням цього методологічного підходу оцінюються наслідки майже всіх стихійних лих і техногенних аварій, що необхідно для обґрунтованого ухвалення рішень про організацію екстреної евакуації населення з районів НС і забезпечення його життєдіяльності у безпечних районах, а також залучення для ліквідації НС сил і засобів ДСНС України різного рівня [34; 94; 182].

Вплив уражальних 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 уражальних чинників в межах поля і частоту події. Поля потенційної небезпеки, зокрема, можна описати у вигляді аналітичних, табличних або графічних залежностей.

2.3. Аналіз вітчизняного нормативно-організаційних механізмів державного управління забезпеченням безпеки критичної інфраструктури

Перш ніж оцінювати вітчизняне нормативного та адміністративне забезпечення держуправління критичною інфраструктурою, зауважимо, що, обрана в країнах Європи концепція критичної інфраструктури була запроваджена 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 та її економічний потенціал, була

Британія. Після того як у вересні 2001 року в США відбувся масштабний теракт, ця держава почала активно вживати заходів із захисту економічної безпеки, серед іншого там до переліку основних об'єктів її критичної інфраструктури було включено:

– 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.

Відповідно до цих світових тенденцій Україна теж почала приділяти більшу увагу створенню власної системи захисту об'єктів критичної інфраструктури. Так була створена Зелена книга – збірка матеріалів, зокрема робіт міжнародних експертів, присвячених питанням захисту цієї інфраструктури [22; 95].

Практична імплементація нових підходів до цієї сфери розпочалася з ухваленням Закону України «Про національну безпеку України» від 21.06.2018 № 2469-VIII. Також було розроблено проєкт Закону України «Про критичну інфраструктуру та її захист», покликаний забезпечити формування потрібної для цього нормативно-правової бази [88; 189; 208].

Необхідно відмітити, що, розробляючи вітчизняну стратегію захисту критичної інфраструктури, є сенс звернутися до досвіду США, в якому провідними є такі напрями:

– запобігання терактів і їх нейтралізація, а також стримування появи чи мінімізація наслідків, спричинених діями терористів, спрямованими на повне знищення, часткове виведення з ладу або використання зі злочинними цілями об'єктів критичної інфраструктури;

– посилення готовності до терористичних актів на національному рівні;

– своєчасне реагування та якнайшвидше відновлення та відбудова об’єктів критичної інфраструктури у разі стихійних лих, терористичних атак чи інших НС.

Крім того, у межах державної системи захисту критичної інфраструктури необхідно об’єднувати зусилля різних інституцій щодо захисту об’єктів цієї інфраструктури і своєчасного реагування на негативні прояви. Зокрема, до таких інституцій слід віднести:

– підсистему цивільного захисту;

– підсистему фізичного захисту;

-підсистему кібернетичного захисту;

– підсистему 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, яка зможе відповідати на нові типи викликів на рівні держави [22; 70]. Тому Уряд доручив Міністерству розвитку економіки, торгівлі та сільського господарства України завдання розробити проєкт закону «Про критичну інфраструктуру України та її захист» [189], і для його виконання було зібрано робочу групу з представників міністерств та інших центральних органів виконавчої влади. У цьому законопроєкті забезпечення захисту критичної інфраструктури офіційно визнається складовою забезпечення нацбезпеки України, і встановлюється, що державна політика у цій сфері має ґрунтуватися на таких принципах:

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

– законодавче встановлення вимог до забезпечення захисту об’єктів критичний інфраструктурі;

– визначення повноважень і відповідальності суб'єктів державної системи захисту цієї інфраструктури;

– забезпечення умов, сприятливих для мінімізації поширення можливих загроз, а також усунення або максимально можливого зменшення наслідків у разі перетворення загрози на НС;

– можливості швидкого й ефективного відновлення нормальної роботи критичної інфраструктури у разі перетворення загроз на НС;

– створення системи оперативного виявлення загроз зазначеній інфраструктурі;

– сприяння взаємодії між державою, господарюючими суб'єктами, експертним середовищем і населенням стосовно забезпечення безпеки цієї інфраструктури та її стабільної роботи;

– налагодження співпраці із захисту цієї інфраструктури на міжнародному рівні [22; 145].

В Україні планується створення комплексної державної системи захисту критичної інфраструктури протягом періоду з 2017 по 2027 роки, покликаної допомогти держуправлінню у цій галузі вийти на якісно новий рівень, що передбачає:

– пошук інноваційних підходів до управління ризиками безпеки критичної інфраструктури;

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

Але слід усвідомлювати, що для цього треба, по-перше, законодавчо закріпити модель розбудови державної системи захисту критичної інфраструктури, а по-друге, створити ефективний механізм реагування на загрози цій інфраструктурі, для чого потрібна консолідація зусиль усього державного сектору безпеки й оборони.

Служба безпеки України забезпечує серед іншого захист економічної безпеки держави, оскільки економічні злочини в сучасних умовах вважаються однією з головних загроз об'єктам критичної інфраструктури. Не випадково Закон України «Про Службу безпеки України» від 25.03.1992 № 2229-XII із останніми змінами і доповненнями надав їй повноваження щодо захисту об'єктів цієї інфраструктури. Загалом СБУ займається зазначеним питанням уже понад п'ять років. Це, перш за все, визначається тим, що складна безпекова ситуація в державі вимагає для забезпечення стабільності функціонування об'єктів життєзабезпечення застосування відповідних заходів як превентивного, так і реагувального характеру [92; 208].

Деякі цільові повноваження СБУ необхідно деталізувати з урахуванням поточних тенденцій в новому проєкті закону «Про критичну інфраструктуру України», де вони:

– більш конкретні;

– зрозумілі для широких верств населення;

– надають інструменти та вказують вектори діяльності, за яким СБУ рухатиметься в бік ефективного захисту критичної інфраструктури, щоб підвищити стійкість держави до викликів і загроз різного характеру [189].

У плані забезпечення захисту критичної інфраструктури досить корисним для України може виявитись досвід Польщі. Це було підтверджено серед іншого на Міжнародному науково-практичному семінарі «Становлення та перспективи розвитку державної системи захисту критичної інфраструктури в Україні» (2019 р.), проведеного в межах проєкту Організації з безпеки і співпраці в Європі (ОБСЄ) «Технічна підтримка реформування спеціальних служб і органів кримінальної юстиції України з метою забезпечення дотримання зобов'язань у сфері захисту прав людини», розробленого на запит СБУ 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 подальший розвиток національної системи захисту в Україні критичної інфраструктури. Практичні й теоретичні рекомендації, отримані від країн, які вже мають масштабний досвід у розглядуваній сфері, дозволять зміцнити засади функціонування державної системи захисту критичної інфраструктури [21; 92; 208].

Найголовнішим державним органом в Україні, що відповідає за управління критичною інфраструктурою, як уже згадувалося, є Державна служба України з надзвичайних ситуацій. Головними її завданнями є такі:

– реалізація державної політики у сфері запобігання та ліквідації НС різного характеру (техногенні катастрофи, аварії, стихійні лиха та інші катастрофи), забезпечення пожежної, виробничої й радіаційної безпеки та цивільної оборони;

– державний нагляд, виконання контрольних, дозвільних та інших спеціальних функцій у галузі захисту населення та територій від НС природного та техногенного характеру, забезпечення пожежної, промислової й радіаційної безпеки та цивільної оборони;

– організація та здійснення заходів реагування на НС;

– координація діяльності інших органів держуправління, місцевих органів виконавчої та адміністративної влади у зазначеній сфері;

– забезпечення функціонування державної системи запобігання та ліквідації НС та державної системи пожежної безпеки;

– керівництво органами і підрозділами з надзвичайних ситуацій;

– забезпечення мобілізаційної готовності органів та підрозділів до НС, виконання завдань у системі територіальної оборони України;

– розвиток матеріально-технічної бази та підтримання високого ступеня бойової готовності органів та підрозділів з надзвичайних ситуацій;

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

До функцій ДСНС України належать, зокрема, такі:

– здійснює організаційне та науково-технічне забезпечення функціонування державної системи запобігання та ліквідації НС і 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 НС природного й техногенного характеру, забезпечення пожежної, промислової та радіаційної безпеки та цивільної оборони, включно із взаємним попередженням про виникнення НС та наданням допомоги; бере участь у розробці проєктів міжнародних договорів з питань, що належать до компетенції ДСНС України;

– фінансує заходи з попередження і ліквідації НС у межах виділених бюджетних асигнувань, вносить пропозиції Уряду України про використання наявних у складі державних і мобілізаційних резервів запасів матеріально-технічних, продовольчих, медичних та інших ресурсів і коштів загальнодержавного фонду фінансування витрат, пов’язаних зі стихійними лихами, аваріями та катастрофами, на ліквідацію НС 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];

– ліцензує в установленому порядку відповідні види діяльності;

– реалізує державний нагляд за дотриманням вимог пожежної безпеки міністерствами, іншими органами держуправління, іншими організаціями, посадовими особами та громадянами;

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

–повністю або частково призупиняє роботу організацій, будівництво, реконструкцію, технічне переозброєння, ремонт об’єктів і проведення інших робіт у разі порушення протипожежних вимог або невиконання 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, яка не відповідає протипожежним вимогам;

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

– узгоджує в установленому порядку проєкти на будівництво об’єктів, щодо яких відсутні протипожежні вимоги;

– організовує ліквідацію аварій, катастроф, стихійних та інших лих, авіаційне виявлення пожеж у лісах і на торфовищах, гасіння пожеж та рятування людей, координує роботу органів держуправління, місцевих виконавчих і розпорядчих органів та інших організацій із запобігання та ліквідації НС;

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

– розробляє, затверджує та/або погоджує в установленому законодавством України порядку нормативно-правові акти, стандарти, норми і правила у сфері захисту населення і територій від НС, забезпечення пожежної, промислової та радіаційної безпеки та цивільної оборони;

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

– інформує органи державного управління, місцеві органи влади, інші організації та населення з питань запобігання та ліквідації НС, забезпечення пожежної, виробничої і радіаційної безпеки та цивільної оборони;

– взаємодіє із ЗМІ;

– бере участь у розробленні та реалізації єдиної державної науково-технічної політики у сфері запобігання та ліквідації НС і пожеж;

– координує проведення наукових досліджень і державних випробувань у сфері запобігання та ліквідації НС, забезпечення пожежної, промислової і радіаційної безпеки та цивільної оборони, бере участь у проведенні таких досліджень та випробувань;

– здійснює відповідно до своєї компетенції сертифікацію у сфері запобігання та ліквідації НС, пожежної, промислової і радіаційної безпеки та цивільної оборони [177; 180; 184];

– узагальнює і практично використовує передовий досвід зарубіжних пожежних та аварійно-рятувальних служб;

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

– організовує 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 під час проведення загальнодержавних та міжрегіональних заходів щодо запобігання та ліквідації НС і 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 і підрозділів;

– забезпечує правовий та соціальний захист працівників і пенсіонерів органів та підрозділів з надзвичайних ситуацій і 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 зазначених органів та підрозділів;

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

– надає платні послуги юридичним та фізичним особам у встановленому законом порядку;

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

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

Так, стосовно ДСНС України Міністр внутрішніх справ у межах своєї компетенції:

– затверджує структуру та штатний розпис органів і 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;

– залучає згідно із законодавством для ліквідації НС та пожеж людські та матеріально-технічні ресурси організацій;

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

– інформує Президента України та Уряд України про діяльність у сфері запобігання та ліквідації НС, забезпечення пожежної, промислової і радіаційної безпеки та цивільної оборони й надає інформацію з цих питань засобам масової інформації;

– вносить у встановленому порядку до Кабінету Міністрів України проєкти нормативно-правових актів і пропозиції про скасування нормативно-правових актів інших органів держуправління, що суперечать законодавчим актам України і рішенням Уряду України;

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

– установлює 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;

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

– установлює відповідно до законодавства України розміри та порядок надання матеріальної допомоги працівникам та пенсіонерам органів і підрозділів з надзвичайних ситуацій;

– розподіляє обов'язки між своїми заступниками щодо керівництва напрямками діяльності ДСНС України;

– 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 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 й подяками ДСНС України, вносить 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 і 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 перебуває 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, потрібних для роботи 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 виконують завдання і функції у сферах:

– цивільного захисту;

– захисту населення та територій від НС різного характеру;

– забезпечення пожежної безпеки;

– забезпечення безпеки людей на водних об'єктах на територіях усіх регіонів України [94; 141; 248].

Головними завданнями територіальних органів і підпорядкованих підрозділів ДСНС України в межах їхньої компетенції є такі:

– реалізація державної політики у сфері цивільного захисту, захисту населення та територій від НС, забезпечення пожежної безпеки та безпеки людей на водних об’єктах;

– виконання контрольних функцій у зазначеній сфері;

– діяльність з організації та здійснення цивільного захисту, захисту населення та територій від НС і пожеж, забезпечення безпеки людей на водних об’єктах та екстреного реагування під час НС загальнодержавного рівня [166; 213].

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

– організовують прогнозування НС у системі моніторингу та прогнозування надзвичайних ситуацій, роботу із запобігання та ліквідації НС загальнодержавного рівня, рятування та життєзабезпечення людей під час НС, забезпечують підтримку ліквідації НС регіонального та міжмуніципального характеру, а також своєчасне ухвалення управлінських рішень у разі переходу цих НС на національний рівень;

– організовують в установленому порядку роботу із запобігання пожежам і контроль за організацією їх гасіння на об’єктах критичної інфраструктури, важливих для нацбезпеки держави, інших особливо важливих пожежонебезпечних об’єктах та особливо цінних об’єктах культурної спадщини України, а також під час проведення заходів загальнодержавного рівня з масовим скупченням людей, перелік яких затверджується Урядом України;

– організовують в установленому порядку пошук і рятування людей на водних об’єктах;

– організовують в установленому порядку разом із зацікавленими органами виконавчої влади України формування та доставку вантажів

гуманітарної допомоги населенню, що постраждало внаслідок НС, включно з населенням інших країн;

– організовують облік атестованих аварійно-рятувальних служб, пожежників, пожежно-рятувальних, пошуково-рятувальних та аварійно-рятувальних формувань і громадських об’єднань із статутними завданнями щодо проведення аварійно-рятувальних робіт і гасіння пожеж;

– організовують 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;

– організовують взаємодію сил і засобів, що беруть участь в аварійно-рятувальних операціях під час НС та гасіння пожеж;

– організовують атестацію 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];

– здійснюють контроль за створенням та забезпеченням готовності сил і засобів цивільного захисту в регіонах України, муніципальних утвореннях та організаціях;

– здійснюють поточне та перспективне планування мобілізаційного розгортання з’єднань і військових частин військ цивільної оборони та військових частин протипожежної служби у воєнний час;

– здійснюють контроль за створенням, збереженням та використанням страхового фонду документації для об’єктів високого ризику та об’єктів систем життєзабезпечення населення;

– здійснюють у межах своєї компетенції в установленому порядку заходи щодо запобігання, виявлення та припинення терористичної діяльності на об’єктах ДСНС України, а також ліквідації наслідків терактів;

– беруть участь у межах своєї компетенції в інформуванні населення за допомогою ЗМІ та інших каналів про очікувані й ті, що виникають, надзвичайні ситуації та пожежі, заходи із забезпечення безпеки населення і територій, прийоми та методи захисту, а також здійснюють пропаганду у сфері цивільного захисту, захисту населення та територій від НС, забезпечення пожежної безпеки та безпеки людей на водних об’єктах;

– беруть участь в управлінні єдиною державною системою запобігання та ліквідації НС;

– беруть участь у підготовці пропозицій з питань надання державної допомоги населенню та територіям, які постраждали від НС регіонального, національного чи транскордонного характеру;

– беруть участь у координації діяльності всіх видів пожежної охорони [150; 216].

Територіальним органам та підпорядкованим підрозділам ДСНС України для реалізації покладених на них завдань надаються такі основні повноваження:

– готують проєкти нормативно-правових актів та інших документів з питань цивільного захисту, захисту населення і територій від НС, забезпечення пожежної безпеки й безпеки людей на водних об’єктах;

– здійснюють 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 НС, забезпечення пожежної безпеки та безпеки людей на водних об’єктах місцевими органами влади, організаціями, їх посадовими особами, громадянами України, іноземними громадянами та особами без громадянства;

– керують підлеглими підрозділами та регіональними головними управліннями ДСНС України з питань бойової та мобілізаційної готовності, проходження військової служби, матеріально-технічного та фінансового забезпечення;

– виконують функції з управління закріпленим державним майном (у межах їхніх повноважень);

– здійснюють повноваження розподільника коштів державного бюджету стосовно регіональних головних управлінь ДСНС України та підпорядкованих підрозділів відповідно до законодавчих та інших нормативно-правових актів України;

– створюють координаційно-дорадчі органи (комісії, групи) на представницькій основі, а також інші колегіальні органи для обговорення актуальних питань діяльності регіонального центру ДСНС України тощо.

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.

Водночас активізується процес деконцентрації повноважень державної виконавчої влади шляхом перебудови й оптимізації системи територіальних структур державних органів виконавчої влади і створення їх регіональних структур.

На регіональному рівні також можна підвищити ефективність державної політики у сфері громадської безпеки та захисту критичних об’єктів під час НС

і терористичних актів. Оптимізація територіального управління не може здійснюватися одночасно. Це розгорнутий у часі процес послідовного реформування державної системи. Існує чимало доказів того, що у міру формування системи територіальних органів і 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; 212].

У цьому контексті принципово важливо підкреслити ще одну обставину: до найважливіших завдань повноважних представників належить формування ефективних механізмів взаємодії держави і суспільства та «зворотного зв'язку» між Президентом України й мешканцями міст та інших населених пунктів.

Окрему увагу варто приділити кібербезпеці критичної інфраструктурі, оскільки сучасні інформаційно-комунікаційні технології почали використовувати для вчинення терактів, у яких найпривабливішими мішенями виступають саме об'єкти критичної інфраструктури [28; 203].

Противник завжди розглядає об'єкти національної інфраструктури як потенційні мішені. Серед них особливо виділяються об'єкти, часткова деградація або повна втрата функціональності яких здатна впливати на стан нацбезпеки і приводити до НС певного рівня і масштабу, – об'єкти критичної інфраструктури.

Нині головним викликом для операторів найважливіших об'єктів інфраструктури стають кібератаки, 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 й активи – фізичні і віртуальні, значення яких є настільки великим, що обмеження їх дієздатності або їх руйнування може призвести до послаблення безпеки, економіки, соціального благополуччя або соціальної безпеки, заподіяння 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 до управління ризиками, а також на підставі даних про інциденти на об'єктах критичної інфраструктури, виокремлює такі сектори останньої:

– енергетика: електрика, природний газ і нафта;

– кредитно-фінансові заклади і біржі;

–повітряний, морський і залізничний транспорт;

– охорона здоров'я;

– інформаційні і комунікаційні технології (ІКТ);

– органи держуправління.

Для підтримки роботи найважливіших об'єктів такої інфраструктури вкрай 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 за лічені секунди) [15; 22; 129].

Розлади в системі електропостачання часто викликають серйозні наслідки каскадного ефекту, неминуче зачіпаючи інші сектори та їх інфраструктуру. У цьому розумінні трансформаторним підстанціям і високовольтним лініям електропередачі часто надається більше значення, ніж електростанціям, оскільки розлади в роботі електростанції зазвичай можна компенсувати, тоді як аварію мережі або аварію на критичних ділянках мережі компенсувати неможливо. Водночас мережі передання енергії розподіляються по великій території і є об'єктами енергетичної мережі, які важко захистити.

Енергія потрібна для роботи всіх секторів, тому аварії в системі електропостачання майже неминуче позначаються на функціонуванні різних об'єктів. Як приклад 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, впливаючи таким чином 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 держуправління 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 уразливу 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 найбільш важливих об’єктів енергетичної критичної інфраструктури, слід узгоджувати на міжнародному рівні. У деяких країнах уряди розробляють спеціальні галузеві плани. У Сполучених Штатах спеціальні галузеві плани розроблені для кожного сектору, включно з енергетичний і сектор комунікацій.

Затверджена 26.05.2015 «Стратегія Національної безпеки України», що розглядає енергетичний сектор на макроекономічному рівні, була ухвалена ще до кібератак на Прикарпаття обленерго й Київобленерго і Чернівціобленерго й тому визначає лише такі загрози енергетичній безпеці:

– 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 14.03.2016, об’єкти енергетики вже розглядаються саме як можлива мета атак. Серед іншого там йдеться про кіберзагрози «автоматизованим системам державного та військового управління, об’єктам критичної інформаційної інфраструктури».

Висновки до другого розділу

1. Проаналізовано організаційно-правові засади держуправління захистом критичної інфраструктури у кризових ситуаціях у різних державах, зокрема у США та західноєвропейських країнах. Виділено такі головні риси цієї

діяльності: системи управління діями у кризових ситуаціях мають державний статус; діяльність із запобігання та ліквідації кризових ситуацій є важливою соціальною функцією будь-якої держави і реалізується більшістю державних установ; право запроваджувати особливий режим діяльності органів управління та населення в зоні стихійного лиха надається не лише главі держави, але й главам суб'єктів держави (наприклад, губернаторам штатів у США); діяльність із захисту критичної інфраструктури в кризових ситуаціях фінансується переважно в межах державних програм; акценти в правовому регулюванні ризику дедалі сильніше зсуваються у бік превентивних заходів.

2. Зазначено, що у деяких державах спеціального регулятора у сфері кібербезпеки критичної інфраструктури не існує, натомість у них офіційні представництва наділяються широкими повноваженнями з підтримки безпеки в національному кіберпросторі.

Підкреслено, що стратегія управління кібербезпекою цієї інфраструктури може вибиратися завдяки такій інформованості лише тими державами, які перебувають на самісінькому початку цього шляху. За даними Міжнародного союзу електрозв'язку, офіційні інституції, що опікуються захистом критичної інфраструктури, діють у тому чи іншому вигляді в більшості країн світу. Такий орган у разі відсутності державного регулятора може також офіційно чи неофіційно діяти як відомство, відповідальне за всі аспекти національної кібербезпеки.

3. Зазначається, що наразі перед держуправлінням, зокрема у сфері забезпечення безпеки критичної інфраструктури, стоять такі цілі: 1) адміністративна реформа – формування нових та вдосконалення вже наявних інститутів державної влади (зокрема, системи виконавчої влади); 2) розгортання та зміцнення громадських інститутів, завдяки яким у державі досягається стійка демократія; 3) створення та втілення в життя соціальних та адміністративно-правових регуляторів, які гарантують задекларований у Конституції комплекс

прав, свобод та обов'язків громадян України; 4) розроблення та практична реалізація державної політики щодо забезпечення безпеки населення та захисту об'єктів критичної інфраструктури; 5) захист внутрішньої і зовнішньої безпеки та забезпечення сприятливих мирних умов для життєдіяльності регіонів України; 6) досягнення збалансованого і взаємопов'язаного розвитку регіонів у взаємодії з центром на основі поглиблення процесів формування і функціонування загальноукраїнського ринку.

4. Показано, що аварії в системах забезпечення останніми роками традиційно становили у найбільший відсоток від загальної кількості НС на різнохарактерних об'єктах вітчизняної критичної інфраструктури – 83,3 %. Аварії в електро-енергосистемах становили 57,1 %. Відповідно, вони посідають перше місце серед НС на різних об'єктах критичної інфраструктури.

5. Підкреслено, що в Україні створюється комплексна державна система захисту критичної інфраструктури на 2017–2027 роки, покликана допомогти держуправлінню у цій галузі вийти на якісно новий рівень, що передбачає:

– вироблення інноваційних підходів до управління ризиками безпеки критичної інфраструктури;

– оптимізацію використання наявних ресурсів, гнучке і швидке реагування на інциденти і кризи.

РОЗДІЛ 3
НАПРЯМИ РОЗВИТКУ ДЕРЖАВНОГО УПРАВЛІННЯ ЗАБЕЗПЕЧЕННЯМ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

3.1. Трансформація державних механізмів забезпечення безпеки та підвищення ефективності захисту критичної інфраструктури

Поняття «захист» може мати різні значення. Найпопулярніше тлумачення цього терміну означає турботу про запобігання небезпекам, різному шкідливому впливу середовища на соціальний суб'єкт чи матеріальний об'єкт, здатним поставити під загрозу його безпеку. Захист може розглядатися в двох його основних значеннях:

– захист як діяльність, покликана забезпечити безпеку об'єктів захисту;

– захист як засіб або ж системне впорядкування засобів для забезпечення безпеки об'єктів захисту.

Пропонуємо далі розуміти під поняттям «захист критичної інфраструктури» сукупність заходів, що плануються та здійснюються з такими цілями:

– досліджувати критичні сектори інфраструктури держави у контексті забезпечення їх безпеки, збереження функціональності й економічної та суспільної стабільності та захищати їх; державна і приватна сфери при цьому мають розцінюватись як рівнозначні;

– забезпечити функціонування системи раннього попередження виявів кризових ситуацій та захист інфраструктури, важливої для вирішення таких ситуацій [22; 66].

Через це ми говоримо насамперед про сектори критичної інфраструктури, важливі для:

– забезпечення належного функціонування уряду, органів держуправління та місцевого самоврядування, перш за все у безпековій сфері, й забезпечення та функціонування основних (життєво важливих) товарів і послуг;

– забезпечення функціональності державної та приватної сфер шляхом налагодження належного руху економіки та функціонування громадських служб;

– підтримання внутрішнього порядку, громадської стабільності та безпеки громадян.

Захист критичної інфраструктури стає результатом аналітичного процесу, який охоплює:

– ідентифікацію галузей і секторів критичної інфраструктури на національному, регіональному та місцевому рівнях;

– ідентифікацію релевантних ризиків для згаданих вище секторів;

– аналіз уразливості певних секторів розглядуваної інфраструктури;

– оцінювання ризиків пошкодження або знищення цих секторів;

– ужиття відповідних запобіжних заходів, зокрема щодо розбудови системи захисту такої інфраструктури.

Захист критичної інфраструктури – комплекс організаційно-технічних заходів, покликаних забезпечити захист критично важливих секторів інфраструктури від різних загроз (терористи, диверсанти, екстремісти), зокрема під час НС чи кризових ситуацій [15; 63; 220].

Сучасні системи захисту такої інфраструктури створюються на основі використання різноманітних засобів і зазвичай містять у собі такі складові (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, логічно та функціонально упорядкованих у такий спосіб, що вона стає знаряддям для забезпечення безпеки об’єктів такої інфраструктури в певний час і в заданому просторі. Відповідно до системного підходу цю систему можна вважати синергетичною з цільовою поведінкою [22; 220].

При цьому бажаними функціями системи фізичного захисту є такі:

– відлякувати потенційних нападників від нападів на об’єкт, що охороняється;

– детектувати порушення об’єктів, приміщень або зон, що охороняються, або детектувати виникнення небезпечної обстановки на об’єкті, або його близькій околиці;

– затримувати рух атакуючих;

– реагувати на порушення функціонування або структури об’єктів, просторів або зон, що охороняються, покликані допустити підхід атакуючих до цих об’єктів, просторів чи зон або поставити під загрозу об’єкт, його функцій чи людей.

Зауважимо, що зростаюче значення місцевого та територіального самоврядування України є підставою створення законодавчих і нормативно-правових документів. Завдяки цьому деталізуються процедури участі громадськості в ухваленні рішень про розміщення і оснащення критично важливих об’єктів.

Отже, громадянське суспільство стає третім, альтернативним бізнесу і державі, сектором, що забезпечує як виробництво економічних благ, так і якість

життя населення, включно з безпекою. Але традиції і правова культура щодо участі українського суспільства в ухваленні рішень про розміщення і спорудження критично важливих небезпечних об'єктів ще не розвинулися.

Норми участі громадськості, задані в загальному вигляді, реалізуються найчастіше формально. Що стосується результатів обговорення, то їх визначає сформований рівень соціального партнерства та суспільної злагоди, іноді − випадкові чинники.

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 проєктом.

Крім того, не ведеться реєстрація й облік висловлених думок.

Цю діяльність пропонується розвивати шляхом використання системного підходу, що містить такі складові:

– економічну;

– адміністративно-кримінальну (штрафи, судові розгляди);

– соціально-психологічну.

Для успішного вирішення проблеми доцільно:

– сприяти використанню показників стану навколишнього середовища в системі оцінювання ефективності діяльності регіональних органів виконавчої влади;

– поступово впроваджувати систему технічних регламентів та привести її у відповідність до міжнародних стандартів;

– заявляти з найвищих трибун, що НС не знають політичних кордонів, вимагають довгострокової перспективної роботи й участі громадянського суспільства, активної позиції людей.

Наразі функції із забезпечення безпеки та контролю (зокрема, щодо критично важливих об'єктів) розосередилися серед міністерств та відомств. Доречно зробити єдиним органом із їх забезпечення Державну службу України з надзвичайних ситуацій. Наразі ДСНС відповідає за ведення реєстру зазначених об'єктів. Головними складовими системи моніторингу, від яких залежатиме вирішення покладеного на ДСНС завдання, мають бути центри моніторингу державних органів виконавчої влади та місцевого самоврядування [138; 172].

Організації, що експлуатують потенційно небезпечні об'єкти, необхідно обов'язково оцінювати на предмет готовності до запобігання та ліквідації НС [41; 169; 172].

Оцінювання готовності об'єктів мають здійснювати комісії ДСНС, Головне управління ДСНС України в областях та місті Києві, управління ДСНС України в областях, центри забезпечення діяльності, а також оперативно-координаційні центри.

Оцінювання готовності об'єкта передбачається проводити 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. До його проведення планується залучати спеціалізовані науково-дослідні, проєктні та інші організації з відповідними ліцензіями.

У нашій країні здійснюється паспортизація територій та небезпечних об'єктів. Вона, звісно, стала підґрунтям для обліку та контролю над територією та особливо небезпечними об'єктами для запобігання НС та їх ліквідації. При

цьому типовий паспорт безпеки небезпечного об'єкта і території має враховувати таку категорію, як критично важливі об'єкти.

Підкреслимо, що згадані об'єкти потребують насамперед запобігання НС. Через це першочерговими стають заходи фізичного захисту від зовнішніх і внутрішніх впливів. Крім того в самому забезпеченні безпеки зазначених об'єктів можна виокремити два провідні напрями:

1) захист об'єктів від зовнішніх впливів, щоб відвернути їх знищення та виникнення аварійних ситуацій;

2) захист людей та навколишнього середовища від негативних чинників, які утворюються у випадку, якщо аварія все ж таки настає.

Технічні регламенти висувають низку вимог до об'єктів технічного регулювання (продукція, включно з будівлями та спорудами, виробничі процеси, експлуатація, зберігання, транспортування, продаж та утилізація). Необхідно розробити єдину національну нормативну базу відповідних проблем для оцінювання ризику критично важливих об'єктів, і цьому може допомогти їх категоріювання.

Захищеність об'єктів розглядуваної інфраструктури є ключовою умовою для забезпечення безпеки особи, суспільства та держави, але наразі пов'язані з цим питання регулюються лише на підзаконному рівні. При цьому вкрай необхідно ухвалити базовий закон у цій галузі, який визначатиме основні поняття, види та категорії критично важливих об'єктів, а також встановлюватиме вимоги до забезпечення безпеки окремих категорій таких об'єктів [15; 22; 82].

Загалом, зауважимо, що ДСНС володіє найбільш широкими можливостями комплексного вирішення завдань, пов'язаних з:

– з'ясуванням техногенної обстановки;

– аналізом і оцінюванням ризику;

– підготовкою та ухваленням управлінських рішень, що стосуються організації заходів забезпечення безпеки зазначених об’єктів.

Основним шляхом удосконалення нормативно-правової бази для забезпечення безпеки критично важливих об’єктів є ухвалення базового закону в цій галузі, який визначатиме базові поняття, види та категорії зазначених об’єктів, а також передбачатиме вимоги до забезпечення безпеки окремих категорій таких об’єктів [169; 212].

У процесі держуправління 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 , що ґрунтується на більш ефективному управлінні ресурсами, він збільшує залежності. Їх можна дещо розширено визначити як взаємний зв’язок між продуктами або послугами, за якого один продукт (послуга) потрібен для створення іншого. 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, охорону здоров’я неможливо реалізувати за відсутності електроенергії, води та аварійних служб одночасно. Залежності можуть викликати ефекти різної інтенсивності та складатися з різних типів. Зокрема, під час і 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 її об’єктів;

– кіберзалежності: функціонування одних об’єктів інфраструктури залежить від інформації, переданої через інформаційну інфраструктуру.

Важливо відзначити, що залежності підвищують рівень уразливості. Загроза стає ще гострішою внаслідок широкої залежності урядових установ та приватного сектору від інформаційно-комунікаційних технологій, що збільшують вплив міжгалузевих і транснаціональних залежностей.

Тож, зауважимо, що сценарій, який викликає найбільшу стурбованість в 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, наприклад звичайна бомбова атака на будівлю може супроводжуватись 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 кількість жертв і посилити громадську паніку [39; 203].

Коли уразливості призводять до збоїв внаслідок 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 уразливостями 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 через те, що залежності можуть

змінюватися відповідно від режиму роботи цього об’єкта критичної інфраструктури. Так, 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 мають розглядати залежності не як статичні, а швидше як динамічні й мінливі відносини. При цьому має відбуватися підвищення обізнаності про взаємозалежності через міжсекторальні мережі (засновані, наприклад, на обговоренні сценаріїв ризику), щоб стимулювати подальшу співпрацю між різними учасниками процесів [10; 215].

Необхідно вказати на те, що не існує єдиної, заздалегідь певної інституційної моделі, яка визначає, як країни повинні захищати свої об’єкти критичної інфраструктури. Отже, швидше за все уряди виберуть структуру, яка найкраще відповідатиме їх характеристикам з урахуванням:

– загроз, що виникають;

– розміру і структури економіки;

– культури суспільної політики і ситуації;

– загальної інституційної практики.

Важливо, щоб управління архітектурою захисту об’єктів критичної інфраструктури враховувало основну конституційну структуру країни, тобто унітарні, централізовані та федеративні, а також децентралізовані держави. Це особливо важливо для розподілу ролей та обов’язків між різними урядовими інституціями та їх рівнями.

Архітектура захисту об’єктів критичної інфраструктури варіюється між двома основними моделями. На одному кінці спектру держуправління такими об’єктами ґрунтується 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 слабко і лише як додатковий інструмент, за винятком певних секторів (таких як атомний сектор), де вони можуть відігравати домінуючу роль. На іншому кінці спектру лежить так званий «обов'язковий підхід, що ґрунтується 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 межах установлених термінів. На практиці країни не використовують жоден з підходів у їх базових формах. Швидше вони об'єднують елементи обох. Їх системи можуть бути визначені лише як переважно добровільні або обов'язкові за своєю природою [22; 138].

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 врешті-решт виявляться неадекватними. Через це 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 цей підхід ґрунтується на вищезазначеному принципі, з часом він дедалі частіше стикається з необхідністю зміцнення своєї правової бази щодо захисту

об’єктів такої інфраструктури. Інакше кажучи, країни повинні вчитися на своєму досвіді [54; 239].

Інституційні межі захисту об’єктів критичної інфраструктури повинні, як мінімум, охоплювати такі аспекти:

– визначити урядове агентство, яке відіграє загальну координуючу роль у розробленні та практичному втіленні 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.

Заслуговує на увагу також державно-приватне партнерство у напрямі захисту об’єктів критичної інфраструктури. Майже в усіх державах переважна більшість активів критичної інфраструктури перебуває у приватній власності. Крім того, приватні оператори становлять авангард інвестицій та головних зусиль у розробці нових технологій виробництва і захисту. Ці обставини в поєднанні з тим, що головна відповідальність за захист активів та систем об’єктів зазначеної інфраструктури покладається на їх власників та операторів, доводять важливість створення ефективного державно-приватного партнерства для досягнення адекватного рівня стійкості.

Під час роботи з державно-приватним партнерством розробники стратегій захисту розглядуваних об’єктів повинні прагнути створити умови для досягнення їх ефективності шляхом:

– оцінювання чинників успіху і стримуючих чинників;

– визначення обсягів;

– визначення форм;

– розгляд проблем і викликів [23; 82].

Зокрема, стосовно оцінювання чинників 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 такі чинники, що лежать у підґрунті ефективного згаданого 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, тобто, обидві організації мають бути взаємно поінформовані про діяльність одне одного; хороший спосіб добитися цього − працювати разом тривалий час, найкраще роки;

– реалістичні очікування: всі організації повинні враховувати доступність ресурсів, бюджет розвитку тощо, щоб мати змогу формувати реалістичні очікування такого партнерства.

Щоб визначити сферу державно-приватного партнерства не варто зосереджуватися на одному конкретному етапі циклу захисту об'єктів

критичної інфраструктури, треба охоплювати їх усі: від розробки та реалізації заходів до етапів управління ризиками та кризами [22; 60].

Переваги об’єднання ресурсів, взаємної підтримки та спільного ухвалення рішень між державним сектором та приватними операторами об’єктів розглядуваної інфраструктури поширюються на такі сфери:

– оцінювання безпеки;

– огляд заходів безпеки;

– виділення критично важливих активів і процесів;

– розробка планів дій у разі настання НС;

– 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 цього партнерства зумовлюється безліччю чинників, зокрема таких:

– переслідувані цілі;

– кількість зацікавлених сторін, які будуть залучені, і від того очікується, що партнерство вирішить стратегічні або операційні питання.

форми державно-приватного партнерство можуть мати будь-який характер, від дуже неформальних форм співробітництва до досить формальних і чітко регламентованих. Ступінь формальності зазвичай пов’язується з рівнем контролю, який прагнуть здійснювати державні органи. Водночас державно-приватне партнерство, орієнтоване на проєкт, як правило, є ефективнішим, ніж орієнтоване на процес, оскільки перший підхід зазвичай передбачає більш чітко визначені місії, терміни та бюджети [53; 80]. При цьому не надто добре розроблене таке партнерство ризикує призвести до появи обмеженої або нульової доданої вартості для захисту розглядуваних об’єктів.

Щоб гарантувати, що державно-приватні домовленості про співпрацю виникнуть і продовжать залишатися актуальними і продуктивними, країнам необхідно знати найбільш поширені причини невдач. Їх можуть спричиняти такі чинники:

– розрив очікувань між приватним та державним секторами;

– нестійкі моделі фінансування;

– нечіткий поділ праці тощо.

Фактично саме переваги і сприйняття витрат і вигід сторін зрештою визначають 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 чинників і є динамічним процесом з періодами як слабких, так і сильних показників [10; 46].

Інші проблеми найчастіше стосуються відсутності мотивації бізнесу інвестувати фінансові ресурси для захисту власних об'єктів критичної інфраструктури. Стосовно цього обговорюється необхідність стратегій захисту таких об'єктів для визначення відповідних типів стимулів в цьому відношенні. ОБСЄ розробила базову восьмиступеневу рекомендацію щодо того, як країни повинні максимізувати вигоди, що можуть одержуватись завдяки державно-приватному партнерству з урахуванням спільних інтересів усіх причетних сторін.

Попри те, що керівні принципи були розроблені в межах передової практики для критично важливої енергетичної інфраструктури, вони, як видається, в цілому можуть бути застосовними у всіх секторах. Нижче етапи зазначеної рекомендації розглянуто більш докладно [10; 51].

Крок 1: необхідність аналізу і визначення мотивації кожного партнера, який залучатиметься до партнерства із захисту критичної інфраструктури, щоб уточнити взаємні очікування і внески.

Крок 2: визначення амбіцій та цілей партнерства щодо захисту об'єктів такої інфраструктури на основі загальних національних цілей забезпечення їх безпеки; уточнити цілі партнерства щодо захисту зазначених об'єктів та завдання, які необхідно виконати.

Крок 3: перевірка існуючої нормативної бази, що стосується кожного критично важливого сектору інфраструктури; визначення обов'язкових і самозобов'язуючих норм, правил і принципів; оцінювання адекватності чинної нормативної бази з урахуванням очікуваних ризиків та наявних рівнів готовності; обговорення того, 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, а також забезпечення механізмів для добровільних зусиль, включно з розробкою та обміном 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, що спирається на готовність усіх сторін цього партнерства до співпраці й розгляду рівнів загрози.

Крок 7: визначення критично важливих етапів, щоб розглянути, що було досягнуто, і визначення подальших потенційних кроків.

Крок 8: забезпечення постійного процесу перевірки для перегляду і оновлення партнерських відносин, щоб гарантувати постійний прогрес, зіставний із загальною картиною ризику і заходами безпеки, потрібними для забезпечення оптимального рівня захисту.

Щоб реалізувати заходи держуправління стосовно стратегічних ризиків для критичної інфраструктури на практиці слід застосовувати системно-правовий, політичний, інформаційний, економічний та організаційно-адміністративний механізми.

Зокрема, з арсеналу політичних заходів, перш за все, необхідно офіційно визнати на найвищому рівні концепцію стратегічного управління ризиками для критичної інфраструктури як методологічну основу подальшого забезпечення сталого розвитку [23; 55].

Для системно-правового забезпечення слід розробляти на загальнодержавному та регіональному рівнях нове та розвивати чинне законодавство, яке дозволить охопити найважливіші та пріоритетні для нацбезпеки держави види стратегічних ризиків для критичної інфраструктури й обумовлені ними загрози. Це потребує копіткої і ємної роботи по внесенню коректив та приведення у відповідність:

− кримінального;

− кримінально-процесуального;

− податкового, страхового;

− адміністративного права.

Для вдосконалення організаційно-адміністративних механізмів необхідно створити в межах проведеної в державі адміністративної реформи компетентний державний орган – свого роду «стратегічного ризик-менеджера»

з усім необхідним для його функціонування, зокрема з повноцінною координацією інфраструктури.

Для реформування органів державної влади треба залучати висококваліфікованих ризик-менеджерів на загальнодержавному, регіональному і місцевому рівнях [40; 215].

Важливу роль у справі становлення організаційних важелів стратегічного управління ризиками для критичної інфраструктури відіграватимуть:

– удосконалення державних систем нагляду та контролю;

– оптимальний розподіл виконавчих та контрольних функцій між рівнями державного та муніципального управління;

– оптимізація діяльності всіх органів державної влади, причетних до процесу управління критичною інфраструктурою.

Обмін інформацією має координуватися компетентним органом, починаючи з введення складу та показників стратегічних ризиків для критичної інфраструктури, оцінювання очікуваної шкоди від їх реалізації, до їх подання органам управління, засобам масової інформації та громадськості в зручному та зрозумілому вигляді.

У цілому економічний механізм зниження стратегічних ризиків для критичної інфраструктури має охоплювати як пряме регулювання на основі цільових витрат державних бюджетів, так і непряме економічне регулювання за рахунок удосконалення податкового та кредитного механізмів щодо зниження податкового навантаження [18; 36].

Усі зазначені механізми можна об’єднати у комплексний механізм управління забезпеченням безпеки критичної інфраструктури (рис. 3.1).

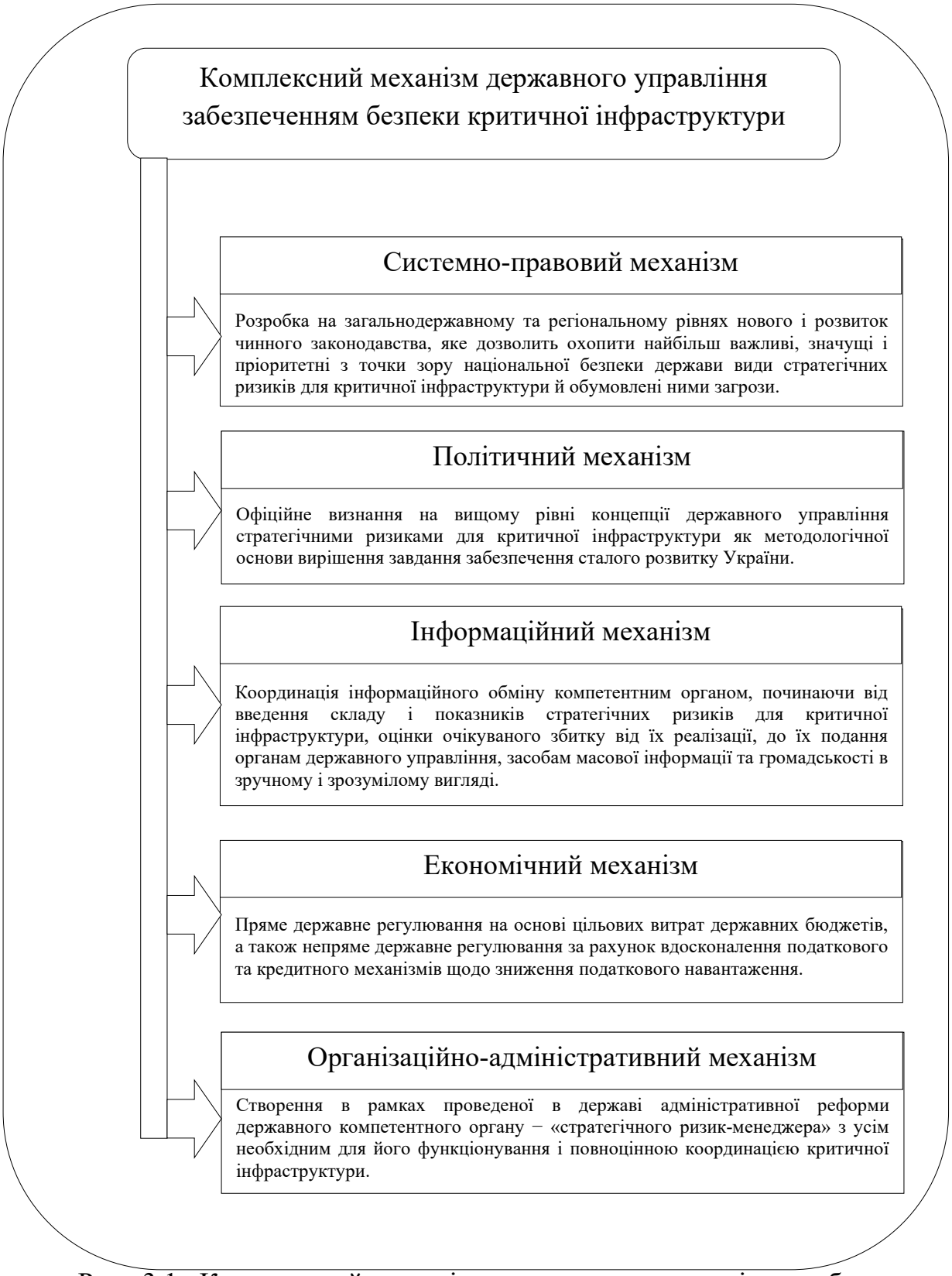

Рис. 3.1. Комплексний механізм державного управління забезпеченням безпеки критичної інфраструктури в Україні

Для практичного здійснення комплексу зазначених заходів щодо необхідно спиратися на всю наявну в державі вертикаль державної влади під координацією незалежного органу держуправління [10; 20; 53].

3.2. Удосконалення системи державного управління захистом критичної інфраструктури

З урахуванням викладеного вище видається, що в найбільш загальній формі система держуправління захистом критичної інфраструктури повинна мати два рівні ухвалення рішень:

1) загальнодержавний;

2) регіональний

Також вона має містити відповідні механізми: політичні, правові, інституційні, адміністративні, економічні, науково-технічні тощо.

Для кожного з рівнів слід визначити відповідні повноваження та визначити ступінь відповідальності за ухвалені рішення: на загальнодержавному − щодо управління зовнішніми та внутрішніми стратегічними ризиками для критичної інфраструктури, регіональними – внутрішніми такими ризиками [22; 55].

Держуправління протидією стратегічним ризикам та загрозам критичній інфраструктурі є пріоритетом у здійсненні системного комплексу організаційно-технічних, фінансових тощо заходів, в першу чергу попереджувального характеру, які застосовуються на підставі експертно-аналітичних методів вирішення низки пов’язаних між собою завдань щодо:

– ідентифікації;

– оцінювання часткових та інтегральних стратегічних загроз критичній інфраструктурі;

– ранжування та вибору пріоритетних стратегічних ризиків для такої інфраструктури;

– визначення методів по зменшенню впливу на стратегічні ризики для цієї інфраструктури до прийнятного та подання пропозицій для ухвалення рішень на відповідному рівні.

Підкреслимо, що ефективно управляти стратегічними ризиками для критичної інфраструктури без формування загальної культури безпеки на всіх рівнях соціальної структури суспільства неможливо, і, перш за все, це стосується тих, хто ухвалює стратегічні державні рішення. По суті, 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 підґрунтям 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 НС найвищої категорії.

Усі 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 чинників, 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 для економії резервів у разі їх браку.

При цьому мінімізація можливостей виникнення чинників, що завдають шкоди критичній інфраструктурі, означає, перш за все послідовний та системний пошук ризиків, здатних зумовити виникнення події, яка завдає шкоди життю, здоров’ю та майну людей, навколишньому середовищу тощо.

При цьому підґрунтям аналізу ризиків для об’єктів критичної інфраструктури є пошук та класифікація можливих НС і подальше впровадження таких заходів, які допоможуть їм запобігти або принаймні мінімізують імовірність їх виникнення.

У загальному розумінні під аналізом ризику зазвичай розуміється використання наявної в розпорядженні інформації для оцінювання ризику для осіб, організацій, суспільства, майна або навколишнього середовища, які випливають із цієї загрози [83; 215].

Аналіз ризиків, найчастіше, має такі складові:

– дефініції рамок і можливостей загрози (небезпеки);

– прогнозу ймовірності загрози;

– оцінювання вразливості елементів, що перебувають під загрозою;

– ідентифікації наслідків і прогнозу ризику.

Як і інші аналізи, аналіз ризиків у першу чергу поділяє систему і джерела ризику на його окремі складові, які потім досліджує.

Кваліативний аналіз застосовує словесну оцінювання або відносну цифрову оцінювання для опису розмірів можливої шкоди і ймовірності, з якою вона може настати.

Квантитативний аналіз ризиків ґрунтується 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 межах цього аналізу, найчастіше, ідентифікується місце можливого виникнення і його ймовірність; розмір можливої загрози залежно від часу та інших умов, а також передбачуваних наслідків для працівників або населення, інфраструктури, довкілля тощо.

Якщо надзвичайна подія все ж таки настає, 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 їх можна поділити 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 усвідомлювати, що йдеться про складові, що безпосередньо усуватимуть 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. Вона створюється на рівні громадського управління (державного управління та самоврядування) і містить у собі 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 ґрунтуватися на стандартних засобах зв'язку, таких як телефон, електронні скриньки зв'язку, веб-сайти, ЗМІ або спеціалізовані засоби комунікації з громадськістю, наприклад місцеві радіосистеми або сирени.

Останнім названим елементом активної превенції є система моніторингу актуальної ситуації. У цьому разі йдеться, перш за все, про розбудову та експлуатацію електронних систем, які реєструють дані про виникнення певного чинника та надають інформацію про перевищення попередньо встановленого рівня. До таких систем можна віднести:

– системи моніторингу рівня водних потоків або проточність;

– датчики, що фіксують концентрації деяких хімічних речовин;

– температуру;

– наявність іонізуючого випромінювання.

Сьогодні йдеться 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 спрямовані на суб'єкт, який перебуває під загрозою. Ним 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. У 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 перебувають 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.

Усі 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, призначених для забезпечення обороноздатності держави, усунення наслідків кризових ситуацій та/або захисту найбільш 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 тим самим продовжити термін, на який запаси будуть достатніми.

Конкретні системи регулюючих заходів, а також галузей, в яких уживатимуться регулюючі заходи, залежать від кожної держави. Найчастіше можна зустрітися 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 із подальшим високим ступенем залежності від їх поставки.

Сьогодні весь світ поділяє думку, що розвинені європейські та північноамериканські держави не здатні в довгостроковій перспективі витримати без електричної енергії. Цивілізація настільки просунулася, що люди вже втратили здатність обходитися без електроенергії і не готові 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 браку необхідних ресурсів, насамперед періоду після Другої світової війни, наприклад системи надання продуктів харчування за талонами. На випадок, якщо надзвичайна подія усе ж стається, необхідно мати систему реагування. Її завданням є максимальне скорочення часу дії несприятливих чинників, а значить, − і мінімізація втрат від їх поставки.

Першим кроком у процесах ідентифікації об’єктів критичної інфраструктури зазвичай стає закріплення всебічного визначення того, що розуміється під таким об’єктом. Це корисно для створення основи, на якій згодом розроблятимуться подальші політичні та нормативні межі.

Об’єкти критичної інфраструктури можуть визначатися, зокрема, з урахуванням тієї ролі, яку вони відіграють у 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 урахуванням впливу на права людини, що стаються 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», пошкодження чи знищення яких суттєво впливатиме на все «в результаті недотримання цих функцій». У тому ж дусі закон «Про збройні конфлікти» передбачає особливий захист інфраструктури, необхідної для виживання цивільного населення, або такої, руйнування якої може потягти за собою появу великої кількості жертв або зашкодити здоров’ю та виживанню населення (Перший додатковий протокол до Женевських конвенцій, ст. 54−56, 1949 року).

Другий етап в ідентифікації об’єктів розглядуваної 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. Низка 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.

Водночас 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 сильно залежать в отриманні доходів від індустрії туризму. Для них захист цієї індустрії як критично важливої може відіграти 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 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 охоплюють вибір / комбінацію з такого:

1) географічне охоплення впливу;

2) тривалість впливу;

3) тяжкість потенційних наслідків в плані:

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 держуправління;

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, що ґрунтується 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, що ґрунтується на операторі (наприклад, Франція), де завдання визначення того, які активи або послуги є критично важливими, залишається за окремими операторами критично важливих об'єктів;

– підхід, що ґрунтується на активах або гібридах (наприклад, у Великобританії), в якому використовуються елементи підходів, орієнтовані як на послуги, так і на оператора.

Як рекомендований підхід до ідентифікації рівня критичної важливості об'єкта пропонується такий сценарій.

1. Проаналізувати наявність об'єктів інфраструктури, що перебуває 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 і вимог на рівні законодавчих та інших нормативних актів, що покладає на організацію обов'язки із 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. За позитивної відповіді організація визнається суб'єктом такої інфраструктури [23; 82].

3. За наявності інфраструктури організації, яка використовується для інформаційного обміну сторонніми системами, робиться запит власникам цих систем про їх належність до суб'єктів критичної інфраструктури. У разі позитивної відповіді конкретизується використання наданої інфраструктури для організації взаємодії об'єктів критичної інфраструктури. Якщо висновок буде позитивним, організація визнається суб'єктом такої інфраструктури.

4. Далі організація розглядає свою інфраструктуру (або її частину, безпосередньо залучену до забезпечення взаємодії між аналогічними об'єктами) як об'єкт критичної інфраструктури.

Доцільно при цьому детальніше розглянути чинники 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. До них належать такі явища, як:

– паводки (включно з підвищенням рівня ґрунтових вод);

– повені;

– затоплення;

– штормові припливи;

– сніг;

– крига;

– посухи;

– бурі.

Особлива небезпека в разі паводків виникає в результаті дії вод, що підмивають дороги, мости, дамби тощо. Небезпека забруднення питної води і виникнення через це значного ризику для здоров'я ще більше підвищується внаслідок витоку шкідливих речовин і відходів, які переносяться повеневими водами. Унаслідок 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 подальших сильних поривів бурі й урагани можуть викликати додаткові загрози від уламків і сміття, шо переносяться, у воронці, яка обертається з неймовірною швидкістю. Бурі посідають одну з перших позицій як за частотою виникнення, так і за відсотковим розподілом економічного збитку для критичної інфраструктури [15; 132].

2. Епідемії. Під епідемією розуміється масове в географічному та часовому плані поширення будь-якої інфекційної хвороби у тварин чи людей. Підвищена небезпека виникає, наприклад, у зв'язку з глобальним товарообігом і туризмом, промисловим утриманням тварин, а також повенями і засухами. Пандемія є епідемією, що охоплює населення низки країн або навіть усього світу. Унаслідок 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 виникають унаслідок людських прорахунків і технічних збоїв.

1. Пожежі. Пожежа є вогнем, який безконтрольно розповсюджується, та що виник у результаті:

– людських прорахунків і технічних збоїв, включно з підпалом;

– удару блискавки;

– виділення небезпечних речовин або вибухів.

Залежно 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 шкідливо впливати на довкілля або людину чи призводити до вибухів і пожеж. Небезпечні речовини за своїми властивостями можуть бути дуже різними: від дратівливих чи легкозаймистих і до вибухонебезпечних, що становлять загрозу для навколишнього середовища, та завдають хронічної і токсичної шкоди.

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 у результаті виділення енергії, що призводить до виникнення ударної хвилі, можливо і з виділенням тепла. Вибухи на критично важливих об’єктах можуть ставатись через помилки людини і технічні розлади (включно з навмисними діями), 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 виникають через тероризм або злочинні дії (рис. 3.2).

Більш докладно зазначені на рис. 3.2 форми прояви сучасного внутрішнього тероризму розкрито у табл. 3.1.

У результаті аналізу загальної ситуації щодо наявності загроз критичній інфраструктури, загрози, що виникають внаслідок тероризму чи злочинних діянь, можна віднести до певних видів загроз залежно від ступеня небезпечності.

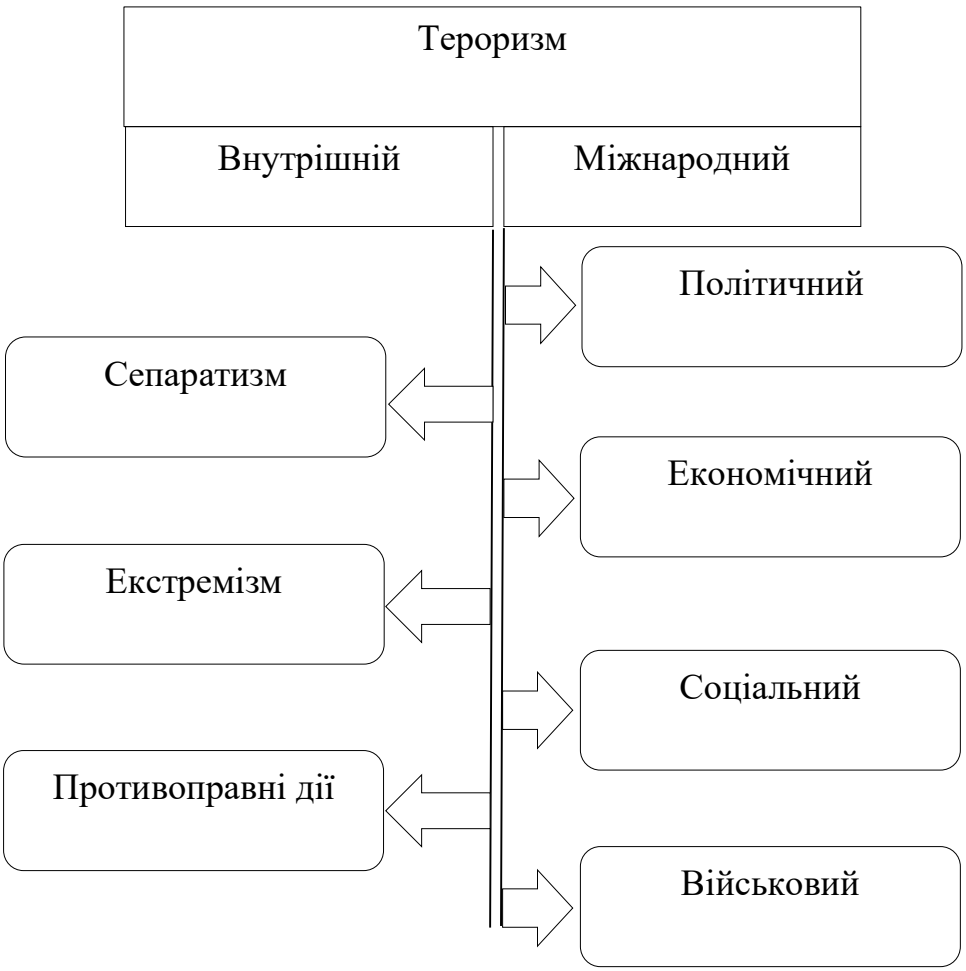

Рис. 3.2. Форми прояву сучасного тероризму

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

При цьому щодо кожного окремого виду таких загроз дається стисла характеристика:

– потенційних злочинців;

– можливих або характерних методів дій потенційних злочинців, їх цілей і мотивів;

– ступеня кримінальної активності потенційних злочинців.

У табл. 3.2 показано характерні особливості різновидів міжнародного тероризму.

Ці види загроз дозволяють наочно показати, які ризики необхідно враховувати. Водночас припущення про те, що такі загрози критичній інфраструктурі належать до відповідного типу загроз, ґрунтується на криміналістичному досвіді, але не обов'язково знаходить повне підтвердження в усіх випадках без винятку.

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

Продовження таблиці 3.2

Соціальний	Створення та підтримка терористичних організацій (осіб, груп), націлених на проведення теракtів з метою порушення громадської безпеки і залякування населення Створення та підтримка громадських організацій і рухів, діяльність яких спрямовано на дискредитацію соціально-економічної політики держави
Військовий	Організація теракtів, що призводять до розв'язування внутрішніх конфліктів, що вимагають залучення збройних сил Організація теракtів, спрямованих на знищення військового майна і загибелі особового складу збройних сил Організація теракtів, спрямованих на дискредитацію військової політики держави Організація теракtів, 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 із забезпечення безпеки підприємств критичної інфраструктури, винних або, відповідно, злочинців, можна поділити на приблизні групи, виходячи з їх конкретних мотивів та можливих методів дії, а також скласти таблицю, що відображає відповідні ступені небезпечності. При цьому не враховуються необережні дії, оскільки вони стосуються загроз, що виникають унаслідок людських прорахунків і технічних збоїв [36; 60; 61].

Питання про те, наскільки потенційні злочинці можуть на практиці завдати серйозної шкоди та в яких місцях це можливо, повинно бути предметом

оцінювання ризиків критичній інфраструктурі з урахуванням виявлених уразливих місць розташування підприємства, що є об'єктом такої інфраструктури.

Такі види загроз критичній інфраструктурі містять низку вихідних положень, з допомогою яких можна визначити їх співвідношення з виявленою обстановкою в плані наявності загроз. Переважно йдеться про такі посилання:

– можливі супутні для дії обставини;

– можливі мотиви і характерні методи дій;

– допоміжні кошти, використання яких є імовірним;

– очікувана кримінальна активність.

Виходячи зі сполучної ланки між злочинцями, включно з їх мотивацією, і варіантів дій, зумовлених властивостями самих об'єктів розглядуваної інфраструктури, доцільно, крім того, скласти таку приблизну класифікацію залежно від можливостей впливу.

Принципово можливі, наприклад, такі варіанти впливу.

1. Навмисна помилка в обслуговуванні обладнання. Під цим розуміються будь-які навмисні дії, здатні привести до збоїв в результаті застосування простих прийомів без використання знарядь учинення злочину. До таких дій можуть, наприклад, належати:

– включення/відключення обладнання;

– відкриття/закриття заглушок трубопроводів (шиберів);

– обертання маховиків та 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 в критичний стан. 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 у межах виробничої зони об’єкта критичної інфраструктури можуть призвести до викиду небезпечних речовин або пошкодження чи 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 унаслідок наїзду вантажних автомобілів.

4. Несанкціоновані дії з використанням елементарних знарядь учинення злочину. У цьому випадку це означає навмисне, часто спонтанне втручання в роботу важливих частин установки з використанням наявних на будь-якому підприємстві, включно, зокрема, з тими, що входять у 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, у першу чергу, працівники самого підприємства.

5. Несанкціоновані дії із застосуванням великовагових знарядь вчинення злочину. У разі такого варіанту впливу передбачається, що йдеться 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 і 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 жаги руйнування після невдалого злому.

6. Підпал із застосуванням елементарних засобів. Під елементарними засобами, зокрема, розуміється підпалювання з використанням сірників, запальничок або недопалків. Тому така можливість впливу існує тільки за 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 йдеться про підпали об’єктів критичної інфраструктури за допомогою речовин, що швидко та інтенсивно згорають. Можливі приклади таких диверсій:

– виливання і підпалювання горючих рідин (наприклад, бензину);

– установлення професійних пристроїв із запальним складом і таймером або дистанційним підривником.

Такі диверсії можуть вчинятися також ззовні та передбачають наявність яскраво вираженої кримінальної активності.

8. Використання вибухових речовин на об’єктах критичної інфраструктури. У цьому випадку може відбуватись застосування саморобних,

промислових або військових вибухових речовин. Можливими прикладами таких диверсій є, наприклад, такі:

– розміщення саморобної бомби-вогнегасника у чутливих ділянках установки або, що більш імовірно, − на периферії будівлі;

– підрив резервуарів і трубопроводів;

– підрив несучих елементів конструкцій, що тягне за собою перекидання резервуарів, руйнування ділянок установки.

9. Обстріл. У найпростішому випадку здійснюється обстріл з пневматичних гвинтівок або рогаток (сталевими кулями), але може йтися і про застосування важкої зброї терористами, наприклад зенітної ракетної зброї. Приклади можливого впливу на критичну інфраструктуру:

– заподіяння течі окремо встановлених резервуарів або трубопроводів;

– організація вибуху.

Обстріл може здійснюватися переважно з-за зовнішнього огородження виробничої території або промислового парку, причому більшій загрозі піддаються розташовані поблизу від огорожі ділянки установки.

10. Авіакатастрофа. У цьому випадку вплив можуть чинити як кінетична енергія падаючих літаків, так і вибух запасу пального або можливої вибухівки, що перебуває на борту літака. 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;

– дистанційного маніпулювання 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 до застосування отруйних речовин, наприклад у районі транспортних вузлів.

12. Об’єднані дії на об’єктах критичної інфраструктури. У цьому випадку також можна уявити собі широкий спектр можливостей:

– вищезгадані «брудні» бомби, що поєднують вибухову дію з радіоактивним зараженням;

– руйнування виробничого обладнання в поєднанні з поширенням небезпечних речовин;

– розрекламовані у ЗМІ індивідуальні акції із серйозними наслідками для діяльності підприємства − об’єкта критичної інфраструктури або постачання населення.

3.3. Модернізація державної політики захисту критичної інфраструктури в Україні

Для об’єктів критичної інфраструктури є характерною поліморфність типів загроз. Ці загрози можуть бути природними або спричиненими необережною поведінкою людини. Деякі загрози можуть породжуватись терористичними або іншими злочинними цілями. Кібератаки з метою отримання викупу, коли зашифровуються дані користувачів і вимагається

оплата в обмін на розблокування даних, є прикладом комерційної діяльності, яка може серйозно вплинути на об’єкти критичної інфраструктури [29; 109].

Загрози для таких об’єктів також можуть бути пов’язані із злочинною поведінкою і 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 таке: чи повинні уряди країн ухвалити єдиний план, який охоплює всі можливі загрози, або, скоріше, передбачити ухвалення стратегій, пов’язаних із конкретною небезпекою чи ризиком? Фактично будь-який підхід відповідає міжнародно-правовій базі. Серед країн, які розробили й ухвалили стратегії об’єктів критичної інфраструктури, більшість застосовує підхід з урахуванням усіх небезпек, тобто стратегічні цілі та організаційні структури сформовано таким чином, щоб ураховувати випадкові, навмисні та природні загрози для розглядуваних об’єктів у цілому.

Підхід, орієнтований на всі небезпеки, часто розглядається як передумова для найкращого використання обмежених наявних ресурсів та запобігання непотрібного дублювання. Основне обґрунтування його застосування зводиться до того, що ті ж самі процеси управління ризиками та співробітництва, а також механізми реагування на кризи можуть широко застосовуватися для реагування на всі види загроз як взаємозамінні [171; 214].

Підходи з урахуванням усіх 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 терактів.

Керівні принципи доповнюють загальну стратегію країни із забезпечення безпеки об’єктів такої інфраструктури, яка розширює сферу її дії шляхом охоплення інших небезпек [23; 82].

В Іспанії інституційну архітектуру для захисту об’єктів розглядуваної інфраструктури зафіксовано в законі 8/2011 «Про встановлення заходів для захисту критично важливих об’єктів інфраструктур». Фактично зазначений іспанський закон спрямовано на протидію терористичній загрозі, хоча він застосовується і до інших (не вказаних) ризиків.

У відповідності до резолюції 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. З огляду на цей документ будь-яка держава може визначити в межах своєї національної політики найкращі форми та способи захисту таких об’єктів від терактів у середовищі з численними загрозами.

Більшість країн, включно з тими, що не мають спеціальних стратегій, присвячених захисту об’єктів критичної інфраструктури, розглядають ці питання в різних політичних нормативних документах, розроблених різними урядовими установами. Ці документи зазвичай охоплюють національну стратегію і політику боротьби з тероризмом. Хоча такі різні політики могли бути ухвалені в різний час і різними державними установами, вкрай важливо, щоб вони стали для всіх частинами зв’язкового посилання та підходу до захисту об’єктів розглядуваної інфраструктури. Це вимагає, зокрема, щоб країни вирішили такі питання:

– взаємодія між цими й іншими політиками захисту об’єктів критичної інфраструктури та конкретною стратегією захисту таких об’єктів;

– ступінь, до якого ці й інші політики та саму стратегію захисту таких об’єктів необхідно налаштувати й оптимізувати, щоб уникнути конфліктів і забезпечити загальну координацію комплексної політики їх захисту на національному рівні.

Відповідно, далі зробимо огляд типів державної політики, які чинять значний вплив на забезпечення безпеки об’єктів критичної інфраструктури, але не обов’язково (або повністю) присвячені цілям захисту таких об’єктів [29; 173].

Зокрема, перший тип державної політики щодо захисту об’єктів критичної інфраструктури − політика щодо «легких мішеней (цілей)». 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» із тим, щоб розробити відповідні плани дій в нештатних і надзвичайних ситуаціях під часи терористичних атак.

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 т. з. легких цілей автоматично не відповідає умовам та вимогам щодо захисту об’єктів критичної інфраструктури, особливо коли йдеться про здійснення норм та правил резолюції 2341 (2017) Ради Безпеки. Втім, із цього не випливає, 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 й навпаки. Це явний підхід, ухвалений Радою Європейського Союзу − організацією, що представляє європейську індустрію безпеки і двадцять п’ять дослідницьких співтовариств. Визнаючи дублюючі функції між політиками щодо «легких цілей» і критичної інфраструктури, Рада Європейського Союзу працює з обома в тій же самій робочій групі.

Замість того щоб використовувати підхід відокремлення, слід вивчити потенціал їх 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 ті ж самі 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. При цьому варто взяти до уваги те, що національна безпека – це мінлива концепція. Країни переводять її на різні підпункти і підходи залежно від низки чинників і уявлень, що стосуються їх конкретної історії, географічного положення або геополітичного контексту [29; 173].

У більшості випадків національна безпека містить у собі принципи, різні політики, процедури і функції, спрямовані на те, щоб гарантувати незалежність, суверенітет і цілісність країни, а також права громадян. Деякі країни чітко включають об’єкти критичної інфраструктури до пріоритетів своєї нацбезпеки. Тісна прив’язка забезпечення безпеки таких об’єктів до сфери завдань нацбезпеки може допомогти забезпечити посилену політичну підтримку для подальшої розробки спеціалізованих стратегій захисту розглядуваної інфраструктури та полегшити їх реалізацію.

Третій різновид державної політики щодо захисту об’єктів критичної інфраструктури − антитерористична політика. Хоча в більшості контртерористичних стратегій ці об’єкти конкретно не згадуються, низка цілей та інституційних механізмів, викладених у них, допомагає зберегти їх цілісність 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 ними після терористичної атаки. Також стратегії боротьби з тероризмом часто встановлюють широкі межі для запобігання вчиненню терористичних злочинів (наприклад, шляхом

вивчення підготовчих законодавчих актів, налагодження взаємодії між розвідувальними та правоохоронними органами тощо).

Глобальна антитерористична стратегія Інтерполу охоплює сферу захисту об'єктів критичної інфраструктури у розділі 4.6 «Зброя і матеріали», визначаючи мандат цієї організації з точки зору «підвищення спроможності держав-членів захищати свою критично важливу інфраструктуру й уразливі цілі від фізичних та кібертерористичних атак». При цьому стратегії забезпечення безпеки зазначених об'єктів повинні об'єднувати концепції та процедури, викладені в основах політики боротьби з тероризмом шляхом їх адаптації до конкретних потреб та умов захисту розглядуваної інфраструктури.

Четвертим різновидом державної політики щодо захисту об'єктів критичної інфраструктури є політика кібербезпеки. Остання, зокрема, часто розглядається 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 посідають центральне місце в захисті об'єктів критичної інфраструктури, забезпечучи основу, на якій країни визначають цілі та засоби захисту критично важливих інформаційних інфраструктур. Водночас низка регіональних інструментів захисту об'єктів критичної інфраструктури чітко пов'язує різні поняття концепції кібербезпеки. Наприклад, Конвенція Африканського союзу про кібербезпеку (2014 рік) передбачає, що держави-члени мають зобов'язатися розробити у співпраці із зацікавленими сторонами національну політику в сфері кібербезпеки, в якій буде визнано важливість критично важливої інформаційної інфраструктури для нації, а також визначено ризики, з якими стикається нація під час використання підходу «всіх небезпек», і те, яким чином мають досягатися цілі такої політики.

Іншим прикладом є стратегія кібербезпеки Європейського Союзу 2013 року, за 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 з виявлення уразливості європейських критично важливих об'єктів інфраструктури та стимулюванню розвитку відмовостійких систем.

За директивою Європейського Союзу про мережеву та інформаційну безпеку (Директива NIS) держави-члени ЄС зобов'язані призначити операторів послуг життєзабезпечення і запровадити нові вимоги до безпеки та звітності для таких організацій. Ураховуючи це, не всі національні стратегії кібербезпеки забезпечують однакове місце об'єктам критичної інфраструктури й однаково визнають їх важливість, щодо цього між країнами існують значні відмінності. Зокрема, деякі стратегії були написані тільки стосовно кіберзлочинності або тільки щодо мережі Інтернету. Вони, як правило, упускають з уваги національні явища дестабілізації та антикризове управління для критичної інфраструктури, а також міжгалузевий вплив [28; 38; 203].

Стратегії, написані стосовно кібербезпеки, що ґрунтуються на національному оцінюванні ризику, мать більш широкі перспективи, які уможливлять забезпечення безпеки розглядуваної інфраструктури.

Корисним інструментом, запропонованим Міжнародним союзом електрозв'язку, є база («сховище») національних стратегій з кібербезпеки. Вона містить у собі велику колекцію національних стратегій кібербезпеки у вигляді одного чи кількох документів та як частину більш широких стратегій у сфері інформаційно-комп'ютерних технологій забезпечення нацбезпеки [28; 77].

Ураховуючи різноманітність підходів у різних наявних на сьогодні стратегіях захисту об'єктів критичної інфраструктури та кібербезпеки, Міжнародний союз електрозв'язку наразі очолює сумісно з різними

глобальними учасниками зусилля зі створення загального довідкового керівництва національних стратегій з кібербезпеки. Цей документ покликаний:

– дати країнам чітке розуміння цілей і змісту національної стратегії кібербезпеки;

– окреслити в загальних рисах існуючі моделі та ресурси захисту критичної інфраструктури;

– спрямовувати країни в процесі розробки своїх стратегій та оцінювання стратегії.

Окрім вищезазначеного, до національної політики належить також і державна політика захисту об'єктів критичної інфраструктури. Так, коли розробляється національна стратегія щодо захисту таких об'єктів, важливо скласти повний перелік усіх національних політик, що мають до неї стосунок.

Можуть існувати деякі політичні та нормативні структури, що стосуються інфраструктури в цілому. Наприклад, у 2017 році Сінгапур ухвалив закон «Про охорону інфраструктури». Цей закон, спеціально присвячений захисту інфраструктури від терористичних дій, вводить низку 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 в контексті активів або систем, які виконують важливі функції для спільноти.

У таких випадках необхідно визначити роль і місце наявних нормативних меж у загальних цілях захисту об'єктів критичної інфраструктури. Деякі політики можуть не згадувати такі об'єкти просто через те, що вони були ухвалені в той момент, коли саме поняття забезпечення безпеки об'єктів критичної інфраструктури ще не ввійшло в основні дискусії щодо політики, або з інших причин. Якщо вони вирішують істотні питання, що стосуються об'єктів

розглядуваної 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, держави розробили цілу низку політик, законів, положень, стратегій, планів та заходів щодо підвищення безпеки хімічних, біологічних, радіологічних та ядерних об'єктів і відповідної інформації. Забезпечити безпеку автоматизованих систем управління (далі – АСУ) критичною інфраструктурою неможливо без забезпечення безпеки АСУ критично важливими об'єктами та критичної інформаційної інфраструктури загалом [15; 17; 23].

Така ситуація обумовлена:

– повсюдним впровадженням широкого спектра інформаційних технологій в системи управління виробничими і технологічними процесами розглядуваних об'єктів;

– глобалізацією сучасних інформаційно-телекомунікаційних мереж;

– перетворенням їх на єдину світову інформаційно-телекомунікаційну мережу з розмитими межами національних сегментів;

– значним збільшенням частки розподілених АСУ критично важливими об'єктами та дедалі ширшим використанням інформаційно-телекомунікаційних мереж і мереж зв'язку загального використання для обміну інформацією.

Водночас серед чинників, що впливають на формування державної політики у сфері забезпечення безпеки АСУ критично важливою інфраструктурою, слід виділити таке:

– інтеграція в єдині комплекси АСУ таких об'єктів 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 таких АСУ;

– практика здійснення іноземними фірмами технічного обслуговування та віддаленого налагодження АСУ 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 таких АСУ до зменшення витрат і, як наслідок, використання стандартних рішень та запозиченого програмного забезпечення;

– інтенсивне вдосконалення засобів та методів використання інформаційно-комунікаційних технологій для заподіяння шкоди Україні, а також спроби їх використання в незаконних цілях і в межах конкуренції, які з часом усе частішають;

– збільшення загрози тероризму, зростання кількості незаконних дій з використанням інформаційно-комунікаційних технологій;

– тенденція приховування спроб або фактів порушення штатного функціонування АСУ таких об’єктів, що склалася серед операторів і власників інформаційних систем;

– недостатній рівень освіти та професійної підготовки персоналу, що обслуговує ці АСУ, зниження технологічної культури виробництва;

– відсутність достатнього нормативно-правового регулювання процесів забезпечення безпеки АСУ критично важливими об’єктами, серед іншого щодо визначення рівня їх реальної захищеності;

– вимушене залучення до створення АСУ таких об’єктів іноземних фірм − виробників та постачальників програмних та апаратних засобів обробки, зберігання та передання інформації та використання зарубіжних програмно-апаратних рішень, що створюють передумови для виникнення технологічної та іншої залежності від зарубіжних держав [167; 198].

При цьому головні принципи державної політики щодо забезпечення безпеки АСУ на критично важливих об’єктах повинні бути такими:

– дотримання законодавства України, а також вимог міжнародних договорів України всіма учасниками процесу створення й експлуатації таких АСУ;

– поєднання інтересів та взаємної відповідальності держави, громадян та організацій, що беруть участь у розробці, створенні та експлуатації цих АСУ;

– персоніфікація відповідальності посадових осіб, операторів, персоналу та інших осіб, які беруть участь у розробці, створенні, введенні в дію, експлуатації та модернізації цих АСУ;

– забезпечення комплексного захисту критичної інформаційної інфраструктури загалом, включно із створенням єдиної державної системи виявлення та попередження комп’ютерних атак на критичну інформаційну інфраструктуру та оцінювання рівня реального захисту її елементів;

– забезпечення дозвільного характеру діяльності в сфері забезпечення безпеки АСУ на критично важливих об’єктах з використанням механізмів ліцензування та сертифікації;

– розподіл функцій між ключовим державним органом виконавчої влади у галузі забезпечення безпеки зазначених об’єктів та інших елементів критичної інформаційної інфраструктури та іншими державними органами виконавчої влади, що здійснюють діяльність у сфері забезпечення безпеки таких об’єктів та інших елементів критичної інформаційної інфраструктури, а також органами державного нагляду та контролю за їх діяльністю й посилення координації їх діяльності;

– регламентація прав та обов’язків власників АСУ 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 під час здійснення діяльності в галузі забезпечення безпеки АСУ на таких об’єктах [82; 184].

У зазначеному контексті принципів державної політики в розглядуваній галузі основні завдання з удосконалення нормативно-правової бази у сфері забезпечення безпеки АСУ на критично важливих об’єктах повинні бути такими:

1) 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 зазначеній сфері;

в) органів державного нагляду та контролю за діяльністю зазначених об’єктів та інших елементів критичної інформаційної інфраструктури;

2) законодавче визначення та закріплення прав та обов’язків власників АСУ критично важливими об’єктами та іншими об’єктами критичної інформаційної інфраструктури та експлуатуючих організацій у сфері забезпечення безпеки таких систем;

3) визначення порядку:

а) розробки, введення в дію, експлуатації та модернізації АСУ критично важливими об’єктами та інших елементів критичної інформаційної інфраструктури;

б) отримання державним органом виконавчої влади у галузі забезпечення безпеки критичної інфраструктури інформації про такі АСУ та інші елементи зазначеної 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 такої інфраструктури;

ґ) дій посадових осіб, персоналу та власників АСУ критично важливими об'єктами та іншими елементами критичної інформаційної інфраструктури в разі виявлення спроб або фактів порушення нормативного функціонування цих об'єктів у разі комп'ютерних інцидентів;

4) 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;

5) нормативно-правове забезпечення функціонування єдиної державної системи виявлення комп'ютерних атак на критичну інформаційну інфраструктуру та моніторингу рівня її реальної безпеки;

6) установлення відповідальності за порушення порядку розробки, введення в дію, експлуатації та модернізації АСУ критично важливими об'єктами та іншими елементами критичної інформаційної інфраструктури;

7) посилення відповідальності за створення чи застосування засобів комп'ютерних атак на таку інфраструктуру;

8) оптимізація законодавства України щодо ліцензування діяльності, пов'язаної з розробленням, виробництвом, експлуатацією та технічним обслуговуванням АСУ критично важливими об'єктами [24; 46; 80].

При цьому головні завдання держуправління у сфері забезпечення безпеки зазначених АСУ є такими:

– розвиток механізмів держуправління та контролю, 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 таких АСУ та критичної інформаційної інфраструктури в цілому;

– створення єдиної державної системи виявлення та попередження комп'ютерних атак на критичну інформаційну інфраструктуру та оцінювання 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, що стимулюватимуть 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, включно з удосконаленням міжнародної кооперації у сфері забезпечення інформаційної безпеки;

– стимулювання, зокрема матеріальне, проведення приватними організаціями та особами досліджень стосовно виявлення уразливостей програмного забезпечення та устаткування, що застосовується в АСУ на критично важливих об'єктах і на інших об'єктах критичної інформаційної інфраструктури з наданням результатів державному органу виконавчої влади у сфері забезпечення безпеки критичної інфраструктури [193; 221].

При цьому головні завдання з удосконалення промислової та науково-технічної політики в галузі забезпечення безпеки АСУ критично важливими об'єктами повинні бути такими:

– здійснення комплексу заходів з розвитку систем, засобів та методів технічного оцінювання рівня реальної захищеності АСУ критично важливими об'єктами та критичною інформаційною інфраструктурою загалом;

– створення єдиних реєстрів програмних і апаратних засобів, що використовуються в таких АСУ; створення баз даних, що стосуються надійності функціонування цих систем, стану їх захищеності, технічного стану обладнання, а також оцінювання ефективності заходів безпеки, що діють і впроваджуються на критично важливих об’єктах;

– реалізація комплексу організаційно-технічних заходів щодо виключення обміну інформацією між АСУ критично важливих об’єктів через територію зарубіжних країн, а у разі технічної неможливості такого виключення – створення та застосування захисних заходів, що забезпечують відсутність будь-яких негативних наслідків впливів на процеси, керовані такими системами управління, у разі порушення штатного функціонування цього каналу зв’язку;

– розробка комплексу заходів зі створення і впровадження телекомунікаційного обладнання, стійкого до комп’ютерних атак;

– створення сховища еталонного програмного забезпечення, що використовується в АСУ на критично важливих об’єктах і на інших об’єктах критичної інформаційної інфраструктури;

– розвиток (з урахуванням мобілізаційної готовності) науково-виробничої бази, що забезпечує випуск систем (засобів) забезпечення безпеки АСУ на критично важливих об’єктах і на інших об’єктах критичної інформаційної інфраструктури;

– розроблення та впровадження імпортозамінюючих технологій, матеріалів, комплектуючих та інших видів продукції, які використовуються в таких АСУ [22; 144].

Головні завдання в галузі розвитку фундаментальної та прикладної науки, технологій та засобів забезпечення безпеки АСУ критичною інфраструктурою та критичною інформаційною інфраструктурою є такими:

– розробка методів та засобів своєчасного виявлення загроз та оцінювання їх небезпеки для АСУ критичною інфраструктурою та інших елементів критичної інформаційної інфраструктури;

– розробка та впровадження спеціалізованих інформаційно-аналітичних систем, розвиток досліджень у галузі математичного моделювання процесів забезпечення безпеки таких АСУ, спрямованих на розроблення ймовірних сценаріїв розвитку ситуації та підтримку управлінських рішень;

– розробка та впровадження комплексних систем захисту та забезпечення безпеки зазначених АСУ, 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 таких систем управління критичною інфраструктурою спеціалізованих економічно доцільних інформаційних технологій, що на технологічному рівні виключають або мінімізують обмін інформацією, що підлягає обов’язковому захисту [70; 71].

Головні завдання вдосконалення освіти, підготовки та підвищення кваліфікації кадрів у галузі забезпечення безпеки АСУ критичною інфраструктурою, а також підвищення загального рівня культури інформаційної безпеки громадян є такими:

– удосконалення системи підготовки, перепідготовки та атестації персоналу (включно з керівників) у зазначеній вище галузі на базі профільних освітніх установ;

– підвищення загального рівня культури інформаційної безпеки громадян, включно з підвищенням інформованості населення про критичну інформаційну інфраструктуру, загрозу інформаційній безпеці та способи захисту від цих загроз;

– формування у суспільній свідомості нетерпимості до осіб, які вчиняють протиправні дії із застосуванням інформаційних технологій стосовно критичної інфраструктури.

Ці основні механізми реалізуються шляхом консолідації зусиль органів державної влади й інститутів громадянського суспільства, спрямованих на захист інтересів України, за допомогою комплексного використання правових, організаційних, технічних, соціально-економічних, спеціальних тощо заходів підтримки.

Координацію діяльності державних органів виконавчої влади з реалізації цих основних механізмів здійснює ДСНС [169; 206].

Зазначені провідні напрями реалізуються в межах:

– існуючих і планованих державних програм;

– плану заходів щодо реалізації цих основних механізмів, який затверджується Урядом України.

Основні механізми й етапи реалізації державної політики у сфері забезпечення безпеки АСУ критичної інфраструктури полягають у такому [29; 55].

На першому етапі необхідно здійснити:

– підготовку плану заходів з реалізації вказаних основних механізмів;

– нормативно-правове визначення та розмежування повноважень і відповідальності державних органів виконавчої влади у сфері забезпечення безпеки, інших державних органів виконавчої влади, які здійснюють діяльність у цій у сфері, органів державного нагляду та контролю, управління діяльністю критично важливих об’єктів та об’єктів критичної інформаційної інфраструктури;

– формування порядку використання сил і засобів виявлення та попередження комп’ютерних атак на таку інфраструктуру;

– розроблення концепції використання сил і засобів ліквідації наслідків інцидентів комп'ютерних атак на цю інфраструктуру;

– визначення необхідних обсягів фінансових ресурсів і їх джерел (бюджетних та позабюджетних) для реалізації програм і планів заходів у галузі забезпечення безпеки АСУ критично важливих об'єктів та критичної інформаційної інфраструктури в цілому на період другого етапу впровадження цих основних механізмів;

– розроблення пропозицій щодо внесення змін у затверджені державні програми і коригування запланованих державних програм стосовно захисту критичної інфраструктури [22; 65].

На другому етапі необхідно здійснити:

1) розроблення нормативно-правових актів, що встановлюватимуть:

а) порядок отримання державним органом виконавчої влади у галузі забезпечення безпеки критичної інфраструктури інформації про АСУ критично важливих об'єктів та інші об'єкти критичної інформаційної інфраструктури;

б) права та обов'язки власників таких АСУ, а також експлуатуючих організацій у галузі забезпечення безпеки;

в) порядок розробки, введення в дію, експлуатації та модернізації цих АСУ;

г) регламент функціонування єдиної державної системи виявлення та запобігання комп'ютерних атак на критичну інформаційну інфраструктуру та оцінювання захищеності її елементів;

ґ) порядок усунення наслідків комп'ютерних інцидентів критичної інформаційної інфраструктури;

д) дії посадових осіб, персоналу та власників таких АСУ в разі виявлення несанкціонованого доступу до оброблюваної інформації та інших комп'ютерних інцидентів;

е) відповідальність за порушення встановленого порядку розробки, введення в дію, експлуатації та модернізації зазначених АСУ;

є) 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;

2) проведення паспортизації АСУ на критично важливих об'єктах;

3) розроблення системи грантів для приватних осіб та організацій, що стимулюватимуть дослідження у сфері виявлення уразливостей програмного забезпечення та обладнання АСУ критично важливих об'єктів та інших об'єктів критичної інформаційної інфраструктури;

4) розроблення комплексних систем захисту та забезпечення безпеки таких АСУ, що відповідають сучасному рівню розвитку інформаційно-комунікаційних технологій і мінімізують участь обслуговуючого персоналу в налаштуванні та експлуатації програмно-апаратних засобів, що входять до їх складу;

5) визначення необхідних обсягів фінансових ресурсів та їх джерел (бюджетних і позабюджетних) для реалізації програм і планів заходів у галузі забезпечення безпеки цих систем управління критично важливими об'єктами та критичної інформаційної інфраструктури загалом на наступних етапах реалізації цих основних механізмів;

6) введення в експлуатацію першого етапу Ситуаційного центру єдиної державної системи виявлення та попередження комп'ютерних атак на критичну інформаційну інфраструктуру й оцінювання рівня реальної безпеки її елементів;

7) створення сил і засобів ліквідації наслідків комп'ютерних інцидентів в критичній інформаційній інфраструктурі [23; 82].

На третьому етапі необхідно здійснити:

– впровадження комплексних систем захисту та забезпечення безпеки АСУ критично важливими об'єктами та іншими об'єктами критичної

інформаційної інфраструктури, що відповідають сучасному рівню розвитку інформаційних технологій і мінімізують участь обслуговуючого персоналу в налаштуванні та роботі програмного та апаратного забезпечення, що входить до їх складу;

– введення в дію першого етапу створення сховища еталонного програмного забезпечення, що використовується в таких АСУ;

– запровадження системи грантів для приватних осіб та організацій для стимулювання досліджень у галузі виявлення уразливостей програмного забезпечення та обладнання таких 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 оцінювання рівня реальної захищеності її елементів, а також створення ситуаційних центрів регіонального та відомчого рівнів;

– створення АСУ критично важливими об’єктами, а також спеціалізованих економічно доцільних інформаційних технологій, що виключають або в максимальному ступені знижують на технологічному рівні обмін інформацією, яка підлягає обов’язковому захисту;

– введення в експлуатацію в цілому єдиної державної системи виявлення та попередження комп’ютерних атак на критичну інформаційну інфраструктуру та оцінювання рівня реальної захищеності її елементів [72; 137; 193].

У період після 2030 року має здійснюватися комплекс заходів з підтримки організаційної, економічної, науково-технічної і технологічної готовності України до запобігання загрозам безпеки її критичній інформаційній інфраструктурі.

Відповідно, у цій роботі пропонується створити єдину державну систему безпеки значущих об’єктів критичної інформаційної інфраструктури, що є комплексом взаємопов’язаних методологічних, організаційних і технічних

рішень для управління процесами захисту таких об’єктів та підвищення ефективності їх захисту на всіх етапах їх життєвого циклу [219; 221].

У межах проєкту 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 проєктування систем захисту інформації значущих об’єктів критичної інфраструктури;

– впровадження систем захисту інформації таких об’єктів;

– створення центру моніторингу та управління інцидентами, що стосуються інформаційної безпеки критично важливих інфраструктурних об’єктів.

Зокрема, в межах створення центру моніторингу й управління інцидентами інформаційної безпеки об’єктів критичної інфраструктури пропонуються:

1) впровадження (зокрема, постачання програмно-апаратних рішень) і розвиток системи аналізу та моніторингу подій безпеки, включно з:

а) розробленням кореляційних правил;

б) підключенням джерел подій, серед іншого таких, що не підтримуються штатно;

в) розробленням звітності технічної, експлуатаційної й організаційної документації системи;

2) постачання, інтеграцію та впровадження засобів сегмента органів державного регулювання;

3) розроблення та впровадження процесів і регламентів функціонування центру моніторингу й управління інцидентами об’єктів критичної інфраструктури, включно з регламентами взаємодії з органами державного регулювання;

4) навчання відповідального персоналу служб інформаційної безпеки й інформаційних технологій, включно з проведенням кібернавчання [29; 172].

Створення єдиної інформаційної платформи для консолідації даних про об'єкти критичної інфраструктури, засоби та системи захисту інформації важливих об'єктів такої інфраструктури, включно із системами захисту інформації, та про їх відповідність чинній нормативно-правовій базі України, а також українським та міжнародним стандартам у галузі захисту інформації значно підвищить рівень держуправління критичною інфраструктурою загалом [137; 193].

Так, впровадження єдиної системи безпеки значущих об'єктів критичної інформаційної інфраструктури дозволить: забезпечити відповідність вимогам нормативно-правової бази, вжити необхідних заходів з підключення до державної системи виявлення, запобігання та ліквідації наслідків комп'ютерних атак на інформаційні ресурси України; мінімізувати ризики штрафних санкцій і приписів з боку регулюючих органів, а також притягнення до адміністративної та кримінальної відповідальності працівників організації, які настають у разі виявлення 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 таких об'єктів; підвищити рівень обізнаності персоналу у сфері інформаційної безпеки такої 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 належить 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 такої інфраструктури.

Висновки до третього розділу

1. Обґрунтовано, що для практичної реалізації заходів держуправління, які стосуються стратегічних ризиків для критичної інфраструктури, треба застосовувати системно-правовий, політичний, інформаційний, економічний й організаційно-адміністративний механізми у межах комплексного механізму держуправління забезпеченням безпеки критичної інфраструктури.

Зокрема, щодо системно-правового механізму є необхідними розробка на загальнодержавному та регіональному рівнях нового та розвиток чинного законодавства, яке охоплюватиме найважливіші, значущі та пріоритетні для нацбезпеки 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 ухвалення в цій галузі базового закону, який би визначить основні поняття, види та категорії зазначених об'єктів і встановить вимоги до забезпечення безпеки окремих категорій таких об'єктів.

У межах політичного механізму насамперед необхідно розробити й офіційно визнати на вищому рівні концепцію державного управління стратегічними ризиками для критичної інфраструктури як методологічне підґрунтя вирішення завдання забезпечення сталого розвитку України.

Інформаційний механізм координуватись компетентним органом, починаючи від введення складу і показників стратегічних ризиків для критичної

інфраструктури, оцінювання очікуваного збитку від їх реалізації, до їх подання органам державного регулювання, ЗМІ та громадськості в зручному і зрозумілому вигляді.

Економічний механізм зниження стратегічних ризиків для критичної інфраструктури має охоплювати як пряме регулювання на основі цільових витрат державних бюджетів, так і непряме економічне регулювання за рахунок удосконалення податкового та кредитного механізмів щодо зниження податкового навантаження.

Для вдосконалення організаційно-адміністративних механізмів необхідно створити в межах проведеної в державі адміністративної реформи державного компетентного органу «стратегічного ризик-менеджера» з усім необхідним для його функціонування, зокрема з повноцінною координацією інфраструктури. Реформа органів державної влади потребуватиме залучення висококваліфікованих ризик-менеджерів у структурах управління на загальнодержавному, регіональному і місцевому рівнях.

Важливу роль у справі становлення організаційних важелів стратегічного управління ризиками для критичної інфраструктури відіграватимуть: удосконалення державних систем нагляду та контролю; оптимальний розподіл виконавчих та контрольних функцій між рівнями державного та муніципального управління; оптимізація діяльності всіх органів державної влади, причетних до процесу управління критичною інфраструктурою.

2. Висвітлено роль державно-приватного партнерства для захисту об’єктів критичної інфраструктури. Підкреслено, що приватні оператори перебувають в авангарді інвестицій та головних зусиль у розробці нових технологій виробництва і захисту. Ці обставини в поєднанні з тим, що основна відповідальність за захист активів та систем об’єктів розглядуваної інфраструктури покладається на їх власників та операторів, підкреслює

важливість налагодження ефективного державно-приватного партнерства для досягнення належного рівня стійкості критично важливих об’єктів.

3. Доведено, що система держуправління стосовно захисту критичної інфраструктури повинна мати два рівня ухвалення рішень – загальнодержавний і регіональний, а також відповідні політичні, правові, інституційні, адміністративні, економічні, науково-технічні тощо механізми.

Зазначено, що для кожного з рівнів треба визначити відповідні повноваження та передбачити ступінь відповідальності за ухвалені рішення: на загальнодержавному рівні − щодо управління зовнішніми та внутрішніми стратегічними ризиками для критичної інфраструктури, на регіональному − внутрішніми ризиками.

4. Запропоновано виділяти такі складові комплексної державної політики, які суттєво впливають на забезпечення безпеки об’єктів критичної інфраструктури, але не обов’язково або не повністю є присвяченими цілям захисту цих об’єктів: політика щодо «легких цілей (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 й інститутів громадянського суспільства, спрямованих на захист інтересів України, зокрема правові, організаційні, технічні, соціально-економічні та спеціальні заходи.

ВИСНОВКИ

У монографії обґрунтовано теоретичні засади та розроблено науково-практичні рекомендації щодо вдосконалення процесів державного управління забезпеченням безпеки критичної інфраструктури. Основні висновки за результатами проведеного дослідження такі.

1. Розкрито сутність критичної інфраструктури як об’єкту державного управління. Обґрунтовано, що у процесі державного управління такими об’єктами слід виділяти два рівні, для кожного з яких характерним є певний зміст.

Зокрема, перший рівень охоплює 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 тощо чинників.

Другий рівень процесу державного управління функціонуванням об’єктів розглядуваної інфраструктури стосується організаційно-технічних систем. Базовими елементами системи державного управління на цьому рівні є такі:

– функціональний контур та інформаційні технології;

– методи та засоби розроблення та ухвалення управлінських рішень;

– методичний апарат аналізу й оцінювання ризику, що враховуватиме соціальні, економічні та інші аспекти.

2. Визначено особливості формування та функціонування державної системи захисту критичної інфраструктури. Показано, що на формування вказаної системи захисту такої інфраструктури України під час НС і терористичних актів впливає велике коло тісно пов’язаних між собою закономірностей. Їх доцільно об’єднати в дві великі групи, що відображають соціально-економічний і організаційний характер будівництва системи.

Зокрема, група закономірностей соціально-економічного характеру відбиває зв'язок формування системи забезпечення безпеки населення та захисту критично важливих об'єктів України під час НС і терактів із зовнішніми та внутрішніми умовами розвитку суспільства та держави.

Інша група закономірностей має організаційний характер і виражає внутрішні складові, притаманні лише цій системі, що більшою мірою зумовлюють особливості її формування порівняно з іншими державними системами, і характеризує взаємозв'язок між складовими системи, а також внутрішню логіку формування кожної з них.

3. Проаналізовано Закордонний досвід державного управління забезпеченням безпеки критичної інфраструктури. Зокрема, виділено такі основні риси цієї діяльності: системи управління діями у кризових ситуаціях мають державний статус; діяльність з попередження та ліквідації кризових ситуаціях вважається важливою соціальною функцією кожної держави і реалізується більшістю державних структур; право запровадження особливого режиму діяльності органів управління та населення в зоні лиха надається не лише 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 дедалі сильніше 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 вибір стратегії управління кібербезпекою критичної інфраструктури може здійснюватися на основі інформованості лише для тих держав, які перебувають на самісінькому 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 у ролі відомства, відповідального за всі аспекти національної кібербезпеки.

4. Окреслено особливості державного управління забезпеченням безпеки критичної інфраструктури в Україні. Відзначено, що наразі перед державним управлінням, зокрема у сфері забезпечення згаданої безпеки, об'єктивно стоять такі цілі: формування нових інститутів державної влади та оптимізація діяльності наявної системи виконавчої влади (адміністративна реформа); розгортання та зміцнення суспільних інститутів, які забезпечують стійкість демократичності суспільства та держави; розроблення й реалізація соціальних та адміністративно-правових регуляторів, які гарантують конституційно проголошений набір прав, свобод та обов'язків громадян України; розроблення та практичне втілення державної політики, спрямованої на забезпечення громадської безпеки та захисту об'єктів зазначеної 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 подальшого формування та функціонування всеукраїнського ринку.

5. Проаналізовано вітчизняний нормативно-організаційний механізм державного управління забезпеченням безпеки критичної інфраструктури. Зауважено, що в Україні діє декілька нормативно-правових актів, що регулюють інформаційну безпеку об'єктів критичної інфраструктури.

Щодо безпосередніх правових норм державного управління критичною інфраструктурою було розроблено проєкт Закону України «Про критичну інфраструктуру та її захист», покликаний забезпечити формування потрібної для цього нормативно-правової бази.

Із цього випливає, що наразі нормативно-організаційний механізм захисту критичної інфраструктури в Україні необхідно суттєво вдосконалити, зважаючи на відсутність специфічних нормативно-правових актів у цієї галузі, а також щодо функціонального розгалуження органів державної влади та місцевого самоврядування. При цьому ключовим органом державної виконавчої влади із захисту зазначених об'єктів є Державна служба України з надзвичайних ситуацій з урахуванням ймовірності виникнення на цих об'єктах природних чи техногенних аварій або катастроф.

6. Запропоновано напрями трансформації державних механізмів забезпечення безпеки та підвищення ефективності захисту критичної інфраструктури. Обґрунтовано, що для практичної реалізації заходів державного управління стратегічними ризиками стосовно критичної інфраструктури слід застосовувати системно-правовий, політичний, інформаційний, економічний й організаційно-адміністративний механізми у межах комплексного механізму державного управління критичною інфраструктурою.

Зокрема, для системно-правового механізму слід розробити на загальнодержавному та регіональному рівнях нове й удосконалити чинне законодавство, яке охопить найбільш важливі, значущі та пріоритетні для нацбезпеки 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 ухвалення базового закону в цій галузі, який визначатиме основні поняття, види та категорії зазначених об'єктів, а також передбачить вимоги до забезпечення безпеки окремих категорій таких об'єктів.

У межах політичного механізму необхідно, перш за все, розробити й офіційно визнати на вищому рівні Концепцію державного управління

стратегічними ризиками для критичної інфраструктури як методологічне підґрунтям для виконання завдання із забезпечення сталого розвитку України.

Інформаційний механізм має забезпечувати координацію з боку компетентного органу, починаючи з введення складу та показників стратегічних ризиків для критичної інфраструктури й оцінювання очікуваних збитків від їх реалізації до їх подання органам державного управління, ЗМІ та громадськості у зручній та зрозумілій формі.

Економічний механізм зниження стратегічних ризиків для критичної інфраструктури має охоплювати як пряме регулювання на основі цільових витрат державних бюджетів, так і непряме економічне регулювання за рахунок удосконалення податкового та кредитного механізмів щодо зниження податкового навантаження.

Для вдосконалення організаційно-адміністративних механізмів необхідно створити в межах проведеної в державі адміністративної реформи державного компетентного органу «стратегічного ризик-менеджера» з усім необхідним для його функціонування, зокрема з повноцінною координацією інфраструктури. Реформа органів державної влади потребуватиме залучення висококваліфікованих ризик-менеджерів у структурах управління на загальнодержавному, регіональному і місцевому рівнях.

7. Виокремлено шляхи удосконалення системи державного управління захистом критичної інфраструктури. Доведено, що ця система повинна мати два рівня ухвалення рішень – загальнодержавний і регіональний, а також відповідні політичні, правові, інституційні, адміністративні, економічні, науково-технічні тощо механізми.

Зазначено, що для кожного з рівнів треба визначити відповідні повноваження та передбачити ступінь відповідальності за ухвалені рішення: на загальнодержавному рівні − щодо управління зовнішніми та внутрішніми

стратегічними ризиками для критичної інфраструктури, на регіональному − внутрішніми ризиками.

8. Визначено орієнтири модернізації державної політики захисту критичної інфраструктури в Україні. Запропоновано виділяти такі складові комплексної державної політики, які суттєво впливають на забезпечення безпеки об’єктів цієї інфраструктури, але не обов’язково або не повністю є присвяченими цілям захисту згаданих об’єктів: політика щодо «легких цілей (мішеней)», політика національної безпеки, антитерористична політика та політика кібербезпеки.

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 й інститутів громадянського суспільства, спрямованих на захист інтересів України, зокрема правові, організаційні, технічні, соціально-економічні та спеціальні заходи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Апостол О. І. Удосконалення досвіду країн Європи та США відносно нормативно-правового забезпечення конкурентоспроможності економіки. *Адаптація правової системи України до права Європейського Союзу : теоретичні та практичні аспекти* : матеріали IV Всеукраїнської науково-практичної конференції за міжнародною участю. Полтава : Россава, 2019. Ч.2. С. 11–12.

2. Андреєв С. О. Формування інституціональних засад діяльності органів місцевого самоврядування в Україні як суб'єктів забезпечення цивільного захисту. *Вісник Національного університету цивільного захисту України. Серія. Державне управління*. 2016. Вип. 1 (4). С. 223–235.

3. Андронов В. А., Варивода Є. О. Державні механізми забезпечення екологічної оцінки у сфері запобігання і ліквідації наслідків надзвичайних ситуацій. *Теорія та практика державного управління : зб. наук. пр.* Харків : Вид-во ХарРІ НАДУ «Магістр», 2013. № 4. С. 236–244.

4. Андрусяк Т. Г. Теорія держави і права : навч. посіб. Львів, 1997. 198 с.

5. Антонов В. О. Суспільство як об'єкт національної безпеки Української держави. *Держава і право. Юридичні і політичні науки*. 2013. Вип. 60. С. 79–84.

6. Аудит пожежної і техногенної безпеки. URL: http://audit.nuczu.edu.ua/ (дата звернення: 13.03.2024).

7. Бабков Ю. П., Адамчук М. М. Запобігання та ліквідація надзвичайних ситуацій. *Збірник наукових праць Харківського університету Повітряних Сил*. 2015. Вип. 4 (45). С. 153–157.

8. Бакуменко В. Д. Методологія державного управління проблеми встановлення та подальшого розвитку. *Вісник УАДУ*. 2003. № 2. С. 11–27.

9. Бакуменко В. Д. Прийняття рішень в державному управлінні : навч. посібн. [у 2 ч.]. Київ : ВПЦ АМУ. Ч. 1 : Теоретико-методологічні засади, 2010.

276 с.

10. Бакуменко В. Д. Прийняття рішень в державному управлінні : навч. посібн. [у 2 ч.]. Київ : ВПЦ АМУ. Ч. 2 : Науково-прикладні аспекти, 2010. 276 с.

11. Бакуменко В. Д., Надолішній П. І., Їжа М. М. та ін. Державне управління : основи теорії, історія і практика : навч. посіб. / за заг. ред. П. І. Надолішнього, В. Д. Бакуменка. Одеса : ОРІДУ НАДУ, 2009. 394 с.

12. Барило О. Г., Потеряйко С. П. Удосконалення організаційного механізму державного управління у надзвичайних ситуаціях. *Вісник Національного університету цивільного захисту України. Серія. Державне управління*. 2016. Вип. 2 (5). С. 264–272.

13. Баштанник В. В. Трансформація державного управління в контексті європейських інтеграційних процесів : монографія. Дніпропетровськ : ДРІДУ НАДУ, 2010. 390 с.

14. Безугла В. О. Інтегральна оцінка конкурентоспроможності регіонів України. *Комунальное хозяйство городов: научно-технический сборник*. 2005. № 70. С. 53–60.

15. Бєлай С. В. Державні механізми протидії кризовим явищам соціально-економічного характеру: теорія, методологія, практика : монографія. Харків : Видавництво НАНГУ, 2015. 249 с.

16. Бєлоусов А. В. Наукові підходи до визначення ризику надзвичайних ситуацій як об’єкту управління. *Наукові розвідки з державного та муніципального управління*. 2015. №1. С. 224–235.

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

18. Безпека людини у надзвичайних ситуаціях : навч. посіб. / За ред. В. І. Голінька. Дніпро : Національний гірничий університет, 2011. 161 с.

19. Біла С. О. Структурна політика в системі державного регулювання

економіки. Київ : Вид-во УАДУ, 2001. 408 с.

20. Білоусов А. В. Сутність, складові та зміст комплексного механізму державного управління ризиками надзвичайних ситуацій. *Державне будівництво*. 2014. № 2. URL: http://www.kbuapa.kharkov.ua/e-book/db/2014-2/doc/2/10.pdf (дата звернення: 13.03.2024).

21. Білявська О. Міжнародні стандарти управління ризиками. *Управління сучасним містом*. 2008. № 1–4/1–12 (29−32). С. 50–56.

22. Бірюков Д. Концепція захисту критичної інфраструктури як елемент загальноєвропейської безпекової політики. *Наукові записки*. 2013. – № 6 (68). С. 106−115.

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

24. Бліщук К. М. Економічний аналіз державної політики: теорія та застосування : навч. посібн. Львів : ЛРІДУ НАДУ, 2011. 160 с.

25. Бобро Д. Г. Удосконалення методології ранжування об’єктів критичної інфраструктури та їх віднесення до критичної інфраструктури : аналітична записка. URL: http://www.niss.gov.ua/content/articles/files/krutuchna_infra-a7636.pdf (дата звернення: 13.03.2024).

26. Бойко-Бойчук О. В. Механізми державного управління: узагальнена модель. URL: concept.at.ua/load/0-0-0-34-20 (дата звернення: 13.03.2024).

27. Болотських М. В., Андреєв С. О. Державна політика у сфері цивільного захисту: аналіз базових (ключових) законодавчих термінів та понять. *Актуальні проблеми державного управління*. 2008. Вип. 1 (33). С. 16−22.

28. Борденюк В. І. Місцеве врядування та державне управління: конституційно-правові основи співвідношення та взаємодії : монографія. Київ : Парлам. вид-во, 2007. 576 с.

29. Борденюк В. І. Окремі аспекти наукового забезпечення реформування місцевого самоврядування в Україні. *Юридична наук*а. 2011. № 1. С. 71−78.

30. Бурдяк О. В. Конкурентоспроможність регіонів як необхідна передумова зростання конкурентоспроможності країни. URL: http://intkonf.org/burdyakov-konkurentospromozhnist-regioniv-yakneobhidna-peredumova-zrostannyakonkurentospromozhnosti-krayini/ (дата звернення: 14.03.2024).

31. Бурячок В. Л., Толубко В. Б., Хорошко В. О. та ін. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / за заг. ред. д-ра техн. наук, професора В. Б. Толубка. Київ : ДУТ, 2015. С. 12.

32. Важинський Ф. Основні методи прогнозування соціально-економічного розвитку регіону. *Збірник науково-технічних праць Українського державного лісотехнічного університету*. 2004. Вип. 14.7. С. 166−170.

33. Валевський О. Л. Держава і реформи в Україні: аналіз державної політики в умовах трансформації суспільства : монографія. Київ : Вид-во НАДУ, 2007. 217 с.

34. Вакуленко В. М., Гринчук Н. М. Державна регіональна політика : навч. посіб. Київ : Вид-во НАДУ. 64 с.

35. Ведунг Е. Оцінювання державної політики та програм. Київ : ВСЕУВИТО, 2003. 350 с.

36. Вітлінський В. В., Великоіваненко П. І. Ризикологія в економіці та підприємництві : монографія. Київ : КНЕУ, 2004. 480 с.

37. Виживання в умовах надзвичайних ситуацій / П. Б. Волянський, О. Г. Барило, С. О. Гур’єв та ін. Харків : ФОП Панов А.М., 2016. 189 с.

38. Вовченко С. Д. Розвиток теоретичних основ функціонування системи захисту населення і територій від надзвичайних ситуацій. *Економіка та держава*. 2013. № 10. С. 141–144.

39. Волошин С. М. Нормативно-правове забезпечення техногенно–

природної безпеки. *Надзвичайна ситуація*. 2013. № 1. С. 33–35.

40. Волянський П. Б. Методологічні підходи до управління ризиками в процесі ліквідації наслідків надзвичайних ситуацій. *Інвестиції: практика та досвід*. 2013. № 13. С. 134–136.

41. Воротін В. Є. Макроекономічне регулювання в умовах глобальних трансформацій : монографія. Київ : УАДУ, 2002. 392 с.

42. Гаєвський Б., Ребкало В. Культура державного управління: організаційний аспект : монографія. Київ : Вид-во УАДУ, 1998. 144 с.

43. Гамов М. С., Шнирков О. І. Регіональна конкурентоспроможність економіки України : навч. посіб. Запоріжжя : ЗНТУ, 2011. 292 с.

44. Ганцюк Т. До проблеми визначення елементів комплексного механізму державного управління. *Державне управління та місцеве самоврядування*. 2014. Вип. 3(22). С. 17–26. URL: http://www.dbuapa.dp.ua/vidavnictvo/ 2014/2014_03(22)/4.pdf (дата звернення: 14.03.2024).

45. Геєць В. Державні цільові програми та упорядкування програмного процесу в бюджетній сфері. Київ : Наук. думка, 2008. 384 с.

46. Герасимчук З. В., Ковальська Л. Л. Конкурентоспроможність регіону: теорія, методологія, практика : монографія. Луцьк : Надстир'я, 2008. 248 с.

47. Герасимчук З. В., Поліщук Г. В. Стимулювання сталого розвитку регіону: теорія, методологія, практика : монографія. Луцьк : РВВ ЛНТУ, 2011. 514 с.

48. Голікова Т. Державне управління територіальним економічним розвитком: теорія і практика : монографія. Київ : Вид-во НАДУ, 2007. 296 с.

49. Головкова Л. С. Управління конкурентоспроможністю потенційних можливостей підприємства в умовах кризи. *Держава та регіони*. *Серія: Економіка та підприємство*. 2009. № 4. С. 47−52.

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

51. Головач Т. В. Грушевицька А. Б., Швид В. В. Ризик-менеджмент: зміст і організація на підприємстві. *Вісник Хмельницького національного університету*. 2010. № 3. Т.1. С. 157-163.

52. Горбулін В. П., Качинський А. Б. Засади національної безпеки України. Київ : Інтертехнологія, 2009. 272 с.

53. Гортенко І. О., Тарангул Л. Л. Економічні райони України : посіб. Київ : Вища школа, 1999. 205 с.

54. Грачов В. Класифікація ризиків та управління ними. *Фінанси України*. 2002. № 10. С. 56–60.

55. Гриньова В. М. Державне регулювання економіки : підручник. Київ : Знання, 2008. 398 с.

56. Гур'єв С., Радиш Я., Терент'єва А. Завдання кризового менеджменту й управління надзвичайними ситуаціями в державному управлінні. *Університетські наукові записки : наук. зб. пр.* 2012. № 2 (20). С. 285–290.

57. Гурне Б. Державне управління. Київ : Основи, 1993.165 с.

58. Данилишин Б. В., Ковтун В. В., Степаненко А. В. Наукові основи прогнозування природно-техногенної безпеки. Київ : ЛексДім, 2004. 520 с.

59. Державна служба статистики України (офіційний сайт). URL: http://www.ukrstat.gov.ua/ (дата звернення: 14.03.2024).

60. Державна регіональна політика України: особливості та стратегічні пріоритети : монографія / за ред. З. С. Варналія. Київ : НІСД, 2007. 820 с.

61. Державне регулювання економіки : навч. посіб. / С. М. Чистов, А. Є. Никифоров, Т. Ф. Куценко. Київ : КНЕУ, 2005. 440 с.

62. Державне управління : навч. посіб. / А. Ф. Мельник, Ю. О. Оболенський, А. Ю. Васіна, Л. Ю. Годієнко. Київ : Знання-Прес, 2003.

343 с.

63. Державне управління : словник-довідник / заг. ред. В. М. Князєва, В. Д. Бакуменка. Київ : Видавництво УАДУ, 2002. 228 с.

64. Державне управління в Україні : навч. посібн. / за заг. ред. В. Б. Авер'янова. Київ : Юрінком Інтер, 1998. 432 с.

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

66. Державне управління: теорія і практика: навч. посіб. / за ред. В. Авер'янова. Київ : Юрінком-Інтер, 1998. 431 с.

67. Державне управління в умовах адміністративної реформи в Україні / за заг. ред. Н. Р. Нижник, О. Д. Крупчана. Київ : Вид. дім «Ін-Юре», 2002. 95 с.

68. Державне управління і менеджмент : навч. посіб. у таблиця і схемах / Г. С. Одінцова, Г. І. Мостовий, О. Ю. Амосов та ін. Харків : ХарРІДУ УАДУ, 2002. 492 с.

69. 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. Харків : Вид-во ХаРІДУ НАДУ «Магістр», 2014. 320 с.

70. Державний науково-технічний центр з ядерної та радіаційної безпеки: 20 років. Київ : Основа, 2012. 344 с.

71. Дєгтяр О. А. Державне та регіональне управління в соціальній сфері : монографія. Харків : С.А.М., 2015. 552 с.

72. Дєгтяр А. О., Крюков О. І. Правове забезпечення державного регулювання інновацій в Україні. *Державне будівництво*. 2011. № 2. URL: http://www.nbuv.gov.ua/e-journals/DeBu/2011-2/index.html (дата звернення: 14.03.2024).

73. Дєгтяр А. О., Степанов В. Ю., Тарабан С. В. Управлінські рішення в

органах державної влади : монографія. Харків : Вид-во ХарРІ НАДУ «Магістр», 2010. 275 с.

74. Дегтярьова І. О. Фактори підвищення конкурентоспроможності сучасного регіону. URL: http://www.ac-ademy.gov.-ua/ej/ej9/doc_pdf/Degtyareva_IO.pdf (дата звернення: 14.03.2024).

75. Джигирей В. С., Шидецький В. Ц. Безпека життєдіяльності : навч. посіб. Львів: Афіша, 2000. 256 с.

76. Дзьобань О. П. Національна безпека в умовах соціальних трансформацій: методологія дослідження та забезпечення : монографія. Харків : Константа, 2006. 440 с.

77. Дзюндзюк В. Б. Вплив надзвичайних ситуацій на соціально-економічний розвиток територій. *Державне будівництво*. 2013. № 2. URL: http://www.kbuapa.kharkov.ua/e-book/db/2013-2/doc/2/01.pdf (дата звернення: 13.03.2024).

78. 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.

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

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

81. Домарацький М. Б. Нормативне й адміністративне забезпечення державного регулювання критичної інфраструктури в Україні: аналіз і оцінка. *Вісник Національного університету цивільного захисту України*. *Серія «Державне управління»*. 2020. Вип. 1 (12). С. 470–475.

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

83. Домарацький М. Б. Специфіка державного регулювання критичної інфраструктури в Україні. *Публічне управління та митне адміністрування*. 2020. № 2(25). С. 24–28.

84. Домбровська С. М., Коврегін В. В., Помаза-Пономаренко А. А. та ін. Державне управління у сфері безпеки соціально-еколого-економічних систем : монографія. Харків : НУЦЗУ, 2017. 244 с.

85. Домбровська С. М. Забезпечення ефективного державного управління підготовкою фахівців у сфері цивільного захисту: створення професійних стандартів. *Теорія та практика державного управління*. 2012. Вип. 4 (39). С. 386–390.

86. Домбровська С. М., Полторак С. Т. Механізми формування безпеки держави. Теорія та практика державного управління і місцевого самоврядування. 2015. № 1. URL: http://el-zbirn-du.at.ua/ (дата звернення : 13.03.2024).

87. Домбровська С. М., Гусаров О. О., Дуднєва Ю. Е. Проблеми та перспективи розвитку державного управління : монографія. Харків : УІПА, 2014. 172 с.

88. Дометрична допомога в умовах надзвичайних ситуацій : практичний посібник / П. Б. Волянський, С. О. Гур’єв, М. Л. Долгий та ін. Харків : ФОП Панов А. М., 2016. 136 с.

89. Дубенко С. Д. Державна служба і державні службовці в Україні : навч.-метод. посібник / За заг. ред. д-ра юрид. наук, проф. Н. Р. Нижник. Київ : Ін Юре, 1999. 244 с.

90. Дубов Д. В., Ожеван М. А. Майбутнє кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців :

аналітична доповідь. Київ : НІСД, 2012. С. 22.

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

92. Енциклопедія державного управління: у 8 т. / наук.-ред. колегія : Ю. В. Ковбасюк (голова) та ін. – Київ : НАДУ, 2011. Т. 2 : Методологія державного управління / наук.-ред. колегія : Ю. П. Сурмін (співголова), П. І. Надолішній (співголова) та ін. Київ : Нац. акад. держ. упр. при Президентові України, 2011. 692 с.

93. Ефективність державного управління / Ю. Бажал, О. Кілієвич, О. Мертенс та ін. ; за заг. ред. І. Розпутенка. – Київ : К.І.С., 2002. 420 с.

94. Європейський цивільний захист. URL: http://ec.europa.eu/ environment/civil/prote/cp10_en.htm (дата звернення: 13.03.2024).

95. Єлагін В. П. Моделювання процесів синергитичної взаємодії головних інститутів. *Державне будівництво*. 2011. № 2. URL: http://nbuv.gov.ua/UJRN/DeBu_2011_2_56 (дата звернення: 14.03.2024).

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

97. Жукова Л. А. Основні стратегічні напрямки державного управління ризиками // *Зб. наук. праць УАДУ*. 2002. Вип. 2. С. 120–129.

98. Запорожець О. І. Безпека життєдіяльності. Київ : Центр навчальної літератури, 2013. 448 с.

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

100. Зелена книга з питань захисту критичної інфраструктури в Україні. URL: http://www.niss.gov.ua/public/ File/2015_table/

Green%20Paper%20on%20CIP_ua.pdf (дата звернення: 13.03.2024).

101. Землянкін А. Механізми управління інноваціями в Україні: стан і перспективи вдосконалення. *Стратегічні пріоритети*. 2014. № 2 (31). С. 43−44.

102. Зеркалов Д. В., Кацман М. Д., Ковтун А. І. Наукові основи цивільного захисту : монографія. Київ : Основа. 2014. 1117 с.

103. Іванець Г. В. Алгоритм прогнозування надзвичайних ситуацій соціального характеру за видами та рівнями, можливих завданих збитків внаслідок них. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2016. № 4 (49). С. 173–176.

104. Іванченко О. М. Методологічні засади універсалізації національного права. *Наукові праці НУ «Одеська юридична академія».* 2013. С. 529–538.

105. Іванюта С.П. Запровадження сучасних підходів для зниження ризику природних катастроф в Україні. Стратегічні пріоритети. 2016. №1 (38). С.110–117.

106. Івашов М. Ф. Актуальні питання економічної теорії та практики її застосування в державному управлінні. Київ : Вид-во НАДУ. 2004. 64 с.

107. Івашов М. Ф. Виклики і загрози епохи глобалізації. *Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія»*. 2012. Т. 186. Вип. 174. С. 84−88.

108. Ігнатова Т. Інституційне середовище в розвитку конкурентоспроможності регіональної економіки. URL: htts://econom.nsc.ru/conf08/info/doklad/ignat2.doc (дата звернення: 14.03.2024).

109. Карамишев Д. В., Прасол В. П. Публічне управління як специфічний вид управлінської діяльності в умовах суспільних трансформацій. *Інвестиції: практика та досвід*. 2014. № 24. С. 156-160.

110. 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.

111. Карпенко О. В. Механізми формування та реалізації сервісно-орієнтованої державної політики в Україні : дис. … д-ра н. з держ. упр. : 25.00.02. Київ, 2016. 37 с.

112. Коваленко С. І. Стратегічні пріоритети підвищення конкурентоспроможності транскордонних регіонів в умовах розширення ЄС. *Вісник соціально-економічних досліджень*. 2013. Вип. 2 (49). Ч. 1. С. 123−130.

113. Коваль О. П. Соціальна безпека: сутність та вимір : наук. доп. . Київ : НІСД, 2016. 34 с.

114. Ковбасюк Ю. В., Бакуменко В. Д. Державне регулювання в умовах ринкової економіки. *Енциклопедія державного управління* : у 8 т. Київ : НАДУ, 2011. Т. 1: Теорія державного управління. С. 153–154.

115. Козьменко О. В. Фінансові методи управління катастрофічними ризиками. *Актуальні проблеми економіки*. 2011. № 4. С. 217–224.

116. Колодій А. М., Копєйчиков В. В., Лисенков С. Л. та ін. Теорія держави і права : навч. посіб. Київ : Юрінком Інтер, 2002. 368 с.

117. Конституція України : станом на 1 верес. 2016 р.: відповідає офіц. тексту. Харків : Право, 2016. 82 с.

118. Корченко А. О., Козачок В. А., Гізун А. І. Метод оцінки рівня критичності для систем управління кризовими ситуаціями. *Захист інформації*. 2015. № 1. Т. 17. С. 86–98.

119. Костюк І. Україна в фокусі кібератак. URL: https://scienceukraine.com/sciblogs/ukraina-v-fokusi-kiberatak (дата звернення: 13.03.2024).

120. Коротич О.Б. Державне управління регіональним розвитком України : монограф. Харків : Вид-во ХарРІ НАДУ «Магістр», 2006. 220 с.

121. Костенко В. Модернізація державної системи цивільного захисту в контексті європейської інтеграції України. *Державне управління та місцеве*

самоврядування. 2013. Вип. 4 (19). С. 107–115.

122. Кравченко О. М. Теоретичні підходи до визначення поняття “механізм державного управління”. *Державне управління: удосконалення та розвиток*. 2009. № 3. URL: http://www.dy.nayka.com.ua/index.php?operation=1&iid=56 (дата звернення: 14.03.2024).

123. Кризовий менеджмент та принципи управління ризиками в процесі ліквідації надзвичайних ситуацій : монографія / С. О. Гур’єв, А. В. Терент’єва, П. Б. Волянський. Київ : б. в., 2008. 148 с.

124. Кравчук М. В. Теорія держави і права (опорні конспекти) : навч. посіб. для студ. вищ. навч. закл. Київ : Атіка, 2003. 288 с.

125. Кравців С. Я., Соболь О. М., Коссе А. Г. Ризик-орієнтований підхід у державному регулюванні у сфері техногенної та пожежної безпеки. *Вісник Національного університету цивільного захисту України. Серія: Державне управління*. 2017. Вип. 1 (6). С. 336–341.

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

127. Криштанович М. Ф. Реалізація механізмів публічного управління у сфері цивільного захисту України щодо національної безпеки. *Вісник Національного університету цивільного захисту України. Серія: Державне управління*. 2017. Вип. 1 (6). С. 341–347.

128. Кудлай Т. П. Теорія держави і права : навч. посіб. − Київ : НАДУ, 2009. 94 с.

129. Кузніченко С. О. Державне управління у надзвичайних ситуаціях: проблеми правового забезпечення. *Юридичний вісник*. 2010. № 3. С. 52–56.

130. Кулєшов М. М. Система реагування на надзвичайні ситуації та механізми управління. *Вісник Національного університету цивільного захисту*

України. *Серія: Державне управління*. 2017. Вип. 1 (6). С. 314–322.

131. Лазор О. Д., Лазор О. Я., Лазор Г. І. Основи державного управління та місцевого самоврядування : навч. посіб. Київ : Дакор, 2007. 312 с.

132. Лапін В. Безпека життєдіяльності людини : навч. посіб. Київ : Знання, 2007. 332 с.

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

134. Ліпкан В. А. Національна безпека та національні інтереси України. Київ : КНТ, 2006. 68 с.

135. Ліхачов С. Національна безпека України як об'єкт державного управління. *Право України*. 2009. № 10. С. 182–189.

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

137. Лозинська Т. М. Теоретико-методологічні засади наукових досліджень в галузі державного управління : монографія / За заг. ред. д-ра. філос. наук, проф. В. В. Корженка. Дніпропетровськ : Комплектавтодор, 2011. С. 151–171.

138. Лошенюк В.Є. Багатовекторна зовнішньоекономічна небезпека для України. *Соціально-економічні проблеми України в глобальному просторі*: Матеріали міжнародної науково-практичної конференції. Чернівці : ЧТЕІ КНТЕУ. 2012. С. 53-56.

139. Лошенюк В. Є. Державне регулювання економіки : навч. посіб. Чернівці : Чернівецький регіональний центр перепідготовки та підвищення кваліфікації, 2003. 74 с.

140. Лугунін О. Є. Статистика. Економічна та соціальна статистика :

курс лекцій. Херсон : МУБіП, 2003. 99 с.

141. Луценко М. М. Оцінка обстановки у надзвичайних ситуаціях. Харків : ХНАДУ, 2009. 183 с.

142. Майстро С. В. Теоретичні засади механізму державного управління системою цивільного захисту. *Теорія та практика державного управління*. 2014. Вип. 3. С. 3−10.

143. Макогон Ю. В., Амоша І. О. Майбутнє України: стратегія поступу : монографія. Донецьк : Академія економічних наук України, 2008. 304 с.

144. Малиновський В. Я. Державне управління : навч. посіб. Київ : Атіка, 2003. 576 с.

145. Малеван О. Ю., Переверзін Ю. П. Напрями удосконалення сфери цивільного захисту держави Тищенко. *Державне управління: удосконалення та розвиток*. 2012. № 11. URL: http://www.dy.nayka.com.ua (дата звернення: 14.03.2024).

146. Малиновський В. Я. Державне управління: навч. посіб. Київ : Атіка, 2003. 576 с.

147. Малишева Н. Надзвичайна ситуація. *Юридична наука*. 2002. С. 54–57.

148. Маслов Є. П. Державна політика у сфері цивільного захисту України в умовах надзвичайних ситуацій. URL: www.zerkalov.kiev.ua (дата звернення: 14.03.2024).

149. Медичний та біологічний захист за умов надзвичайних ситуацій : навч. посіб. / М. Д. Близнюк, П. Б. Волянський, М. Т. Гафарова та ін. Харків : ФОП Панов А.М., 2016. 324 с.

150. Мезенцева О. М. Аналіз надзвичайних ситуацій в Україні за характером та наслідками. *Наукові записки*. 2014. Вип. 15. С. 130–133.

151. Мельник О. В. Розуміння категорії «національна безпека» у вітчизняному та зарубіжному правознавстві. *Держава і право. Юридичні і*

політичні науки. 2007. Вип. 38. С. 147–153.

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

153. Мельтюхова Н. М. Технологія державного управління : навч. посіб. / За заг. ред. Г. І. Мостового, О. Ф. Мельникова. Харків : Вид-во ХарРІ НАДУ «Магістр», 2005. 152 с.

154. Методичні рекомендації з питань організації та реалізації заходів цивільного захисту в органах виконавчої влади на підприємствах, в установах і організаціях. Київ : ДСНС України, 2015. URL: http://undicz.dsns.gov.ua/files/2015/8/11/Metod_rekomendaciyi.pdf (дата звернення: 14.03.2024).

155. Мирна Н. В. Опрацювання комплексного механізму державної регіональної політики. Державне будівництво. 2010. № 1. URL: http://nbuv.gov.ua/UJRN/DeBu_2010_1_20 (дата звернення: 14.03.2024).

156. Михайлюк О. В. Цивільний захист : навчальний посібник. Ч.1. Соціальна, техногенна та природна безпека. Миколаїв : НУК, 2005. 136 с.

157. Михасюк І., Мельник А., Крупка М. Державне регулювання економіки. Львів : Українські технології, 1999. 640 с.

158. Могил С. Держава як суб’єкт попередження і ліквідації наслідків аварій і катастроф. *Актуальні проблеми держави та права*. Вип. 6. Ч. ІІ, 2009. С. 107–114.

159. Моделі ефективності державного управління : монографія / В. С. Загорський, М. Д. Лесечко, Р. М. Рудніцька та ін. Львів : ЛРІДУ НАДУ, 2010. 100 с.

160. Моделювання економічної безпеки: держава, регіон, підприємство : монографія / В. М. Геєць, М. О. Кизим, Т. С. Клебанова та ін. Харків : ВД

«ИНЖЕК», 2006. 240 с.

161. Мороз В. М. Розвиток громадянського суспільства: взаємозобов'язання і взаємовідповідальність між основними учасниками соціального діалогу. *Вісник Національного університету цивільного захисту України. Серія: Державне управління*. 2014. Вип. 2. С. 14−22.

162. Мороз О. В., Карачина Н. П., Шиян А. А. Концепція економічної безпеки сучасного підприємства : монографія. Вінниця : ВНТУ, 2011. 241 с.

163. Надолішній П. Організаційно-функціональна структура державного управління: поняття і соціальна практика. *Вісн. НАДУ*. 2003. № 3. С. 31–43.

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

165. 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. Київ : ТОВ «Інтердрук», 2016. 203 с.

166. Нижник Н. Р. До проблеми ефективності державного управління в Україні. *Підвищення ефективності державного управління: стан, перспективи та світовий досвід : зб. наук. пр.* Київ : Вид-во УАДУ, 2000. С. 6–11.

167. Нижник Н. Р., Ситник Г. П., Білоус В. Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку). Ірпінь : Акад. ДПС України, 2000. 304 с.

168. Никифоров А. Є. Інноваційна діяльність: теорія і практика державного управління : монографія. Київ : КНЕУ, 2010. 420 с.

169. Нікітін Ю. В. Теоретико-правовий підхід до визначення загроз як детермінуючих чинників впливу на національну безпеку України. *Держава і право. Юридичні і політичні науки*. 2008. Вип. 41. С. 502–508.

170. Нормативно-правова база у галузі безпеки і оборони України / заг.

ред. : А. Гриценко, А. Єрмолаєв, Ф. Флурі. Київ : Центр дослідж. армії, коверсії та роззброєння, 2012. 800 с.

171. Одінцова Г. С., Мельтюхова Н. М. Теорія і історія державного управління : опорний конспект лекцій і методичні вказівки до проведення практичних занять. Харків : УАДУ, 2001. 136 с.

172. Одокієнко С. М., Тарандушка Л. А., Жирякова І. А. Аналіз виникнення надзвичайних ситуацій техногенного та природного характеру в Україні. *Пожежна безпека: теорія і практика*. 2013. №15. С. 115−123.

173. Олійник А. Ю., Гусарєв С. Д., Слісаренко О. Л. Теорія держави і права : навч. посіб. Київ : Юрінком Інтер, 2001. 176 с.

174. 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. Київ : ІДУЦЗ, 2017. 127 с.

175. Офіційний веб-сайт Державної служби України з надзвичайних ситуацій. URL: http://www.dsns.gov.ua/ua/Vnutrishniy-audit.html (дата звернення: 14.03.2024).

176. Піхняк Т. А. Проблеми механізму державного регулювання економічного зростання. URL: http:// www.nbuv.gov.ua/portal/soc_gum/ Znphktei/2011_1/statti/pixnyak/pixnyak.htm (дата звернення: 14.03.2024).

177. Пал Л. А. Аналіз державної політики. Київ : Основи, 1999. 422 с.

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

179. Полковниченко Д. Державна політика у сфері попередження надзвичайних ситуацій на основі концепції ризиків. *Теорія та практика державного управління*. 2013. № 4. URL: http://www.kbuapa.kharkov.ua/e–book/conf/2013–4/doc/3.pdf (дата звернення: 14.03.2024).

180. Полковниченко Д. Ю. Особливості формування системи державного управління в умовах безпеки та надзвичайних ситуаціях. *Теорія та практика державного управління і місцевого самоврядування*. 2016. № 2. URL: http://nbuv.gov.ua/UJRN/Ttpdu_2016_2_23 (дата звернення: 14.03.2024).

181. Пономаренко Г. О. Управління у сфері забезпечення внутрішньої безпеки держави: адміністративно-правові засади : монографія. Харків : Вид. СПД ФО Вапнярчук Н. М., 2007. 448 с.

182. Пономаренко С. С., Максимов А. В. Науково-теоретичний аналіз впливу НС на соціально-економічний розвиток: загальнодержавний і локально-територіальний рівні. *Вісник Національного університету цивільного захисту України. Серія. Державне управління*. 2017. Вип. 1 (6). С. 322–328.

183. Порфілов О. Підходи до розроблення та прийняття управлінських рішень в умовах невизначеності та ризику. *Вісник Нац. ун-ту «Львівська. політехніка». Серія: Юридичні науки.* 2016. № 855. – С. 218–224.

184. Порядочний Л. В., Заплатинський В. М. Безпека в надзвичайних ситуаціях та цивільна оборона : навч. посіб. Київ : Київ. нац. торгов.-екон. ун-т, 2003. 301 с.

185. 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. Київ : ІДУЦЗ, 2016. 64 с.

186. Приходченко Л. Л. Забезпечення ефективності державного управління: теоретико-методологічні засади : монографія. Одеса : Вид-во Оптимум, 2009. 299 с.

187. Природні та техногенні загрози, оцінювання небезпек : навч. посіб. / В. А. Андронов, А. С. Рогозін, О. М. Соболь та ін. Харків : Вид-во НУЦЗУ, 2011. 264 с.

188. Приходченко Л. Л. Забезпечення ефективності державного управління на засадах демократичного врядування : автореф. дис. ... д-ра наук з держ. упр. : 25.00.02. Запоріжжя, 2010. 36 с.

189. Приходько В. М. Потенційно небезпечні об’єкти – як фактор дестабілізації. *Системи обробки інформації*. 2014. № 7. С.45–47.

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

191. Про заходи щодо реконструкції та модернізації теплоелектростанцій у період до 2010 року : розпорядження Кабінету Міністрів України від 08.09.2004 р. № 648-р. URL: https://www.kmu.gov.ua/npas/8475876 (дата звернення: 14.03.2024).

192. Про організаційні заходи з підготовки обладнання електростанцій, теплових та електричних мереж до стабільної роботи в осінньо-зимовий період : розпорядження Кабінету Міністрів України від 02.07.2012 р. № 418-р. URL: https://zakon.rada.gov.ua/laws/show/418-2012-%D1%80#Text (дата звернення: 14.03.2024).

193. Про поводження з відпрацьованим ядерним паливом щодо розміщення, проектування та будівництва централізованого сховища відпрацьованого ядерного палива реакторів типу ВВЕР вітчизняних атомних електростанцій : Закон України від 09.02.2012 р. № 4384-VI. *Відомості Верховної Ради України*. 2012. № 40. Ст. 476.

194. Про поводження з радіоактивними відходами : Закон України від 30.06.1995 р. № 255. *Відомості Верховної Ради України*. 1995. № 27. Ст. 198.

195. Про порядок прийняття рішень про розміщення, проектування, будівництво ядерних установок і об’єктів, призначених для поводження з радіоактивними відходами, які мають загальнодержавне значення : Закон

України від 08.09.2005 р. № 2861-IV. *Відомості Верховної Ради України*. 2005. № 51. Ст. 555.

196. Проневич О. С. Державне управління у надзвичайних ситуаціях: концептуально-правовий базис та інституційна надбудова. *Форум права*. 2015. № 5. С. 186–193.

197. Публічне адміністрування в Україні : навч. посіб. / В. Б. Дзюндзюк, О. Б. Коротич, Н. М. Мельтюхова та ін. Харків : Вид-во ХарРІ НАДУ «Магістр», 2012. 256 с.

198. Радиш Я. Ф., Терентьєва А. В. Досвід взаємодії міжнародних цивільно-військових сил при ліквідації наслідків надзвичайних ситуацій. *Держава та регіони*. 2009. № 2. С. 157–160.

199. Райт Г. Державне управління. Київ : Основи, 1994. 432 с.

200. Романюк О. Д. Методи економіко-статистичного аналізу : навч. посіб. Київ : УАДУ, 1997. 144 с.

201. Ромін А., Приходько Р. Методологічні засади державного управління сферою захисту населення і територій від надзвичайних ситуацій. *Публічне управління: теорія та практика : зб. наук. пр.* Харків : Вид-во ДокНаукДержУпр., 2013. № 4. С. 41–47.

202. Рудніцька Р. М., Сидорчук О. Г., Стельмах О. М. Механізми державного управління: сутність і зміст / за наук. ред. д.е.н., проф. М. Д. Лесечка, к.е.н., доц. А. О. Чемериса. Львів : ЛРІДУ НАДУ, 2005. 28 с.

203. Русецький А. А. Аналіз стану загроз критичній інфраструктурі в Харківській області. *Актуальні проблеми вітчизняної юриспуденції*. 2017. № 1. Т. 2. С. 18–20.

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

205. Садковий В. П., Ромін А. В., Островерх О. О., Домбровська С. М.

Державне управління у сфері цивільного захисту в Україні: нормативно-правовий аспект : монографія. Харків : ТОВ «Оберіг», 2013. 190 с.

206. Саліхова О. Б. Високотехнологічні виробництва: від методології оцінки до піднесення в Україні : монографія. Київ : Ін-т екон. та прогнозув., 2012. 624 с.

207. Сапа Н. В. Теоретико-методологічні засади механізму антикризового державного управління. *Гуманітарний вісник ЗДІА*. 2009. Вип. 38. С. 106–116.

208. Семенченко А. І. Механізм стратегічного управління забезпеченням національної безпеки у кризових та надзвичайних ситуаціях. URL: http://old.niss.gov. ua/book/StrPryor/2/6-3-Semenchenko.pdf (дата звернення: 14.03.2024).

209. Ситник Г. П. Безпека як категорія і функція державного управління. *Вісн. Нац. академії держ. управління*. 2004. № 1. С. 350–357.

210. Ситник Г. П. Олуйко В. М., Вавринчук М. П. Національна безпека України: теорія і практика. Київ : Кондор, 2007. 616 с.

211. Скрипник О. А. Сучасні тенденції формування системи державного управління у сфері цивільного захисту населення від надзвичайних ситуацій в Україні. *Державне управління та місцеве самоврядування*. 2015. № 2 (14). URL: http://www.dridu.dp.ua/zbirnik/2015-02(14)/14.pdf (дата звернення: 14.03.2024).

212. Служба безпеки України (офіційний сайт). URL: https://www.ssu.gov.ua/ (дата звернення: 14.03.2024).

213. Смірнова О. Виробничий ризик: сутність і управління. *Управління ризиком*. 2001. № 2. С. 20–23.

214. Соболь О. М., Приходько Р. В. Організаційно-правовий механізм державного управління у сфері захисту населення і територій від надзвичайних ситуацій. URL: http://www.kbuapa.kharkov.ua/e-book/db/20122/doc/2/13.pdf (дата звернення: 14.03.2024).

215. 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.

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

217. Старостіна А. О., Кравченко В. А. Ризик-менеджмент: теорія та практика : навч. посіб. Київ : Видавництво «Політехніка», 2004. 200 с.

218. Стеблюк М. І. Цивільна оборона та цивільний захист : підручник. Київ : Знання, 2010. 487 с.

219. Стеченко Д. М. Державне регулювання економіки : навч. посіб. Київ : Знання, 2006. 262 с.

220. Стратегія і тактика національної безпеки: зарубіжний досвід, проблеми та перспективи України / за заг. ред. В. П. Горбуліна. Київ : Нац. центр з питань євроатлант. інтеграції, 2006. 304 с.

221. Стрельцов В. Ю. Розвиток публічної служби України в умовах біпатризму. *Теорія та практика державного управління. Збірник наукових праць*. Харків: Вид-во ХарРІ НАДУ “Магістр”, 2010. Вип. 4 (31). С. 394−398.

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

223. Суходоля О. М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. *Стратегічні пріоритети*. 2016. № 3(40). С. 62–76.

224. 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. Київ : НАДУ,

2009. 56 с.

225. 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.

226. 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. Київ : Юрінком Інтер, 2002. 368 с.

227. Теорія держави і права. Академічний курс : підруч. / ред. О. В. Зайчук, Н. М. Оніщенко. – Київ : ЮрІнтер, 2006. 688 с.

228. Титаренко А. В. Методологічні засади державного управління сферою захисту населення і територій від надзвичайних ситуацій. *Вісник Національного університету цивільного захисту України*. *Серія : Серія. Державне управління.* 2016. Вип. 1 (4). С. 216–222.

229. Труш О. О. Досвід побудови та функціонування систем цивільного захисту країн-членів європейського союзу Південної Європи. *Теорія та практика державного управління*. 2010. № 1. С. 112–123.

230. Україна: 30 років на європейському шляху / Ю. Якименко [та ін.] ; Український центр економічних і політичних досліджень імені Олександра Разумкова. Київ : Заповіт, 2021. 392 с.

231. Український соціум: загрози екстремальних ситуацій : монографія / Г. В. Рева, В. К. Врублевський, В. П. Ксьонзенко ; за ред. В. К. Врублевського. Київ : Інтелект, 2003. 432 с.

232. Усаченко Л. М., Тимцуник В. І. Історія державного управління в Україні : навч. посіб. Київ : ТОВ «НВП «Інтерсервіс», 2013. 292 с.

233. Федорчак О. В. Класифікація механізмів державного управління. *Демократичне врядування*. 2008. Вип. 1. URL: http://www.academy.lviv.ua (дата звернення: 14.03.2024).

234. Фещур Р. В., Барвінський А. Ф. Статистика: теоретичні засади і прикладні аспекти : навч. посіб. Львів : Інтелект-Захід, 2003. 576 с.

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

236. Харламов В. В. Теоретичні засади державного управління вищою освітою у сфері цивільного захисту. *Вісник Національного університету цивільного захисту України. Серія. Державне управління*. 2017. Вип. 1 (6). С. 69–75.

237. Харченко Н. П. Поняття механізму держави, наукові пошуки теоретико-правової дефініції. *Вчені записки Таврійського національного університета імені В. І. Вернадського*. 2007. Т. 20(59). № 2. С. 278–284. (Серія «Юридичні науки»).

238. Харчук А. І. Сукач Р. Ю., Колісник М. Я. Організація управління у надзвичайних ситуаціях. URL: http://ubgd.lviv.ua (дата звернення: 14.03.2024).

239. Цвєтков В. В. Державне управління: основні фактори ефективності (політико-правовий аспект). Харків : Право, 1996. 164 с.

240. Чечель А. О. Передумови удосконалення економічного механізму природокористування в Україні. *Збірник наукових праць Донецького державного університету управління. Серія «Економіка»*. Том XI. Випуск 149 «Управління економічним розвитком промислових підприємств». 2010. С.80−87.

241. Чечель О. М. Принципи та механізм державного регулювання економіки. *Вісник Академії митної служби України*. 2013. № 2. С. 103–111. (Серія «Державне управління»).

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

243. Шахов В., Мадіссон В. Національний інтерес і національна безпека

в геостратегії України. Вісник Національної академії державного управління при Президентові України. 2013. № 2. С. 44–56.

244. Швайка Л. А. Державне регулювання економіки : підручник. Київ : Знання, 2008. 462 с.

245. Шевцов А., Їжак. Реформування системи цивільного захисту населення відповідно до завдань європейської та євроатлантичної інтеграції. URL: http://www.niss.gov.ua/Monitor/mart2009/3.htm (дата звернення: 14.03.2024).

246. Шлемко В. Т., Бінько І. Ф. Економічна безпека України: сутність і напрямки забезпечення : монографія. Київ : НІСД, 1997. 144 с.

247. Шоботов В. М. Цивільна оборона : навчальний посібник. Київ : Центр навчальної літератури, 2006. 438 с.

248. Штимер Л. Т. Облікова система установ державного сектору економіки: проблеми та перспективи розвитку. *Економічний форум*. 2015. № 1. С. 276–282.

249. Юхновський І. В. Державне регулювання інноваційно-інвестиційної діяльності економіки України. *Економіка та держава*. 2011. № 4. С. 48–52.

250. Якимчук А. Ю., Корецький О. М. Публічне адміністрування : навч. пособ. Донецьк : Юго-Восток, 2014. 224 с.

251. International Telecommunication Union. URL: https://www.itu.int/ru/Pages/default.aspx (дата звернення: 14.03.2024).