МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІННИЦЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ
МИХАЙЛА КОЦЮБИНСЬКОГО

ЯРЕМЕНКО О.І., СТРАХНІЦЬКИЙ Я.О., ЗУБАР І.В., НАМАЗОВА Ю.І.

МЕНЕДЖМЕНТ ПІДПРИЄМСТВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ СУЧАСНИХ БЕЗПЕКОВИХ ВИКЛИКІВ

Монографія

ВІННИЦЯ – 2025

УДК 351.862.2: [351.778+351.824.11] (477) (043.5)

DOI: https://doi.org/10.31652/351.862.2-1-236

Яременко О.І., Страхніцький Я.О, Зубар І.В., Намазова Ю.І. Менеджмент підприємств критичної інфраструктури в умовах сучасних безпекових викликів. Вінниця: ТОВ «Видавництво-друкарня Діло», 2025. – 236 с.

Авторський колектив:

ЯРЕМЕНКО Олександр Іванович – кандидат наук з державного управління, доцент, доцент кафедри публічного управління та менеджменту, декан факультету права, публічного управління і менеджменту ВДПУ імені Михайла Коцюбинського

СТРАХНІЦЬКИЙ Ярослав Олександрович – доктор філософії з публічного управління та адміністрування, співробітник УСБУ у Вінницькій області

ЗУБАР Іван Валерійович – кандидат економічних наук, старший викладач кафедри публічного управління та менеджменту ВДПУ імені Михайла Коцюбинського

НАМАЗОВА Юлія Ісмаілівна – доктор філософії з публічного управління та адміністрування, старший викладач кафедри публічного управління та менеджменту ВДПУ імені Михайла Коцюбинського

Рецензенти:

Довгань В. І. доктор наук з державного управління, професор, провідний науковий співробітник науково-дослідного відділу Національної академії Державної прикордонної служби України імені Богдана Хмельницького, Заслужений діяч науки і техніки України

Захарченко В. І. доктор економічних наук, професор, професор кафедри адміністративного менеджменту та альтернативних джерел енергії Вінницького національного аграрного університету

Климчук О. В. доктор економічних наук, професор, професор кафедри публічного управління та менеджменту Вінницького державного педагогічного університету імені Михайла Коцюбинського

Монографія присвячена дослідженню проблем менеджменту підприємств критичної інфраструктури та державної політики їх захисту в умовах гібридних загроз. Проаналізовано наукові підходи до визначення критичної інфраструктури та менеджменту критично-важливих підприємств крізь призму забезпечення національної безпеки та сталого розвитку. Розглянуто інституційно-правове регулювання та оцінено спроможність національної системи захисту об’єктів критичної інфраструктури, включаючи організаційні, технічні та кадрові аспекти. Проведено аналіз ефективності чинної державної політики в умовах воєнного стану та досліджено зарубіжний досвід, зокрема у контексті нової Директиви ЄС 255. Запропоновано напрями інституційних змін для підвищення ефективності системи захисту критичної інфраструктури.

Рекомендовано вченою радою Вінницького державного педагогічного університету імені Михайла Коцюбинського (Протокол № 12 від 25 червня 2025 р.).

ЗМІСТ

ВСТУП

Сучасний розвиток світового суспільства базується на функціонуванні найважливіших секторів забезпечення життєдіяльності країн. Формування новітньої безпекової парадигми вимагає не лише удосконалення усталених концептуальних засад забезпечення захисту критично важливих об'єктів інфраструктури, а й переосмислення концепцій менеджменту відповідно сучасним реаліям впливу гібридних загроз, оскільки розлагодженість у роботі будь-якого із цих секторів загрожує суспільству глобальним дисбалансом та навіть руйнуваннями. Варто також відзначити, що разом із розвитком цивілізації сучасний світ постав перед обличчям безпрецедентних викликів, які радикально змінюють уявлення про безпеку та стабільність. Глобалізація, стрімкий технологічний прогрес, асиметричні загрози, такі як кібератаки, тероризм, гібридні конфлікти, а також наслідки зміни клімату та пандемій, створюють комплексне поле ризиків для функціонування будь-якої держави та суспільства. В епіцентрі цих викликів опиняються підприємства критичної інфраструктури – основи життєдіяльності країни, що забезпечують її функціонування в усіх сферах: від енергетики та транспорту до фінансової системи та охорони здоров'я. Безперебійна та надійна робота цих об'єктів є запорукою національної безпеки, економічної стабільності та соціального добробуту.

З огляду на ці факти та нинішню ситуацію військового вторгнення в Україні, питання безпеки та захисту об'єктів критичної інфраструктури, а також ефективної системи менеджменту стають все більш актуальними. По-перше, наслідки стихійних лих, аварій, катастроф та інших надзвичайних ситуацій набувають все більш масштабних і небезпечних наслідків для суспільства та стабільності функціонування економіки. По-друге, кризові явища, з якими стикнулося наше суспільство у період військової агресії, продемонструвало значимість об'єктів критичної інфраструктури та необхідність кардинальної зміни системи її захисту, що обумовлює потребу в удосконаленні системи менеджменту таких підприємств. По-третє, питання забезпечення організаційної структури, адміністративних функцій, напрямів розвитку та основ функціонування системи захисту критичної інфраструктури детермінує необхідність чіткої детекції місця та ролі держави. Це, у свою чергу, актуалізує необхідність вирішення проблем у модернізації державної безпекової політики у сфері забезпечення захисту критичних об'єктів в умовах воєнного стану в Україні.

Аналіз сучасних наукових доробків, засвідчив посилену увагу дослідників до питань захисту критичної інфраструктури, особливо удосконалення державної політики в умовах зростання військових загроз. Значний внесок у дослідження зазначеного вектора проблем зробили такі науковці, як: О. Я. Лазор, О. Д. Лазор, С. І. Азаров, В. Л. Сидоренко, С. А. Єременко, А. В. Пруський, О. П. Єрменчук, Г. Ю. Зубко, С. І. Кондратов, О. М. Суходоля, А.В. Заболотний, І. Г. Юник,

О. П. Єрменчук, М. Б. Домарацький, Д. С. Бірюков, С. В. Бєлай та інші. Аналізу наукових джерел із проблематики державного управління у сфері національної безпеки, у тому числі менеджменту підприємств критичної інфраструктури присвячено вагомий теоретичний доробок як українських, так і зарубіжних учених таких як: М. Ф. Криштанович, Я. Я. Пушак, М. І. Флейчук, В. І. Франчук, С. І. Крук, В. А. Ліпкан, Д. Г. Бобро, С. П. Іванюта, С. І. Кондратов, О. М. Суходоля, Д. М. Павлов, М. А. Микитюк та ін.

Водночас, недостатньо вивченими залишаються окремі аспекти специфіки державної політики у сфері захисту критичної інфраструктури, складової її теоретичного обґрунтування та практичних дієвих напрямів менеджменту на критично важливих підприємствах в умовах правового режиму воєнного стану. Сукупність сучасних безпекових викликів зумовлює потребу у глибокому аналізі понятійно-категоріального апарату, осмисленні еволюційного розвитку систем захисту критичної інфраструктури, а також у вивченні кращих практик, напрацьованих у провідних країнах Європи. Особливу увагу слід приділити структурним елементам, що формують основу ефективного менеджменту підприємств критичної інфраструктури в українському контексті. Це зумовлює актуальність наукового дослідження, викладено у тексті монографії.

Монографія присвячена дослідженню теоретичних та прикладних аспектів менеджменту та державного управління у сфері критичної інфраструктури в контексті сучасних безпекових викликів. Проведені дослідження мали на меті систематизувати ключові проблеми, що стоять перед суб’єктами критичної інфраструктури та запропонувати дієві механізми та інструменти для підвищення їхньої стійкості, адаптивності та здатності ефективно протистояти різноманітним загрозам. Особлива увага приділяється аналізу передового міжнародного досвіду та розробці рекомендацій щодо формування ефективної системи управління ризиками, впровадження сучасних технологій захисту, розвитку партнерства між державою та приватним сектором, а також підготовки висококваліфікованих кадрів. Дана праця має на меті стати цінним джерелом знань для науковців, практиків, державних службовців, які залучені до процесу забезпечення національної безпеки та управління критичною інфраструктурою, а також для широкого кола читачів, зацікавлених у розумінні складних викликів сучасності та шляхів їх подолання.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДИЧНІ ЗАСАДИ ФОРМУВАННЯ МЕНЕДЖМЕНТУ ПІДПРИЄМСТВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЇХ ЗАХИСТУ

1.1. Теоретичні підходи до формування системи менеджменту на підприємствах критичної інфраструктури

Події, що відбуваються в Україні, зокрема у сфері національної безпеки, зумовлюють нагальну потребу в радикальній трансформації системи соціально-економічних та управлінських відносин. У цьому контексті особливого значення набуває питання формування ефективної системи менеджменту на підприємствах критичної інфраструктури як ключового елемента забезпечення стабільного функціонування суспільства. Актуальність дослідження обумовлена необхідністю розробки оптимальної моделі управління, яка відповідатиме сучасним викликам та зрушенням у безпековій парадигмі. У зв'язку з цим доцільним є зосередження на вивченні особливостей становлення і розвитку теорії управління, а також здійснення наукового аналізу сучасних концепцій менеджменту, що враховують специфіку функціонування об'єктів критичної інфраструктури в умовах загроз національній безпеці.

Як зазначає Синиченко А. В., будь-яке підприємство, незалежно від форми власності чи організаційно-правового статусу, потребує ефективної моделі управління. Учений розглядає менеджмент як продуктивну силу, здатну інтегрувати всі наявні ресурсні компоненти з метою приведення їх у скоординований, поступальний рух сталого розвитку [235]. Система менеджменту, таким чином, є не лише управлінським механізмом, а й об'єктивною необхідністю, що детермінована характером суспільного виробництва та організації діяльності людей і для підприємств критичної інфраструктури .

Будь-яка модель менеджменту ґрунтується на певній концепції, яка виступає теоретичною основою її формування та реалізації. Концепція менеджменту – це цілісна система ідей, принципів та уявлень, що визначають мету функціонування організації, механізми взаємодії між суб'єктом і об'єктом управління, а також характер внутрішньої структури управлінських відносин. До ключових елементів концепції менеджменту учені відносять визначення взаємозв'язків між окремими структурними ланками підприємства, розробка ефективних механізмів координації їх діяльності, а також урахування впливу зовнішнього середовища на розвиток організації. У контексті функціонування об'єктів критичної інфраструктури, це особливо важливо, оскільки їх стійкість значною мірою залежить від здатності менеджменту оперативно адаптуватися до змін у безпековому середовищі [89].

Найбільш відомим прикладом первинної систематизації управлінських

підходів є класифікація, представлена в класичному підручнику американських науковців М. Х. Мескона, М. Альберта та Ф. Хедоурі «Основи менеджменту» [359]. У межах аналізу еволюції менеджменту як наукової дисципліни автори виокремили чотири основні підходи до управління: підхід на основі класифікації управлінських шкіл, процесний підхід, системний підхід та ситуаційний підхід. З огляду на сучасні реалії, ідеї, висунуті представниками провідних управлінських шкіл XX століття, вже не сприймаються як інноваційні або універсальні моделі для побудови ефективних систем менеджменту. Проте їхні ключові положення продовжують знаходити відображення в сучасних теоретичних концепціях і практиці управління, зокрема в умовах функціонування об'єктів критичної інфраструктури.

Роль ранніх теорій менеджменту полягає в тому, що вони заклали підвалини для формування наукових принципів сучасного управління та окреслили стратегічні вектори його подальшого розвитку. Системний, ситуаційний та процесний підходи, які й нині активно використовуються у сфері менеджменту, вважаються інтегрованими. Вони спрямовані на подолання обмеженості часткових концепцій шляхом їхнього синтезу в єдину цілісну парадигму управління, що є особливо актуальним для управління підприємствами критичної інфраструктури [283].

Що стосується реалізації системного підходу в менеджменті, то він передбачає насамперед аналіз підприємств (організацій) як складних відкритих систем, що функціонують як сукупність взаємопов'язаних і взаємодіючих елементів – людей, завдань, структури, технологій. Ці елементи зорієнтовані на досягнення різних цілей в умовах динамічного зовнішнього середовища. Саме системний підхід забезпечив концептуальну основу для подальших досліджень взаємодії організації із зовнішнім середовищем і став відправною точкою для розвитку численних теорій стратегічного та адаптивного управління.

Ситуаційний підхід, у свою чергу, стверджує, що не існує єдиних, універсальних методів ефективного управління. Ефективність управлінських рішень залежить від конкретної ситуації, що потребує попереднього аналізу впливових факторів. Таким чином, обґрунтований вибір управлінських інструментів можливий лише за умови комплексної оцінки контексту, в якому функціонує організація. Менеджмент як здатність досягати поставлених цілей шляхом використання інтелектуального потенціалу й мотиваційної поведінки інших людей, може набувати як оперативного, так і стратегічного характеру. Водночас методи оперативного й стратегічного управління перебувають у взаємозв'язку та взаємозалежності.

Підхід до управління як до процесу передбачає розгляд менеджменту у якості безперервного циклу, що складається із взаємопов'язаних дій – управлінських функцій. До основних функцій менеджменту, згідно з класичними теоріями, належать: планування, організація, мотивація, керівництво, координація, контроль, комунікації, дослідження, оцінювання,

прийняття рішень, а також підбір і розстановка персоналу. Такий підхід дозволяє створити гнучку та адаптивну систему управління, здатну ефективно реагувати на виклики зовнішнього середовища, що особливо актуально для об'єктів критичної інфраструктури.

Джерелами наукових засад менеджменту як теорії ринкового управління є праці видатних дослідників і практиків. Одним із найвпливовіших мислителів у цій сфері був Пітер Ф. Друкер. Його теоретичний внесок глибоко відображає природу сучасного менеджменту:

1. «Менеджмент існує задля результатів, яких установа досягає у зовнішньому середовищі. Менеджмент має визначити, яких результатів необхідно досягнути; менеджмент повинен мобілізувати ресурси організації для досягнення цих результатів» [360, с. 64].

2. «До сфери уваги і відповідальності менеджменту входить все, що якимось чином впливає на продуктивність організації і результативність її діяльності – всередині організації чи за її межами, у підконтрольних організації сферах або у сферах, що нею не контролюються» [360, с. 65].

3. «Кожна організація діє, виходячи зі своєї теорії бізнесу, іншими словами, на підставі ряду уявлень про те, у чому полягає її бізнес, якими є її цілі, як визначаються результати, хто є її споживачами, що ці споживачі цінують і за що сплачують» [360, с. 73].

Соціально-економічні трансформації господарського механізму сприяють появі нових форм і методів ведення господарської діяльності у сфері критичної інфраструктури, що, у свою чергу, зумовлює нові вимоги до систем менеджменту таких підприємств. Ці вимоги набувають особливого значення в умовах інтенсивного розвитку всіх секторів національної економіки та формування ефективного ресурсного потенціалу в межах стратегії сталого розвитку [235].

Зменшення впливу непередбачуваних факторів та підвищення рівня прогнозування загальної стратегії підприємства на сьогодні залишається складним завданням, що перебуває у межах компетенції лише обмеженої кількості менеджерів. Однією з ключових передумов вирішення цього завдання є глибока трансформація управлінського мислення. Менеджери мають усвідомити, що впровадження сучасного менеджменту – це не просто заміна термінології, а якісна зміна управлінських підходів. Основна концептуальна зміна полягає у переході від методів адміністративного примусу до методів мотивації працівників, що ґрунтуються на активному використанні їхнього інтелектуального і творчого потенціалу.

Враховуючи специфіку управлінської діяльності, ефективність впровадження системи менеджменту має оцінюватися не лише за економічними показниками, але й за соціально-психологічними критеріями. До останніх належать здатність організації адаптуватися до змін, рівень задоволення потреб персоналу, ефективність використання їх мотиваційного ресурсу, а також здатність керівників формувати сприятливе соціальне середовище в колективі. У цьому контексті продуктивність управління

підприємством визначається не лише кількісними та якісними показниками ефективності, а й адаптивними можливостями управлінської системи. Ці можливості залежать від готовності менеджерів реалізовувати прийняті рішення, а також від обґрунтованості та точності самих управлінських рішень. Адже саме від них значною мірою залежить результативність діяльності підприємства в цілому та, як наслідок, рівень матеріального та професійного добробуту самих менеджерів [284, с. 155]. Однією з ключових причин неефективного управління на підприємствах у сучасних умовах є нездатність менеджерів швидко адаптуватися до кардинальних змін, що відбуваються в економіці держави. Така інерційність управлінського мислення часто зумовлює розгубленість керівників, призводячи до хаотичного, стихійного прийняття рішень, а отже – до нестабільності організаційних процесів, що неприпустимо для підприємств критичної інфраструктури.

Методологічною основою ефективного менеджменту є принципи його впровадження. Результати досліджень засвідчують, що для оптимізації управлінських процесів доцільно керуватися такими базовими принципами менеджменту:

– Принцип орієнтації на мету: організаційну структуру підприємства слід будувати не під можливості персоналу, а як інструмент досягнення чітко визначених цілей, підбираючи для цього кваліфікованих виконавців;

– Принцип єдиноначальності: кожен працівник повинен підпорядковуватися лише одному безпосередньому керівнику і отримувати завдання виключно від нього;

– Принцип спеціалізації: регулярні функції слід чітко розподіляти між співробітниками управлінського апарату, уникаючи дублювання зусиль;

– Принцип делегування повноважень: керівник має уникати виконання завдань, які можуть бути ефективно реалізовані підлеглими.

Управління командою ускладнюється потребою забезпечення балансу між раціональними стратегіями і емоційним резонансом із працівниками. Сучасні працівники цінують менеджерів, які розглядають їх не лише як ресурс, а як особистостей із власними потребами, що включає повагу до балансу між роботою та особистим життям – суттєве відхилення від класичних концепцій управління минулого.

Варто відзначити, що менеджмент – як наука і мистецтво перебуває у постійній еволюції. Сучасні організації часто інтегрують елементи кількох теоретичних підходів для досягнення максимальної ефективності. Хоча більшість сучасних систем управління є гібридними, фундаментальні теорії менеджменту залишаються основою формування управлінських практик:

– Класична теорія управління базується на задоволенні фізичних і економічних потреб працівника. Її ключовими принципами є спеціалізація праці, централізоване керівництво і максимізація прибутку.

– Теорія поведінкового менеджменту (рух за людські стосунки) акцентує увагу на розумінні людської поведінки в робочому середовищі.

Вона враховує мотиваційні чинники, зокрема вирішення конфліктів, очікування працівників та динаміку групової взаємодії.

– Сучасна теорія менеджменту передбачає застосування математичних і системних методів, таких як кількісний підхід, системний підхід та підхід на випадок непередбачених ситуацій, з метою аналізу взаємодії між менеджерами та працівниками.

Застосування зазначених підходів у сфері управління об'єктами критичної інфраструктури дозволить сформувати адаптивні, надійні системи менеджменту, здатні ефективно функціонувати в умовах постійних викликів та загроз національного і глобального рівня.

Як відомо, причиною будь-яких управлінських дій, особливо у сфері критичної інфраструктури, є необхідність усунення небажаних відхилень від запланованих значень ключових показників діяльності. Подібні відхилення, як правило, виникають під впливом внутрішніх або зовнішніх загроз, які порушують стабільність функціонування підприємства та ставлять під загрозу його безпеку. У цьому контексті доречним є дослідження професора В. І. Франчука, де він визначає безпекову діяльність як сукупність дій підприємства, спрямованих на протидію загрозам, захист корпоративних інтересів і впровадження ефективних управлінських технологій. Зокрема, йдеться про використання таких інструментів, як: контролінг, аутсорсинг, бюджетування, реінжиніринг бізнес-процесів, збалансована система показників, система управління якістю, маркетингові технології, технології залучення та утримання клієнтів, технології управління персоналом, моніторинг зовнішнього та внутрішнього середовища, корпоративна культура, логістика [272].

У науковій праці [7] безпекову діяльність визначено як «збереження цілісності процесів чи систем на основі засвоєння та розвитку безпекової культури». Водночас, доцільним видається подання розширеного формулювання, яке враховує управлінсько-технологічний підхід:

Безпекова діяльність – це діяльність щодо забезпечення максимально ефективного використання наявних ресурсів з метою захисту власних інтересів підприємства від деструктивного впливу внутрішніх і зовнішніх загроз, а також адаптації до мінливих умов функціонування з мінімальними втратами. Таке тлумачення дозволяє осмислити безпекову діяльність не лише як реакцію на загрози, а як активний управлінський процес, що є органічною частиною загальної системи менеджменту.

Узагальнюючи вищезазначене, а також позиції науковців [118], до системи менеджменту у сфері безпекової діяльності та забезпечення стабільності підприємств критичної інфраструктури можемо включити такі складові:

– здатність стратегічно планувати розвиток підприємства, формулювати цілі, визначати конкретні завдання та знаходити способи їх реалізації;

– уміння організовувати й згуртовувати трудовий колектив;

– здійснення контролю за виконанням завдань шляхом надання

повноважень, делегування обов'язків, мотивації чи санкцій за результати праці;

– постійний моніторинг ринку, прогнозування тенденцій і швидке прийняття рішень з урахуванням принципів ефективності (мінімальні витрати – максимальний результат);

– здатність раціонально розподіляти ресурси, визначаючи пріоритетність людського й матеріального потенціалу.

Ці складові формують функціональну основу менеджменту, яка має бути адаптована до умов високої загрозовості та нестабільності середовища, особливо у випадку підприємств критичної інфраструктури. Універсальні завдання менеджменту, зокрема на підприємствах критичної інфраструктури наведемо на рис. 1.1.

Прийняття стратегічних і тактичних управлінських рішень, спрямованих на збереження, розвиток і підвищення конкурентоспроможності підприємства в умовах зовнішніх і внутрішніх загроз.

Формування позитивного іміджу підприємства на ринку як надійного партнера, здатного забезпечувати стабільність, інноваційність та дотримання зобов'язань.

Прагнення до лідерства у галузі через освоєння нових напрямів діяльності, впровадження інновацій та розвиток стратегічних переваг.

Пошук альтернативних шляхів розвитку організації, адаптація до змін зовнішнього середовища та оперативне реагування на виклики.

Систематична робота з персоналом, що включає стимулювання працівників до високопродуктивної праці шляхом морального та матеріального заохочення, створення сприятливого психологічного клімату.

Постійний моніторинг і аналіз потреб підприємства, організація безперебійного постачання ресурсами, що необхідні для ефективної господарської діяльності.

Забезпечення досягнення запланованого рівня прибутковості, утримання досягнутих позицій та впровадження заходів для подальшого покращення економічних результатів.

Управління ризиками, що включає ідентифікацію потенційних загроз, розробку механізмів їх нейтралізації, а також подолання кризових ситуацій без нанесення шкоди ані підприємству, ані його працівникам.

Рис. 1.1. Основні завдання менеджменту на підприємствах критичної інфраструктури

Джерело: узагальнено на основі [359; 360]

Вітчизняні та зарубіжні вчені відзначають, що на сучасному етапі розвитку теорії і практики управління пріоритетними напрямами еволюції менеджменту є:

– інтеграція ситуаційного та стратегічного підходів в управлінській

діяльності організацій;

– прагнення до оптимального розподілу всіх видів ресурсів (матеріальних, фінансових, трудових, інформаційних) за всіма напрямами функціонування організацій;

– постійне уточнення і корегування цілей організацій як реакція на динамічні зміни у зовнішньому і внутрішньому середовищах;

– підвищення рівня професійної підготовки менеджерів, з урахуванням потреб адаптивного, кризового та інноваційного управління;

– формування культури безперервного професійного розвитку працівників усіх рівнів;

– активне впровадження глобальних інформаційно-комунікаційних мереж і технологічних інновацій у практику управління;

– поступове залучення найманих працівників до процесів прийняття управлінських рішень, розвиток моделей партисипативного управління.

У сучасних теоріях менеджменту організації розглядаються як відкриті системи, які функціонують у постійному взаємозв'язку з оточенням. Внутрішні елементи таких систем перебувають не лише у взаємодії між собою, а й під впливом зовнішнього середовища – економічного, соціального, правового, технологічного та політичного.

Структурно організація поділяється на дві ключові підсистеми: керуючу та керовану, які спільно формують цілісну систему менеджменту.

– Керуюча підсистема (суб'єкт управління) представлена менеджером або апаратом управління, що здійснює цілеспрямований вплив на об'єкт управління.

– Керована підсистема (об'єкт управління) охоплює предмети, процеси або соціальні структури, на які спрямовано управлінські дії: робочі місця, виробничі підрозділи (бригади, відділи, цехи), технологічні процеси та трудові колективи.

Зрозуміння організації як відкритої динамічної системи є ключовим для ефективного управління в умовах невизначеності, особливо на підприємствах критичної інфраструктури, де необхідне гнучке реагування на загрози та адаптація до змін середовища [30]. У процесі функціонування організації формується ефект синергії, який проявляється у зростанні сукупної ефективності управлінської діяльності внаслідок інтеграції, поєднання та взаємодії керуючої та керованої підсистем. Завдяки цьому ефекту загальний результат перевищує суму індивідуальних показників ефективності кожної окремої складової системи, якщо вона діяла б ізольовано.

Синергетичний ефект є особливо важливим у контексті функціонування підприємств критичної інфраструктури, де управлінська взаємодія повинна забезпечувати не тільки ефективність, але й стабільність та адаптивність до ризиків. Завдяки синергії досягається узгодженість між стратегічними цілями та поточними процесами, що підвищує загальну стійкість організації до змін зовнішнього середовища.

Незалежно від галузевої специфіки, всі підприємства мають низку

загальних характерних особливостей, серед яких [89]:

– визначення місії та стратегічних цілей діяльності підприємства;

– залежність від зовнішнього середовища, яке впливає на всі ключові процеси;

– наявність ресурсної бази, що включає людські ресурси, матеріали, капітал, технології та інформацію;

– горизонтальний поділ праці, який передбачає чітке визначення завдань та функцій, що зумовлює утворення структурних підрозділів і функціональних служб;

– вертикальний поділ праці, спрямований на координацію діяльності підрозділів і забезпечення ефективного управлінського процесу;

– формування формальних і неформальних груп у внутрішній структурі організації;

– наявність системи управління, що забезпечує цілеспрямованість і узгодженість дій усіх елементів організації;

– здійснення різноманітних видів діяльності – виробничої, фінансової, торговельної, науково-дослідної, інвестиційної.

У рамках сучасних підходів до менеджменту організація розглядається як відкрита система, яка перебуває в постійному обміні з зовнішнім середовищем. Це середовище впливає на функціонування підприємства через сукупність чинників, які умовно поділяються на два основні типи:

1. Чинники прямого впливу (мікросередовище) – включають постачальників, споживачів, конкурентів, ринкову інфраструктуру, партнерів, державу;

2. Чинники непрямого (опосередкованого) впливу (макросередовище) – охоплюють соціально-економічні, політичні, правові, культурні, демографічні та технологічні аспекти.

Розуміння і системний аналіз взаємодії підприємств критичної інфраструктури з цими двома рівнями середовища є необхідною умовою ефективного стратегічного та операційного управління, особливо на об’єктах, де стабільність та стійкість системи є визначальними чинниками.

Аналіз характеру системних змін, що відбулися наприкінці ХХ століття у наукових засадах менеджменту як теорії ринкового управління, дає підстави узагальнити основні напрями його розвитку:

– визнання підприємства як відкритої системи, що функціонує під впливом динамічних зовнішніх чинників. Унаслідок цього управлінські акценти зміщуються від внутрішніх процесів до аналізу зовнішнього середовища та реалізації стратегій, орієнтованих на ринкові можливості;

– прагнення до прогнозування майбутніх тенденцій, формування гнучких управлінських структур та створення адаптивних механізмів для своєчасного реагування на загрози;

– орієнтація на досягнення довгострокових цілей, розвиток стратегічного мислення та впровадження систем стратегічного управління;

– зростання ролі людського ресурсу, впровадження форм соціального

партнерства, демократизація управлінських відносин, активізація організаційної культури як елемента управління;

– посилення маркетингової орієнтації в управлінні через зміну ринкової влади на користь споживача;

– визнання інновацій визначальним чинником формування конкурентних переваг і довгострокової стійкості підприємств;

– інтеграція міждисциплінарного підходу до модернізації техніко-технологічної бази підприємств через конвергенцію виробничих та наукових галузей;

– формування засад соціальної відповідальності бізнесу, включаючи етичні принципи функціонування;

– розвиток корпоративного управління як відповідь на інституційні зміни – від ізольованих підприємств до інтегрованих корпоративних структур;

– перехід від акценту на короткострокову ефективність до забезпечення інтересів усіх стейкхолдерів;

– широке впровадження сучасних інформаційних систем, моделей управління ризиками та економіко-математичних методів для сценарного планування;

– формування нових форм бізнесу – ділових альянсів, мережевих структур, електронної комерції;

– інтернаціоналізація управлінських практик в умовах глобалізації, жорсткої конкуренції та зростання протекціоністських тенденцій.

Звернемо увагу, що у межах трансформації управлінських підходів зростає значення забезпечення інформаційної безпеки підприємств, що є критично важливим компонентом загальної системи безпеки, зокрема для об’єктів критичної інфраструктури. Стандартна система менеджменту інформаційної безпеки (СМІБ) характеризується наявністю всіх ключових елементів сучасного управління, зокрема:

– наявність чіткої політики інформаційної безпеки, що відповідає стратегічним цілям суб’єкта господарювання;

– впровадження системного підходу до реалізації, підтримки, моніторингу та вдосконалення безпеки, узгодженого з організаційною культурою;

– підтримка з боку керівництва всіх рівнів управління;

– розуміння ризиків та управління ними (ризик менеджмент), формування відповідного рівня компетентності серед персоналу;

– розповсюдження політик, інструкцій та стандартів інформаційної безпеки серед усіх учасників організаційної діяльності, включаючи контрагентів;

– забезпечення фінансування заходів із забезпечення інформаційної безпеки;

– навчання, інформування та підвищення обізнаності працівників щодо

актуальних питань безпеки;

– налагодження ефективної системи реагування на інциденти;

– системна оцінка ефективності функціонування СМІБ і розробка рекомендацій щодо її вдосконалення [254].

Реалізація СМІБ може бути організована як сукупність управління цільовими процесами, що ініціюються за подієвими або часовими критеріями й відображають стратегічну орієнтацію підприємства на стійкість, захищеність та конкурентоспроможність (рис. 1.2).

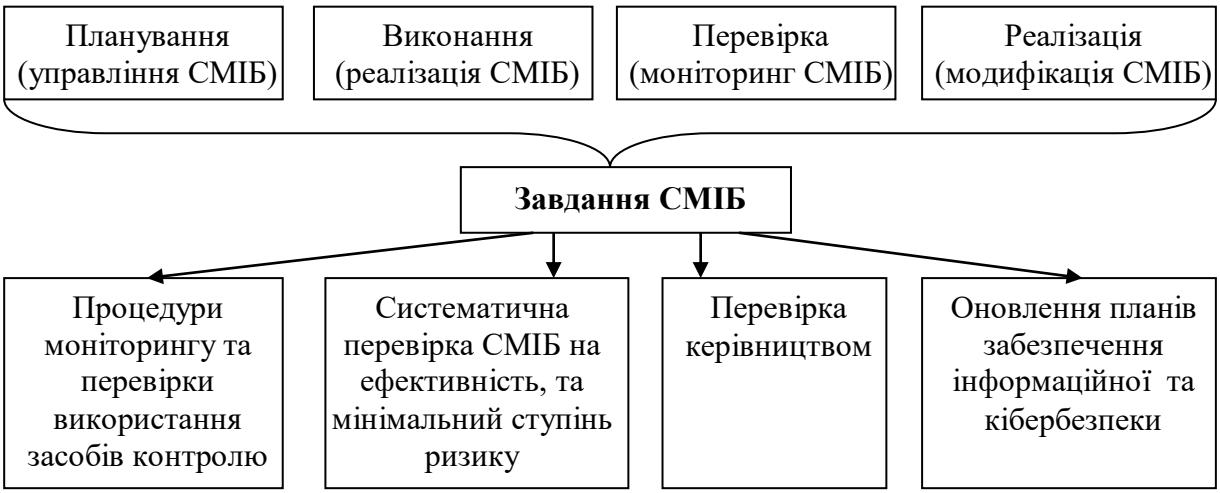


Рис. 1.2. Модель системи менеджменту інформаційної безпеки підприємства

Джерело: узагальнено за даними [115; 254]

Важливо враховувати, що визначення рівня (порогів) ризиків в сфері інформаційної безпеки підприємств критичної інфраструктури є виключною прерогативою вищого керівництва. Це пояснюється тим, що саме керівництво несе остаточну відповідальність за інвестиції в систему менеджменту інформаційної безпеки, а також за її загальну ефективність. Ключовим чинником у формуванні такої системи є дотримання вимог державних та міжнародних нормативно-правових актів і стандартів. При цьому слід зазначити, що стандарти відіграють роль орієнтирів або зразків дій, проте не є жорсткими догмами. Керівництво діє у багатовимірному середовищі, де необхідно враховувати взаємозалежні фактори та приймати зважені рішення щодо доцільності та меж впровадження положень з інформаційної безпеки.

Вітчизняні нормативно-правові акти часто мають декларативний характер і не завжди враховують специфіку інформатизації діяльності окремих підприємств. Натомість міжнародні стандарти (зокрема серії ISO/IEC 27000) характеризуються високою методологічною узгодженістю, що дозволяє уніфікувати вимоги в таких напрямах, як:

– управління доступом до інформації;

– захист даних;

– формування політик користування інформаційними ресурсами;

– впровадження автоматизованих систем захисту.

Процеси СМІБ можуть бути організовані у вигляді дерева процесів, яке відображає взаємозв'язки між етапами управління ризиками, реалізації заходів та контролю.

Особливої уваги заслуговує стандарт ISO/IEC 27003 «Information technology – Security techniques – Information security management system implementation guidance» [298], що базується на методології процесного підходу. Цей стандарт включає специфікації для всіх формальних атрибутів процесів СМІБ.

Реалізація СМІБ неможлива без інтеграції з процедурами контролю, що мають бути формалізовані в окремому блоці вимог. До обов'язкових функцій управлінських структур належать:

– моніторинг процедур захисту та контроль ефективності впроваджених заходів;

– оперативне виявлення порушень та загроз інформаційної безпеки;

– забезпечення своєчасного інформування керівництва;

– проведення внутрішніх аудитів та оцінювання залишкових ризиків;

– аналіз інцидентів, пропозиції щодо вдосконалення політик безпеки;

– періодичний перегляд ризиків відповідно до змін у зовнішньому та внутрішньому середовищі;

– перевірка керівництвом відповідності політики інформаційної безпеки сферам її застосування.

Етапи формування ефективної СМІБ:

Формування системи менеджменту інформаційної безпеки підприємства передбачає реалізацію десяти основних етапів, які можуть бути адаптовані до особливостей суб'єкта господарювання, у т.ч. об'єктів критичної інфраструктури:

1–2. Встановлення сфери застосування СМІБ та визначення загальної політики підприємства у сфері інформаційної безпеки з урахуванням стратегічних і організаційних чинників.

3–7. Оцінка ризиків та визначення захисних заходів на основі системи ризик-менеджменту.

8–10. Затвердження заходів, отримання підтримки керівництва, формулювання вимог з міжнародних і національних стандартів, оцінка економічної доцільності впровадження політик.

Під час визначення сфери застосування політики інформаційної безпеки доцільно враховувати:

– стратегічні цілі бізнесу;

– організаційну структуру;

– географічне розміщення активів;

– наявні інформаційні та технологічні ресурси [115].

У зв'язку з активною фазою військових дій на території України вплив зовнішніх чинників на функціонування вітчизняних підприємств, особливо тих, що належать до критичної інфраструктури, набув критичного характеру.

До ключових негативних факторів, що загрожують стабільності підприємств критичної інфраструктри, належать:

1. Ліквідація активів у результаті бойових дій.

2. Втрата ділової активності: припинення діяльності підприємств, постачальників і покупців через безпекові загрози; неможливість забезпечення довоєнних обсягів реалізації через падіння попиту та зміни ринкової кон'юнктури.

3. Згортання зовнішньоекономічної діяльності: обмеження експорту та імпорту внаслідок втрати портів, блокади морських шляхів, логістичних труднощів у залізничній і автомобільній галузях, валютного регулювання з боку НБУ.

4. Інфляція: зростання вартості енергоресурсів, дефіцит товарів, зниження доходів населення, міграційні процеси.

5. Відсутність інвестицій: зниження інвестиційної активності через надмірну ризиковість.

6. Криза банківської системи: втрати активів, скорочення обсягів кредитування, підвищення облікової ставки до 25 %.

7. Девальвація національної валюти: зростання вартості імпорту, інфляційний тиск.

Ці фактори демонструють, що підприємства не мають змоги безпосередньо впливати на зовнішнє середовище. У цьому випадку актуальним стає застосування антикризового менеджменту. Завдання антикризового управління на підприємствах критичної інфраструктри полягає у мінімізації негативних впливів шляхом використання адаптивних та альтернативних стратегій з метою збереження життєстійкості організації до моменту стабілізації умов. Система антикризового управління буде ефективною лише за умови синергії між її структурними блоками та постійної наявності зворотного зв'язку. Згідно з позицією Шарапова В., результативність антикризового менеджменту забезпечується через дотримання таких принципів:

1. Превентивність та терміновість реагування – швидке виявлення негативних впливів і своєчасне коригування.

2. Адаптивність – наявність гнучкої системи управління із зворотним зв'язком.

3. Використання внутрішніх ресурсів – орієнтація на самостійність у подоланні кризи.

4. Ефективність – переважання результатів над витратами на реалізацію антикризових заходів [282].

У звичайному (мирному) стані навколишнього середовища система захисту об'єктів критичної інфраструктури повинна ґрунтуватися на трьох базових складових:

– контроль – постійне відстеження параметрів безпеки та стану захищеності систем;

– регулювання – коригування параметрів функціонування з

урахуванням змін у середовищі;

– розробка та впровадження заходів безпеки – комплексна система заходів, спрямованих на запобігання, протидію та нейтралізацію потенційних загроз.

Наголос слід робити на ухваленні управлінських рішень, які базуються на аналізі наявних ризиків та прогнозуванні нових потенційних загроз. У сучасних умовах ці загрози є невід'ємною частиною трансформаційної діяльності, яка постійно генерує нові форми впливу на безпекове середовище. У даному випадку, варто відзначити, що система менеджменту на підприємствах критичної інфраструктури за кордоном широко застосовує цикл Шухарта–Демінга (PDCA), що є базовою моделлю не лише для управління якістю, а й для управління безпекою, екологічною сталістю та гігієною виробничих процесів. Застосування PDCA забезпечує неперервний, циклічний підхід до вдосконалення систем управління, дозволяючи підприємству розробити, впровадити й підтримувати екологічну та безпекову політику, яка ґрунтується на лідерстві та зобов'язаннях вищого керівництва щодо дотримання принципів сталого розвитку [310].

Основні етапи PDCA реалізуються у такій послідовності:

1. Планування (Plan) – встановлення цілей і процесів, необхідних для досягнення результатів, що відповідають політиці підприємства у сфері безпеки.

2. Реалізація (Do) – впровадження запланованих процесів у практику діяльності підприємства.

3. Перевірка (Check) – оцінювання результатів, моніторинг і вимірювання ефективності реалізованих процесів з урахуванням вимог, складання звітності.

4. Удосконалення (Act) – впровадження коригувальних дій для постійного покращення результатів функціонування системи.

Таким чином, менеджмент критичної інфраструктури в умовах стабільного середовища має бути не статичним, а динамічним процесом, що базується на регулярному аналізі, адаптації та впровадженні удосконалень з урахуванням прогнозних і фактичних загроз (рис.1.3).

Безпекова діяльність у сфері критичної інфраструктури є формою активної реакції суб'єктів управління на безпекову дійсність. Її сутність полягає у реалізації змін, спрямованих на забезпечення стійкості та захищеності систем, на основі засвоєння та розвитку безпекової культури. Це діяльність, що орієнтована на протидію загрозам, відновлення стабільності процесів та захист інтересів підприємства, забезпечуючи при цьому цілісність функціонування критично важливих систем [13]. Запропоновані безпекові механізми спрямовані на превентивне реагування – тобто попередження потенційних загроз ще до їх реалізації. Розробка ефективної системи безпеки вимагає всебічного вивчення методів управління нею, включно з менеджментом безпеки, що охоплює весь спектр організаційної, нормативної та ресурсної підтримки діяльності підприємства.

У сучасних умовах функціонування підприємств критичної інфраструктури, що характеризуються високим рівнем ризиків, виникає необхідність перегляду підходів до управління безпекою. Сьогодні безпековий менеджмент розглядається не лише як складова загальної управлінської структури, а як самостійний об'єкт управління, що вимагає спеціальних інструментів, механізмів і кадрової підтримки.

Рис. 1.3. Менеджмент у сфері безпекової політики об'єктів критичної інфраструктури

Джерело:сформовано на основі [13; 310]

Ефективне управління безпекою критичної інфраструктури можливе за умови дотримання таких ключових умов:

– легітимність усіх видів діяльності, що здійснюються в межах підприємства;

– системний підхід до організації безпеки, який охоплює всі рівні та елементи управління;

– достатній обсяг ресурсного забезпечення, зокрема кадрового, інформаційного, технічного й фінансового.

Система забезпечення безпеки підприємств у сфері критичної інфраструктури розглядається як впорядкована сукупність взаємопов'язаних

елементів, які в комплексі забезпечують захист інтересів підприємства від внутрішніх і зовнішніх загроз. Така система має бути інтегрованою, адаптивною та орієнтованою на динамічне реагування на зміну безпекового середовища.

Цілі управління безпекою підприємства у сфері критичної інфраструктури повинні відповідати встановленим вимогам до системи економічної безпеки, що забезпечують її стійкість і адаптивність у кризових умовах. Узагальнене уявлення про ці вимоги може бути подано у вигляді структурної схеми (рис. 1.4).

.

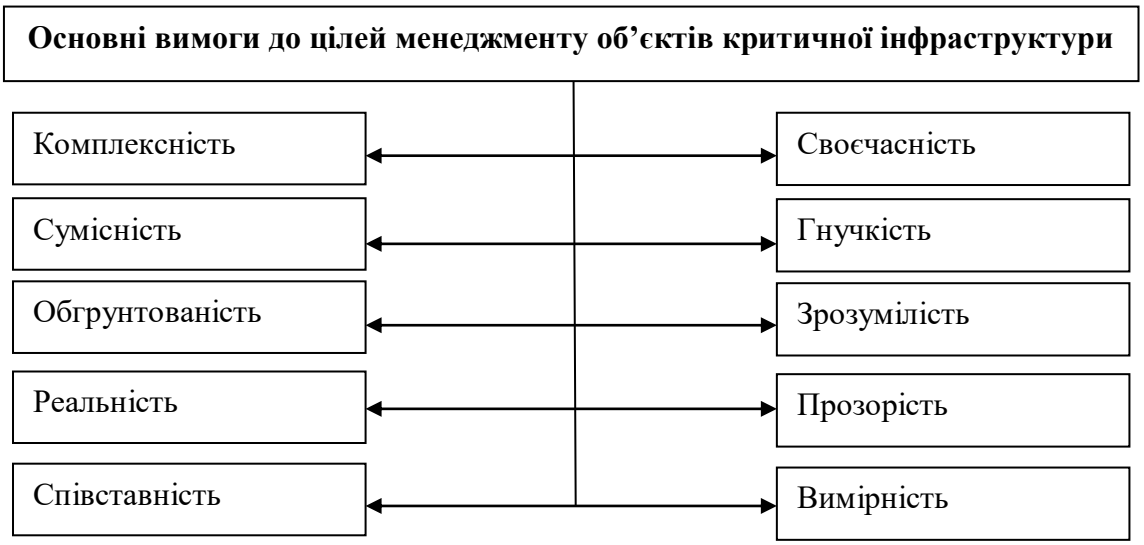


Рис. 1.4. Основні вимоги до цілей менеджменту об'єктів критичної інфраструктури

Джерело:сформовано на основі [13; 45]

Отже, цілі безпекового менеджменту підприємства у сфері критичної інфраструктури повинні мати комплексний характер. З одного боку, вони мають бути спрямовані на взаємоузгодження інтересів усіх зацікавлених сторін (стейкхолдерів), ефективне протистояння актуальним і потенційним загрозам, а також на забезпечення цих процесів необхідними ресурсами – у відповідній кількості та якості. З іншого боку, цілі безпекового менеджменту повинні бути органічно інтегровані у загальну систему цілей управління підприємством критичної інфраструктури, утворюючи єдину стратегічну платформу. Такий підхід забезпечує узгодженість між функціональною безпекою та операційною ефективністю, що є особливо важливим для підприємств, від стійкості яких залежить функціонування критично важливих систем держави та суспільства.

Система управління безпекою визначається як упорядкований підхід до управління, який охоплює організаційні структури, сфери відповідальності, політику та процедури. Згідно із системним підходом, будь-яка послуга або продукт, пов'язані з діяльністю об'єктів критичної інфраструктури, мають бути безпечними. Для реалізації цієї мети прийнято низку нових регламентів. Використання проактивних методів управління дозволило виявляти нові

загрози та вчасно коригувати управління змінами. Одним з ефективних інструментів системного підходу стало впровадження глобальних планів безпеки, які синхронізують міжнародні, регіональні та національні ініціативи задля забезпечення цілісності й стійкості об'єктів критичної інфраструктури [3; 4]. Зокрема актуальним є приведення системи захисту критичної інфраструктури до вимог концепції сталого розвитку. Відповідно до неї, система безпеки об'єктів критичної інфраструктури охоплює такі ключові компоненти:

– економічну та технологічну (інфраструктура, економічна ефективність, технологічна модернізація, цифрова безпека);

– соціальну (доступ до основних послуг, охорона здоров'я, освітні ініціативи, підвищення якості життя);

– екологічну (протидія змінам клімату, контроль викидів, стале використання ресурсів, екологічно чисті технології).

Сучасне управління об'єктами критичної інфраструктури дедалі більше зосереджується на довгостроковій перспективі, запроваджуючи практики обслуговування та експлуатації, які враховують соціальні, екологічні та економічні аспекти прийняття бізнес-рішень. За спостереженнями Bhatt G. [287] цей сегмент активно інтегрує принципи сталого розвитку, оскільки цифровізація й сталість є ключовими рушійними силами розвитку менеджменту з 1970-х років, що істотно впливає на роль менеджерів із управління об'єктами критичної інфраструктури. Водночас, за словами Bruneau M та ін. [288], професіонали менеджери часто сприймаються як консервативні, що ускладнює впровадження принципів сталого розвитку.

Концепція сталого управління об'єктами (Sustainable Facility Management – SFM) об'єднує менеджмент та сталий розвиток шляхом впровадження інноваційних технологій і бізнес-практик, які забезпечують баланс між соціальними, економічними та екологічними впливами. Глобальні виклики, пов'язані зі зміною клімату та вимогами до енергоефективності, стимулюють менеджерів до розробки рішень, які мінімізують негативний вплив на довкілля. Менеджери відіграють ключову роль у впровадженні принципів сталого розвитку в ширший контекст середовища розвитку критичної інфраструктри. Проте ефективне застосування цих принципів потребує партнерської взаємодії із зацікавленими сторонами, а також розробки стратегій, що сприяють здоров'ю, безпеці та добробуту працівників. Стале управління дозволяє вирішувати численні проблеми менеджменту, оптимізуючи операційну діяльність на стратегічному, тактичному та оперативному рівнях. Це потребує цілісного підходу до інвестицій, управління просторами, експлуатації та технічного обслуговування. Попри те, що SFM часто зосереджується на технічних і екологічних аспектах [4], зростає увага до соціальної та економічної стійкості підприємницької діяльності. Переваги сталого управління наявними об'єктами – зокрема енергоефективність, зменшення відходів, збереження води та контроль викидів.

Згідно з дослідженням International Facility Management Expert Center (IFMEC) у Нідерландах [144], стратегічний менеджмент об'єктів критичної інфраструктури здатне сприяти досягненню всіх 17 Цілей сталого розвитку (ЦСР), оскільки менеджмент охоплює всі рівні організації – від корпоративного до операційного – і здатне змінювати поведінку на індивідуальному рівні.

Зв'язок менеджменту об'єктів критичної інфраструктури із цілями сталого розвитку (ЦСР):

– ЦСР 1 (подолання бідності): створення робочих місць та економічне зростання.

– ЦСР 2 (нульовий голод) і ЦСР 3 (здоров'я і благополуччя): забезпечення харчування і умов праці в школах, лікарнях, компаніях.

– ЦСР 4 (якісна освіта): підтримка навчальних закладів.

– ЦСР 5 (гендерна рівність) і ЦСР 10 (зменшення нерівності): рівний доступ до можливостей.

– ЦСР 6 (чиста вода): ефективне управління водними ресурсами в будівлях.

– ЦСР 7 (чиста енергія): енергоефективне управління об'єктами.

– ЦСР 9 (інновації та інфраструктура): впровадження AI, IoT та інших «розумних» технологій.

– ЦСР 11 (стійкі міста): обслуговування інфраструктури міських об'єктів.

Отже, стале управління об'єктами критичної інфраструктури, на переконання вчених [2] передбачає:

Енергоефективність: впровадження енергоощадних технологій для зменшення навантаження на енергосистему, зниження ризиків від перебоїв постачання та мінімізації викидів.

Раціональне використання водних ресурсів: управління водозабезпеченням об'єктів через сучасні системи фільтрації, іригації, повторного використання води тощо.

Управління відходами: зниження обсягів утворення небезпечних та побутових відходів на об'єктах за рахунок сортування, утилізації та впровадження програм циркулярної економіки.

Екологічну сертифікацію інфраструктури: впровадження міжнародних стандартів (наприклад, ISO, LEED), що підтверджують екологічну та техногенну безпеку об'єктів критичної інфраструктури.

Зазначимо також, що система менеджменту безпеки об'єктів критичної інфраструктури тісно пов'язана з глобальною екологічною безпекою, адже загрози дедалі частіше виходять за межі локальних осередків і перетинають адміністративні кордони. Неузгодженість законодавства та міжсекторальної політики створює додаткові перешкоди для реалізації ефективних управлінських рішень.

Як зазначалося вище, особливого значення набуває концепція антикризового менеджменту, зокрема в умовах воєнного часу вона охоплює:

1. превентивні заходи з виявлення кризових явищ (діагностика, моніторинг, раннє попередження);

2. відновлювальні дії (забезпечення життєстійкості, відновлення функціонування, ліквідність і стабілізація фінансового стану);

3. стратегічне стабілізування (збереження довгострокової платоспроможності, мінімізація втрат, ефективне управління ресурсами).

Криза не є виключно негативним явищем: її поява створює умови для трансформацій і вдосконалення управлінських процесів. Основні завдання антикризового менеджменту включають: своєчасне виявлення проблем, застосування стабілізаційних механізмів, збереження функціональності та забезпечення сталого розвитку об'єкта критичної інфраструктури.

За ДСТУ ISO Guide 73 [38], ризик визначається як невизначеність щодо досягнення цілей. У ширшому розумінні ризик можна охарактеризувати як ймовірність настання події, що може завдати шкоди або мати негативні наслідки для функціонування системи. Оцінювання ризику включає два ключові аспекти – імовірність виникнення події та масштаб її наслідків. Зазвичай можливість завдання шкоди зумовлена порушенням нормального функціонування системи, а ймовірність реалізації цієї можливості у визначений момент часу відображає рівень ризику.

У контексті управління об'єктами критичної інфраструктури, аналіз ризиків є одним із ключових інструментів забезпечення їхньої стійкості та безпеки. Виділяють чотири основні функції ризику:

1. Захисна функція – формує раціональне ставлення до можливих невдач, сприяє підготовці до несприятливих сценаріїв.

2. Аналітична функція – передбачає необхідність вибору з-поміж кількох альтернатив під час ухвалення управлінських рішень, особливо в умовах невизначеності.

3. Інноваційна функція – стимулює пошук нетрадиційних, нестандартних рішень для подолання потенційних загроз або викликів.

4. Регулятивна функція – має суперечливий характер і проявляється у двох формах:

– конструктивній – коли ризик сприяє розвитку, адаптації та вдосконаленню системи;

– деструктивній – коли ризик призводить до порушення стабільності або руйнування критичних процесів.

Таким чином, правильне розуміння природи ризику та його функцій є важливою передумовою ефективного управління об'єктами критичної інфраструктури, особливо в умовах зовнішньої нестабільності, техногенних загроз або надзвичайних ситуацій [305]. Ідентифікація ризику включає процес виявлення, усвідомлення, складання переліку та описування елементів ризику – джерел небезпек, небезпечних факторів, загроз, небезпечних подій, їхніх потенційних наслідків, імовірностей виникнення. Оцінювання ризику включає процес порівняння оціненого ризику з конкретними критеріями ризику для визначення їхньої значущості та є

необхідним для подальшого прийняття рішень щодо їхньої обробки. Це є найбільш ефективним запобіжним заходом, під час якого враховуються можливі транспортні події і небезпеки, що можуть викликати негативні наслідки. Він дає змогу формувати і запроваджувати заходи щодо зниження ймовірності виникнення небезпек

Керування ризиками є скоординованою діяльністю, що охоплює прийняття управлінських рішень і контроль над заходами щодо реагування на ризики. Основна мета цієї діяльності – забезпечення припустимого рівня ризику, який не загрожує стабільності функціонування об'єкта критичної інфраструктури. Процес ідентифікації загроз або небезпечних чинників передбачає системний моніторинг зовнішніх змін у нормативно-правовому полі (у тому числі змін у законодавстві, директивах ЄС тощо), а також внутрішніх змін, серед яких:

– оновлення або зміни в технологічних процесах керування;
– модернізація або впровадження нового обладнання;
– зміни в методах експлуатації систем;
– коригування захисних заходів та технічних рішень у сфері безпеки;
– модифікація режимів обслуговування, у тому числі із залученням зовнішніх підрядників (аутсорсинг).

Ідентифікація загроз є неперервним процесом, що базується як на внутрішніх, так і зовнішніх джерелах інформації, з обов'язковим документуванням усіх процедур. Особлива увага приділяється потенційним змінам у технологічних ланцюгах, автоматизованих системах керування, обладнанні, персоналі та взаємодії між елементами системи. При цьому варто враховувати всі рівні ймовірності реалізації загроз – від малоймовірних до високореалістичних сценаріїв. Важливим завданням є визначення межі між обґрунтованими ризиками та надто спекулятивними, які не потребують детального аналізу.

Невід'ємним елементом менеджменту підприємств критичної іфнраструтекри також варто розглядати управління інфраструктурними активами, що включає інвентаризацію, моніторинг, технічне обслуговування та стратегічне планування, з метою забезпечення працездатності об'єктів і мінімізації експлуатаційних ризиків. Основними викликами в цьому процесі є:

1. Вимоги до безпеки та надійності критичної інфраструктурних систем, які залежать від їхнього типу та функціонального призначення.

2. Моніторинг якості експлуатації – необхідність регулярного виявлення дефектів, що можуть впливати на безпеку користувачів та функціональність системи в довгостроковій перспективі.

3. Контроль витрат – ефективне планування фінансових ресурсів і технічного обслуговування, з акцентом на профілактичні заходи та багаторічне планування.

Отже, для досягнення ефективного менеджменту підприємств критичної інфраструктури доцільно впроваджувати такі передові практики:

– Стратегічне планування – формування чіткого бачення, впровадження систем моніторингу, визначення регулярних циклів інспекції та оцінювання технічного стану.

– Мультисекторальна співпраця – тісна взаємодія між органами державної влади, технічними підрозділами, підрядними структурами, проєктувальниками та експлуатаційними службами.

– Використання сучасних технологій – застосування цифрових інструментів, таких як 3D-моделювання, віртуальна реальність, ГІС, BIM (інформаційне моделювання інфраструктури), для підвищення точності проєктування, управління й обслуговування.

– Профілактичне технічне обслуговування – впровадження системи регулярного превентивного обслуговування для виявлення й усунення потенційних відмов до моменту їх критичного впливу на систему.

Зазначимо, що управління підприємствами критичної інфраструктури також охоплює прийняття рішень щодо розподілу ресурсів у часі та просторі з метою досягнення максимальної ефективності. Для цього використовуються два типи інформації:

– інформація про поточний стан об’єкта, що отримується шляхом інспекції;

– інформація про майбутній стан, що ґрунтується на прогнозуванні, з використанням математичних моделей ефективності.

Процес прийняття рішень інтегрує також механізми зворотного зв’язку – результати моніторингу впливають на вибір майбутніх дій з обслуговування, перевірок і планування, створюючи саморегульовану систему управління. Цей ефект представлено петлею зворотного зв’язку на рис. 1.5. Отже, можна стверджувати, що менеджмент підприємств критичної інфраструктури передбачає не лише технічне обслуговування об’єктів, а й формування стратегій щодо їхньої стійкості до ризиків, загроз та надзвичайних ситуацій.

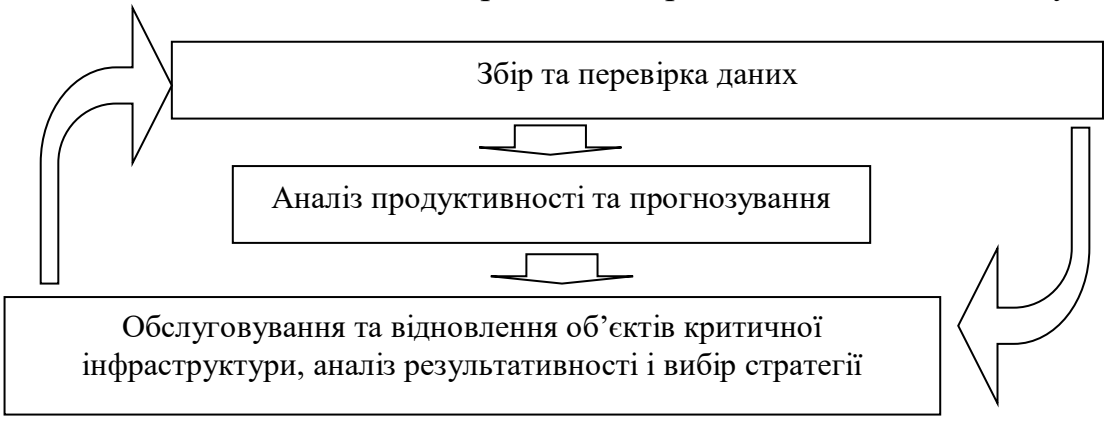


Рис. 1.5. Процес управління підприємствами критичної інфраструктури

Джерело: сформовано на основі [361]

У країнах з високим рівнем урбанізації та інтенсивною експлуатацією

інфраструктури зростає потреба у системному підході до управління безпекою таких об’єктів, які досягли або перевищили свій проєктний термін експлуатації. Рішення щодо заходів з технічного обслуговування, модернізації або заміни таких об’єктів стають особливо значущими з огляду на потенційні соціальні, екологічні та економічні наслідки аварій чи збоїв.

Ключовим елементом такого менеджменту є ідентифікація ризиків – процес виявлення небезпечних факторів або загроз, що можуть вплинути на функціонування об’єкта. Це включає аналіз:

– змін у технологічних процесах та обладнанні,

– нормативно-правових вимог (включаючи Директиви ЄС та законодавство України),

– участі третіх сторін (аутсорсинг),

– впливу кіберзагроз на автоматизовані системи керування (АСУ),

– та інших внутрішніх і зовнішніх джерел ризику.

Невід’ємною частиною цього процесу є аналіз невизначеностей, зокрема:

– Стохастична (алеторична) невизначеність, яка відображає випадковий характер зовнішніх або внутрішніх подій (наприклад, погодні катастрофи або збої техніки).

– Епістемічна невизначеність, яка виникає через неповноту або неоднозначність інформації, недосконаліть моделей або відмінності в експертних оцінках щодо майбутньої поведінки об’єкта.

Ця остання є особливо важливою у сфері безпеки критичної інфраструктури, оскільки неправильний вибір моделі прогнозування стану об’єкта або сценарію ризику може призвести до серйозних помилок в управлінні.

Щоб зменшити вплив епістемічної невизначеності, рекомендується:

– використовувати сценарне планування та багатоваріантне моделювання,

– впроваджувати системи раннього попередження (Early Warning Systems),

– застосовувати інтегровані цифрові платформи (напр., GIS, BIM, SCADA) для збору, обробки й візуалізації даних у режимі реального часу,

– здійснювати багаторівневу координацію між операторами інфраструктури, державними органами, правоохоронними структурами та громадськістю.

Таким чином, ефективний менеджмент підприємств критичної інфраструктури передбачає гнучке управління ризиками, врахування як технічних, так і організаційних чинників, постійний моніторинг стану об’єктів і здатність адаптуватися до мінливого середовища, забезпечуючи безперервність і безпеку надання суспільно важливих послуг [362]. Управління об’єктами критичної інфраструктури поєднує принципи інженерії, архітектури, організаційного управління та безпеки для координації фізичного середовища, працівників і процесів. Важливою метою

є забезпечення високої надійності систем, мінімізації ризиків та забезпечення оперативної реакції на загрози. Серед ключових компонент менеджменту у сфері безпеки критичної інфраструктури можемо виділити наступні:

1. Експлуатація та технічне обслуговування: регулярне планове обслуговування й моніторинг стану інфраструктури (електропостачання, водопостачання, зв'язку, транспортних вузлів тощо) є критичними для запобігання аваріям та забезпечення безперервної роботи.

2. Управління простором: стратегічне планування та оптимізація простору під критичні об'єкти з урахуванням безпеки, швидкого доступу екстрених служб і евакуаційних маршрутів. Також передбачає контроль доступу до чутливих зон.

3. Екологічна стійкість та управління ризиками довкілля: врахування екологічних загроз у процесі експлуатації інфраструктурних об'єктів. Наприклад, запровадження енергоощадних технологій, екологічного моніторингу та сценарного планування на випадок природних катастроф.

4. Здоров'я та безпека персоналу: реалізація заходів із захисту персоналу від фізичних, хімічних, біологічних загроз, а також впровадження систем моніторингу безпечних умов праці на об'єктах критичної інфраструктури.

5. Фізична та інформаційна безпека: розробка та впровадження комплексних систем безпеки, які включають відеоспостереження, контроль доступу, кіберзахист, резервування систем управління та захист конфіденційної інформації.

6. Управління проєктами модернізації та підвищення стійкості: реалізація інфраструктурних проєктів з урахуванням принципів безпеки, довготривалої експлуатаційної надійності та стійкості до навмисних атак або природних катастроф.

Управління безпекою критичної інфраструктури активно інтегрує цифрові технології, що дозволяють підвищити рівень моніторингу, передбачуваності та оперативності реагування:

– Системи управління інфраструктурою (BMS/SCADA) здійснюють централізований моніторинг та контроль життєво важливих систем у режимі реального часу.

– Інтернет речей (IoT) забезпечує збір даних з датчиків для виявлення аномалій, контроль температури, вологості, тиску та інших параметрів, критичних для безпеки.

– Цифрові двійники дозволяють змоделювати поведінку інфраструктурних систем в умовах надзвичайних ситуацій та випробовувати сценарії втручань без ризику для реального об'єкта.

– Комп'ютеризовані системи управління об'єктами (CAFM) централізують інформацію щодо активів, обслуговування, розкладів інспекцій, інцидентів і ризиків, забезпечуючи аналітику для прийняття обґрунтованих управлінських рішень.

Менеджмент критичних об'єктів набуває нових форм під впливом технологій, зміни клімату, вимог до безпеки та соціальних трансформацій.

Сучасні та майбутні підходи передбачають трансформацію простору, процесів і технологій. Функціонування критичної інфраструктури дедалі більше орієнтується на адаптивність, зокрема в умовах змішаного або дистанційного формату роботи персоналу. Це вимагає гнучкого зонування, можливості швидкої трансформації приміщень та ефективного просторового планування для забезпечення безпеки, спостереження та контролю. Відповідно, організація простору за принципом діяльності (activity-based planning) дозволяє підвищити оперативність роботи персоналу, забезпечити фізичну безпеку і стійкість об'єкта до внутрішніх та зовнішніх загроз [2].

Безпека критичної інфраструктури також неможлива без менеджменту енергонезалежності та здатності адаптуватися до змін клімату. Відповідно, менеджери критичних підприємств повинні розвивати локальні джерела енергії (сонячні, вітрові установки), впроваджувати системи накопичення енергії та забезпечувати резервне живлення в разі надзвичайних ситуацій. Паралельно необхідно посилювати захист об'єктів від кліматичних ризиків: ізолювання, водозахист, використання вогнестійких і водостійких матеріалів. Це підвищує функціональну надійність об'єкта в умовах природних катастроф.

Забезпечення безпеки критичної інфраструктури включає також турботу про фізичне та психічне здоров'я працівників. Біофільний дизайн, якісна вентиляція, природне освітлення, зони відпочинку – все це підвищує стійкість персоналу, що працює в умовах підвищеної відповідальності. Інфраструктура має відповідати вимогам стандартів здорового середовища (WELL Building Standard), які зосереджені на контролі якості повітря, води, шумового навантаження та ергономіки робочого місця [10].

Менеджмент об'єктів критичної інфраструктури дедалі більше опирається на великі дані (Big Data) та інтелектуальну аналітику. Збір інформації з сенсорних систем дозволяє прогнозувати збої у роботі обладнання, своєчасно виявляти вразливості та оптимізувати ресурси. Наприклад, завдяки аналітиці використання простору можна раціоналізувати маршрути евакуації, оптимізувати навантаження на технічні системи або спрямувати ресурси на найбільш навантажені вузли інфраструктури.

Отже, інтегровані системи менеджменту на підприємствах критичної інфраструктури стають обов'язковим елементом її стійкості. Управління може здійснюватися в реальному часі через хмарні платформи, з можливістю дистанційного моніторингу та реагування на інциденти. Це забезпечує не лише ефективність, а й підвищує захищеність об'єкта від зовнішніх і внутрішніх загроз. Менеджмент у сфері безпеки критичної інфраструктури – це багатовекторна діяльність, що поєднує сталий розвиток, технологічну інноваційність і адаптивне управління. Впровадження сучасних технологій, підвищення кліматичної стійкості, діджиталізація процесів і створення безпечного середовища для працівників формують нову парадигму управління, орієнтовану на безперервність функціонування, стійкість до ризиків і ефективну взаємодію з навколишнім середовищем.

1.2. Визначення критичної інфраструктури як об’єкту управління

Забезпечення непорушності автентичних принципів і фундаментальних засад національної безпеки має ключове значення для будь-якої суверенної держави. В умовах запровадженого в Україні воєнного стану ця проблема набуває особливої актуальності у сфері державного управління. Це зумовлено чинною нормативно-правовою базою, зокрема положенням п. 9 ст. 1 Закону України «Про національну безпеку України», відповідно до якого національна безпека визначається як «захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз» [62]. У п. 10 цієї ж статті національні інтереси України трактується як «життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян» [62].

Зазначені положення виокремлюють стратегічні напрями реалізації національних інтересів, серед яких домінують:

1. Забезпечення територіальної цілісності, державного суверенітету та дотримання демократичних засад конституційного ладу, включно з недопущенням зовнішнього втручання у внутрішні справи держави;

2. Сприяння сталому економічному розвитку з метою підвищення рівня та якості життя населення;

3. Реалізація євроінтеграційного вектору розвитку України у політичній, правовій, економічній та безпековій площинах, а також формування взаємовигідних відносин із міжнародними партнерами на засадах рівноправності та з перспективою вступу до Європейського Союзу та НАТО [62].

Аналіз основоположних положень цього Закону дозволяє стверджувати, що система національної безпеки України ґрунтується на гармонійному поєднанні трьох складових: життєво важливих інтересів держави, стратегічних загроз і національної системи захисту. Варто підкреслити, що поняття «загроз критичній інфраструктурі» вперше було інституціоналізовано у Стратегії національної безпеки України 2015 року, яка визначила захист об’єктів критичної інфраструктури як один із пріоритетних напрямів державної політики у сфері національної безпеки [240].

У цьому контексті доцільно навести позицію М. Б. Домарецького [40, с. 83], який пропонує класифікувати життєво важливі інтереси держави за такими ключовими напрямами:

– гарантування ефективного захисту критично важливих об’єктів та населення в умовах надзвичайних ситуацій і терористичних загроз;

– забезпечення життєздатності та безпеки населення під час воєнних дій;

– підтримання безперервного функціонування інфраструктурних об’єктів, що є визначальними для життєдіяльності населення і стабільності економіки.

Таким чином, захист об’єктів критичної інфраструктури набуває першочергового значення в системі гарантування національної безпеки України. Цей підхід знайшов своє нормативне закріплення у Законі України «Про критичну інфраструктуру» від 16 листопада 2021 року, який встановлює правові та організаційні засади її функціонування й захисту.

Аналогічна стратегічна орієнтація простежується й у міжнародному досвіді. Зокрема, у Стратегії внутрішньої безпеки США [300] виділено шість ключових напрямів забезпечення національної безпеки, одним із яких є саме захист критично важливих об’єктів, що має універсальне значення для розвинених держав (рис. 1.6).

Рис. 1.6. Структура системи забезпечення національної безпеки США
Джерело: сформовано авторами за даними [33], [300]

У Стратегії національної безпеки України [240] визначено перелік основних загроз, які необхідно враховувати під час формування державної політики у сфері захисту критичної інфраструктури. До них належать:

– ризики виникнення надзвичайних ситуацій техногенного та природного походження, вплив кліматичних змін і поширення інфекційних захворювань;

– глобальна гонка озброєнь із використанням новітніх технологій;

– зростання масштабів міжнародної злочинності у кіберпросторі, терористичної діяльності, торгівлі наркотиками, людьми, зброєю, сепаратизму;

– пандемія COVID-19 як чинник, що зумовив ланцюгові деструктивні ефекти: збільшення рівня безробіття, криза систем охорони здоров’я та соціального захисту, обмеження логістики, зниження продовольчої безпеки, трудова міграція та поглиблення глобальної фінансово-економічної нестабільності;

– зростання проявів демонстрації «національної сили» у міжнародній конкуренції, включаючи збройну агресію РФ проти України;

– застарілість систем озброєння радянського виробництва через хронічне недофінансування їх модернізації;

– низька ефективність державного управління, обумовлена поширеністю корупційних практик;

– недостатній рівень добробуту населення;

– слабкий рівень правової захищеності у ключових сферах, значна частка державної власності в економіці та обмежена конкуренція, зокрема у секторах критичної інфраструктури, що гальмує інвестиційну активність;

– погіршення якості життєвого середовища (нераціональне природокористування, зниження якості води, повітря, харчових продуктів);

– поглиблення демографічної кризи та активізація еміграційних процесів.

Окрему увагу слід приділити зростанню загроз для критичної інфраструктури внаслідок несанкціонованих фізичних або кібервтручань, її технічної зношеності, дефіциту інвестицій у модернізацію, активних бойових дій на сході країни та тимчасової окупації частини території.

Згідно з аналізом законодавчих актів іноземних держав [292], [300], загрози критичній інфраструктурі умовно поділяються на три основні категорії: зловмисні дії, надзвичайні ситуації техногенного та природного характеру. Д. Г. Бобро [11, с. 86] пропонує доповнити цей перелік ще однією категорією – сукупними ризиками, які є особливо небезпечними, оскільки здатні провокувати так званий «ефект доміно», спричиняючи каскадні порушення у функціонуванні взаємопов’язаних об’єктів критичної інфраструктури.

Таке явище доцільно позначити терміном «каскадний ефект дестабілізації критичної інфраструктури», що означає виникнення комплексних наслідків унаслідок порушення функціонування одного або кількох інфраструктурних об’єктів. Наприклад, функціонування системи водопостачання безпосередньо залежить від енергопостачання насосних станцій, які, у свою чергу, забезпечують життєдіяльність пожежних та аварійно-рятувальних служб.

У країнах із розвиненою нормативно-правовою базою критична інфраструктура розглядається як ключовий елемент національної безпеки. В Україні в останні роки спостерігається активізація зусиль держави щодо формування стратегічного бачення захисту критичної інфраструктури, зокрема в рамках Стратегії національної безпеки. Разом з тим, ця сфера вимагає суттєвої модернізації системи державного регулювання, особливо в контексті євроінтеграційних прагнень та міжнародної практики управління безпекою.

Актуальність цього напряму посилює потребу у глибокому науковому опрацюванні, розробці та впровадженні концепції державної політики у сфері захисту критичної інфраструктури. Першим кроком у цьому процесі має стати уточнення дефініції «критична інфраструктура», що дозволить закласти методологічне підґрунтя для формування ефективної системи

державного управління у цій сфері.

Дослідження української та міжнародної нормативно-правової бази засвідчує, що термін «критично важливі об'єкти» широко використовується у законодавстві більшості країн, проте його тлумачення варіюється. Поняття «критична інфраструктура» вперше почало фіксуватися у 1990-х роках, а в Україні воно офіційно увійшло в обіг із 2006 року. Категоризація об'єктів за ступенем критичності була здійснена лише у 2021 році прийняттям Закону України «Про критичну інфраструктуру», де критичність трактується як «ступінь (відносний рівень) важливості об'єкта критичної інфраструктури, класифікована залежно від його впливу на виконання життєво важливих функцій та/або надання життєво важливих послуг» [60].

Наразі у науковому, діловому та урядовому дискурсі дефініція «критична інфраструктура» перебуває у процесі постійного уточнення. Універсальним критерієм вважається наявність взаємозв'язку між державними й приватними об'єктами, що прямо або опосередковано впливають на рівень національної безпеки та забезпечення життєво важливих функцій суспільства. Згідно з дослідженнями вчених [47, с. 112; 251, с. 69], до критичної інфраструктури відносяться транспортна й енергетична мережі, газо- та нафтопроводи, системи життєзабезпечення, річкова та морська інфраструктура, зв'язок, служби поводження з небезпечними відходами, оборонна промисловість, екстрені служби та органи влади. У США до цього переліку додано також об'єкти культурної спадщини – національні символи, музеї, виставки, що мають стратегічну цінність [13].

Визначення, запропоноване колективом авторів під керівництвом С. П. Азарова та В. Л. Сидоренка, розглядає критичну інфраструктуру як «сукупність взаємопов'язаних сегментів і складових об'єктів національного господарського комплексу, що забезпечують функціонування життєво важливих сфер. Їх часткова або повна втрата функціональності може безпосередньо і в короткі строки вплинути на стан національної безпеки, спричиняючи надзвичайні ситуації відповідного рівня та масштабу» [1, с. 45].

Уряди більшості розвинених країн розробили власні підходи до нормативного закріплення поняття критичної інфраструктури. США виступили піонерами у цьому напрямі, закріпивши відповідну дефініцію в «USA Patriot Act» від 23 жовтня 2001 року [353]. Згідно з документом, критична інфраструктура – це «життєво важливі для країни фізичні чи віртуальні активи й засоби, повне знищення або часткова втрата функціональності яких здатна спричинити негативний вплив на національну безпеку, економіку, здоров'я населення або їх комбінацію» [353].

Європейський підхід також має вагоме значення. Зокрема, у 2002 році під час засідання Євроатлантичної ради НАТО зазначалося, що критична інфраструктура охоплює кібернетичні та фізичні системи, необхідні для стабільного функціонування економіки та державного управління. У Директиві Європейської Комісії 2008/114 [295] критична інфраструктура визначається як об'єкти, системи або їх частини, що є важливими для

підтримки життєво необхідних функцій суспільства. Їх порушення або руйнування може суттєво вплинути на функціонування країни-члена ЄС [295, с. 168].

У Німеччині поняття «критична інфраструктура» закріплено в Національній стратегії її захисту, де воно охоплює фізичні та організаційні структури, які мають вирішальне значення для функціонування суспільства й економіки. Їхній збій може спричинити дефіцит постачання, загрозу громадській безпеці та інші серйозні наслідки [331, с. 8]. На відміну від загальноєвропейського підходу, німецька концепція акцентує на стабільності постачання товарів і послуг першої необхідності.

У Республіці Польща визначення критичної інфраструктури закріплено в Ustawa o zarządzaniu kryzysowym (Закон «Про антикризове управління»), відповідно до якого критична інфраструктура охоплює «системи та їх функціонально пов'язані об'єкти, включаючи будівельні споруди, технічні засоби, установи та служби, що мають ключове значення для безпеки держави та її громадян, а також забезпечують належне функціонування органів державної влади і приватного сектора» [354, с. 1]. З аналізу цього визначення можна виокремити акцент на важливості безперервного функціонування державних органів управління та визначенні спеціалізованих структур, відповідальних за підтримку життєдіяльності критичних секторів.

Слід наголосити, що зарубіжні підходи до дефініції критичної інфраструктури фокусуються не стільки на фізичних характеристиках об'єктів, скільки на значущості функцій і послуг, які вони забезпечують для суспільства, держави та економіки.

У ряді інших країн спостерігається власна специфіка тлумачення цього поняття. Так, у Хорватії до критичної інфраструктури належать об'єкти, мережі, послуги, матеріальні ресурси та ІТ-системи, виведення з ладу яких може серйозно вплинути на безпеку та здоров'я населення або на спроможність державної влади виконувати свої функції. В Австралії критична інфраструктура охоплює фізичні об'єкти, інформаційні системи, телекомунікаційні мережі та логістичні ланцюги, порушення або знищення яких спричиняє серйозний вплив на соціальну стабільність, економіку чи обороноздатність країни. В Ізраїлі критичною вважається така інфраструктура, виведення якої з ладу потенційно може спричинити серйозні соціально-економічні наслідки, що загрожують стабільності суспільства і національній безпеці. У Японії відповідальність за формування системи критичної інфраструктури покладається на бізнес-суб'єкти, які надають незамінні послуги, і втрата доступу до яких або зниження їхньої ефективності негативно впливають на суспільне життя та економічну активність [47, с. 112].

Таким чином, у більшості країн світу відбувається зміщення акценту з матеріально-технічного аспекту до значення функціонального призначення інфраструктурних елементів. Такий підхід відкриває нові можливості для формування методологічно обґрунтованих критеріїв виокремлення

критичних елементів інфраструктури та визначення пріоритетів їхнього захисту.

Аналіз наведених інтерпретацій дозволяє дійти висновку, що більшість з них орієнтовані на забезпечення національної безпеки, життєдіяльності населення та сталості функціонування держави. Відповідно, доцільно погодитися з визначенням С. Гнатюка, В. Сидоренка, Н. Сєйлової [28, с. 85], які характеризують критичну інфраструктуру як глобальну систему стратегічно важливого значення, що об'єднує різнорідні за своєю природою об'єкти, з'єднані між собою функціональними зв'язками, що підкреслює міждисциплінарний характер взаємодії критичних елементів.

Таким чином, хоча дефініції критичної інфраструктури в різних країнах мають певні відмінності, вони, переважно, зумовлені національними особливостями та специфікою правових систем.

Важливою складовою державної політики у сфері захисту критичної інфраструктури є питання ідентифікації об'єктів, які мають стратегічне значення, серед широкого спектра національних ресурсів. Аналіз нормативно-правової бази України дозволяє згрупувати потенційно важливі об'єкти у так званий квадро-комплекс:

1. Об'єкти загальнонаціонального значення.
2. Життєво необхідні об'єкти.
3. Стратегічно важливі об'єкти.
4. Соціально значущі об'єкти.

Суттєвою проблемою реалізації державної політики в цій сфері вітчизняні дослідники вважають складність верифікації критичних об'єктів на різних рівнях – національному, регіональному та місцевому. Вирішення цього питання частково запропоновано у Законі України «Про критичну інфраструктуру» [60], де подано перелік ключових послуг та функцій, надавачі яких підлягають пріоритетному захисту. Серед них: водопостачання і водовідведення, фармацевтична промисловість, енергозабезпечення, діяльність біолабораторій, продовольче забезпечення, охорона здоров'я, виробництво вакцин, інформаційні та фінансові послуги, електронні комунікації, оборона і держбезпека, транспорт, цивільний захист, правоохоронна діяльність, правосуддя, утримання під вартою, рятувальні служби, космічна сфера, дослідження, хімічна промисловість тощо.

Однак цей перелік не є вичерпним і остаточним. Він може суттєво варіювати залежно від особливостей держави та її потреб. Наприклад, у США на національному рівні налічується приблизно 1700 об'єктів критичної інфраструктури, а на регіональному та місцевому – понад 33 тисячі [300].

Цю думку підтверджує також В. О. Євсєєв [45, с. 170], який зауважує, що світова практика демонструє доцільність включення до сфери критичної інфраструктури об'єктів, які можуть стати потенційними цілями терористичних атак, а також тих, що підлягають охороні під час надзвичайних ситуацій та в особливий період, і стратегічно важливих підприємств для економіки та безпеки. До них належать державні установи,

органи місцевого самоврядування, об’єкти, що охороняються за контрактами з Державною службою охорони, радіаційно небезпечні об’єкти, аварійно-рятувальні служби, системи екстреного реагування, платіжні системи, Національна система конфіденційного зв’язку, об’єкти культурної спадщини.

Критичність інфраструктурного об’єкта визначається не лише масштабом потенційних наслідків його виведення з ладу, але й впливом на життєдіяльність суспільства та держави. При цьому враховується спектр наслідків, включно з екологічними, економічними, соціальними, фінансовими, техногенними чинниками, а також тривалість негативного впливу та можливість відновлення.

Відповідно, об’єкти критичної інфраструктури визначаються як такі, що у разі ураження, зокрема через елементи критичної інформаційної інфраструктури, можуть призвести до наслідків, які безпосередньо впливають на національну безпеку – у контексті безпеки особи, суспільства та держави [9] (рис. 1.7).

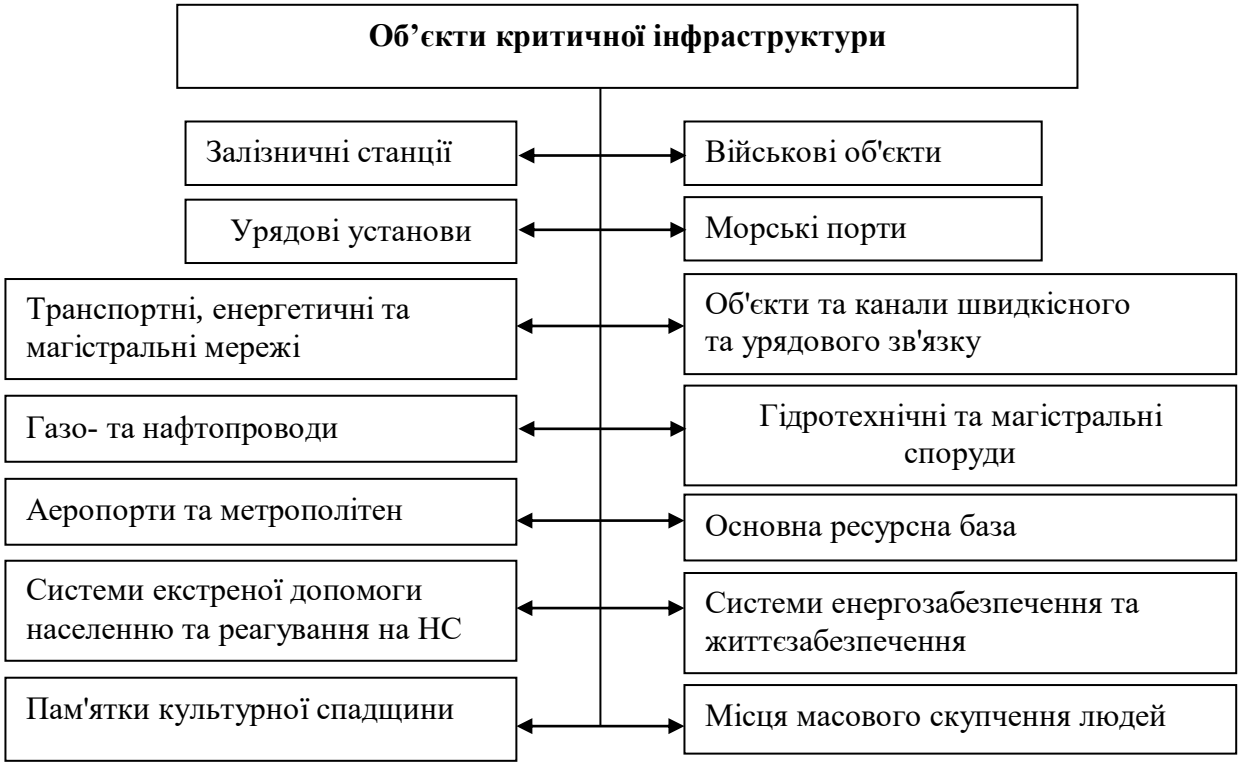


Рис. 1.7. Об’єкти критичної інфраструктури
Джерело:сформовано на основі [1]

На думку дослідників Бірюкова Д.С. і Кондратова С.І., об’єкти критичної інфраструктури класифікуються за рівнем значущості на місцеві, регіональні та загальнодержавні. Вони також пропонують ієрархію сфер критичної інфраструктури за основними групами, зокрема: охорона здоров’я та безпека життєдіяльності населення, економічна безпека, обороноздатність і національна безпека, імідж і гідність держави [9, с. 110].

Проведений аналіз нормативно-правових актів зарубіжних країн дозволяє зробити висновок, що більшість із них виділяє 12 ключових

секторів критичної інфраструктури. До найважливіших серед них, які визнані у переважній більшості держав, належать: фінансовий сектор (24 із 29 країн), енергетика (29 із 29), транспорт (29 із 29), водопостачання (24 із 29), а також інформаційні та телекомунікаційні технології (27 із 29).

В українському правовому полі наразі функціонують нормативні документи, що визначають окремі категорії об'єктів, які підлягають посиленому захисту. До них належать:

– підприємства, що мають стратегічне значення для економіки та безпеки [205];
– об'єкти підвищеної небезпеки [64];
– важливі державні об'єкти [203];
– об'єкти, які охороняються за договорами підрозділами державної служби охорони [213];
– об'єкти, що підлягають захисту в умовах надзвичайного стану та в особливий період [64];
– особливо важливі енергооб'єкти [229];
– об'єкти нафтогазового сектору, що мають особливе значення [204];
– система національного конфіденційного зв'язку [63];
– платіжні системи [70];
– система екстреного реагування за номером 112 [71];
– аварійно-рятувальні служби [90];
– нерухомі об'єкти культурної спадщини [69].

Таким чином, аналіз міжнародного законодавства і наукових підходів до ідентифікації критичної інфраструктури вказує на необхідність більш детальної класифікації таких об'єктів у контексті формування державної політики їх захисту. Орієнтація на міжнародний досвід у визначенні критеріїв критичності дає змогу Україні адаптувати підходи до забезпечення безпеки об'єктів, враховуючи як потенційні ризики для громадян, так і масштаби можливих наслідків.

Важливим критерієм є також міжсекторальна взаємозалежність об'єктів критичної інфраструктури, що проявляється у так званому «каскадному ефекті». Збої або вихід з ладу одного об'єкта можуть ініціювати системні порушення у функціонуванні інших, пов'язаних об'єктів. Наприклад, виведення з ладу енергетичних об'єктів спричиняє припинення подачі води або зупинку телекомунікацій. Порушення зв'язку, своєю чергою, унеможливлює управління, контроль і функціонування низки інших систем, таких як банківські апарати. Згідно з науковими підходами, об'єкти за рівнем критичності поділяють на три категорії: високий, середній та низький, хоча в окремих методиках можливі варіації цих рівнів.

До категорії критичної інфраструктури можуть бути віднесені лише ті об'єкти, які мають надзвичайне значення для національної безпеки. У міжнародній практиці сформовано три ключові напрями захисту критичної інфраструктури:

1. захист від загроз у сфері державної безпеки, включаючи внутрішні

ризики та фізичне знищення об’єктів;

2. протидія кіберзагрозам;

3. реагування на надзвичайні ситуації.

Таким чином, критична інфраструктура – це сукупність об’єктів, порушення функціонування яких може спричинити незворотні наслідки для життєдіяльності держави, здоров’я та безпеки її громадян, а також соціально-економічної стабільності. Стійке функціонування критичної інфраструктури є основою забезпечення національної безпеки та стабільності економіки.

Тривала відсутність у національному законодавстві чіткого визначення поняття «критична інфраструктура» та переліку відповідних об’єктів створювала значні інституційні бар’єри для формування ефективної системи безпеки в цій сфері. Вперше термін «критична інфраструктура» на офіційному рівні був згаданий у «Рекомендаціях парламентських слухань з питань розвитку інформаційного суспільства» у 2006 році [240]. У подальшому, в Стратегії національної безпеки України 2012 року «Україна у світі, що змінюється» [240] цей термін використовувався у вузькому контексті – лише щодо енергетичної та інформаційної безпеки.

Більш комплексний підхід до питання критичної інфраструктури було реалізовано у рішенні РНБО від 01.03.2014 р. «Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України» [226], у якому МВС доручалося посилити охорону об’єктів енергетики та критичної інфраструктури. Проте, окреме згадування енергетичних об’єктів поряд із критичною інфраструктурою, на нашу думку, є помилковим, оскільки ці об’єкти логічно входять до складу критичної інфраструктури. Водночас, юридичне визначення поняття у документі відсутнє.

Указ Президента від 26.05.2015 р. № 287/2015 [266] також серед загроз національній безпеці України визначив загрози для критичної інфраструктури. У новій редакції Стратегії національної безпеки України «Безпека людини – безпека країни» [265] зазначено, що серед актуальних загроз є погіршення технічного стану критичної інфраструктури, нестача інвестицій у її оновлення, несанкціоноване втручання, зокрема кібер- та фізичного характеру, а також ризики, зумовлені бойовими діями і тимчасовою окупацією частини території України.

У рамках співпраці з експертами країн-членів НАТО при Національному інституті стратегічних досліджень було підготовлено проєкт «Зеленої книги з питань захисту критичної інфраструктури в Україні» [169], оприлюднений у жовтні 2015 року. У цьому документі під критичною інфраструктурою України розуміються фізичні або віртуальні системи й ресурси, які забезпечують виконання ключових функцій і послуг, зупинка яких може спричинити найсерйозніші негативні наслідки для життєдіяльності суспільства, економічного розвитку та національної безпеки [79, с. 15].

Інституційне визначення поняття «критична інфраструктура» в Україні було закріплене у постанові КМУ № 563 від 23.08.2016 р. «Про затвердження

Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» [210]. У ній критична інфраструктура тлумачиться як сукупність об'єктів, які мають ключове значення для економіки, промисловості, функціонування суспільства й безпеки громадян, виведення з ладу яких може вплинути на національну безпеку, оборону, довкілля, призвести до значних економічних втрат або людських жертв.

Згодом у розпорядженні КМУ № 1009-р від 06.12.2017 р. «Про схвалення Концепції створення державної системи захисту критичної інфраструктури» [230] поняття критичної інфраструктури було уточнено й звужено. Згідно з новим формулюванням, вона становить сукупність об'єктів, які мають стратегічне значення для економіки, безпеки держави, суспільства та населення, а порушення їхньої діяльності може завдати шкоди життєво важливим національним інтересам України [230].

Розглядаючи наукові підходи до визначення сутності та значення критичної інфраструктури, доцільно звернутися до позиції О. П. Єрменчука, який розглядає цей феномен як «систему надзвичайно важливих матеріальних і нематеріальних елементів національної інфраструктури, а також сукупність систем і активів, як фізичних, так і віртуальних, що забезпечують її стабільне функціонування та настільки важливі для країни, що їх виведення з ладу, руйнування або пошкодження (внаслідок реальних загроз) може призвести до загибелі людей, значних матеріальних втрат і критичних негативних наслідків для функціонування суспільства, соціально-економічного розвитку держави й національної безпеки» [46, с. 138].

Аналізуючи це визначення, підтримуємо позицію Д. С. Бірюкова, який вважає, що такий підхід є актуальним з огляду на пріоритет надання життєво важливих для суспільства, особи та держави функцій і послуг [8, с. 160]. Водночас слід зауважити, що наведене трактування не враховує системного характеру взаємозв'язків між елементами критичної інфраструктури, на який вже раніше зверталася увага. Саме ця системна ознака, на нашу думку, зумовлює масштабність можливих наслідків, що виявляються у вигляді так званого «каскадного ефекту» порушення функціонування елементів критичної інфраструктури. Подібний погляд поділяє і С. М. Чумаченко, який наголошує, що «множинність елементів критичної інфраструктури об'єднана зв'язками різного характеру, які формують спільну властивість системи, відмінну від властивостей її окремих елементів» [279, с. 43].

Узагальнюючи наукові концепції та положення чинного законодавства, можна виокремити ще одну принципову рису об'єктів критичної інфраструктури – їхня належність до загальної національної інфраструктури, яка являє собою інтегровану систему державного управління та інфраструктурних елементів, що забезпечують безперервне функціонування основних сфер життєдіяльності держави, економіки та суспільства. Таку позицію поділяє і О. П. Єрменчук, зазначаючи, що критична інфраструктура формується шляхом виокремлення в наявних інфраструктурних системах

держави тих елементів, які є життєво важливими для її існування [46, с. 139]. Ці системи відображені, зокрема, у статті 1 Закону України «Про основи національної безпеки України» [67]. Отже, при формуванні державної політики у сфері захисту критичної інфраструктури її зміст доцільно ґрунтувати на узгодженні з положеннями національного законодавства як у сфері безпосереднього захисту критичної інфраструктури, так і національної безпеки та оборони в цілому.

Кульмінаційним етапом нормативного осмислення поняття «критична інфраструктура» стало ухвалення Закону України «Про критичну інфраструктуру» [60], підписаного Президентом після прийняття Верховною Радою 16 лютого 2021 року. У зазначеному нормативному акті термін «критична інфраструктура» подано у спрощеній формі як «сукупність об'єктів критичної інфраструктури», а самі об'єкти визначаються як «системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам» [60]. Проте варто звернути увагу, що чинна редакція закону демонструє переважання технократичного підходу, де в центрі визначення опиняється економічна складова. Такий підхід, на нашу думку, суперечить статті 3 Конституції України, де вказано, що «людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю» [99].

Отже, здійснений аналіз наукових підходів до дефініції «критична інфраструктура» дозволяє виявити фрагментарність її змістовного наповнення та недостатню системність у відображенні характерних ознак цього поняття. Враховуючи це, доцільно переглянути семантичну структуру термінології в галузі національної безпеки, орієнтуючись на антропоцентричну й гуманітарну парадигму. Відповідно, варто акцентувати увагу на необхідності включення до складу критичної інфраструктури тих об'єктів, порушення функціонування яких може спровокувати незворотні негативні процеси в державі, що призведуть до загроз життю, здоров'ю громадян, а також суттєво ускладнять соціально-економічну ситуацію [244].

Аналіз наукових доробків учених а також врахування закордонного досвіду теоретизування предикату «критична інфраструктура», дає підстави ініціювати авторське бачення змістовного наповнення даного терміну що буде відповідати принципам системності, множинності галузей, пріоритетної тріади людина-суспільство-держава, цілеспрямованості, відповідності антропоцентричного аспекту.

Так критичну інфраструктуру пропонуємо розуміти як «множинність розташованих в межах території країни функціонально пов'язаних елементів національної інфраструктури чи їх частини у вигляді фізичних, організаційних інформаційно-комунікаційних структур (незалежно від форми власності), технологій, активів, засобів, систем, мереж, поставок, процесів та фахівців які ними управляють, які є вирішальними для забезпечення

державою життєво важливих для суспільства функцій (здоров'я, захищеності, соціально-економічного благополуччя громадян, забезпечення суверенітету та сталого розвитку країни) порушення функціонування, знищення, збій або дисфункція у роботі яких матиме критичний вплив на здатність влади забезпечувати вказані функції та може спричинити виникнення людських жертв, значних матеріальних та екологічних збитків, інших драматичних наслідків та призведе до суттєвого порушення національної безпеки й оборони» [284]. Отже, авторське бачення у приведеному формулюванні дозволяє акцентувати приналежність критичних об'єктів до національної інфраструктури, а надання її складовим життєво важливих характеристик, свідчить про існування загроз до виникнення кризових ситуацій у національній безпеці.

Віднесення інфраструктурних об'єктів до категорії критичних здійснюється на основі сукупності критеріїв, що відображають їх значущість у забезпеченні критично важливих послуг та життєво необхідних функцій, а також враховують тривалість часу, необхідного для подолання наслідків порушення їх функціонування до моменту відновлення стабільного режиму роботи. Серед основних критеріїв виділяють:

– реалізацію функцій, що забезпечують національні життєво важливі інтереси;

– наявність специфічних загроз, орієнтованих на об'єкти критичної інфраструктури;

– ризики порушення базових умов життєдіяльності населення;

– ступінь вразливості об'єктів критичної інфраструктури та ймовірні наслідки для здоров'я населення, соціальної сфери, економіки, довкілля, обороноздатності й міжнародного іміджу держави;

– масштаб негативного впливу на діяльність стратегічно важливих секторів або втрату унікальних національно значущих ресурсів і систем, що матимуть тривалий ефект для суміжних секторів;

– терміни ліквідації руйнівних наслідків та тривалість негативного впливу на функціонування інших галузей;

– каскадний вплив на взаємопов'язані сектори критичної інфраструктури [60].

Результати досліджень засвідчують, що державна політика у сфері захисту критичної інфраструктури базується на низці ключових положень:

– визнання необхідності забезпечення стійкості та захищеності критичних об'єктів;

– формулювання законодавчих засад і принципів щодо визначення стратегічних пріоритетів у сфері захисту критичної інфраструктури;

– ідентифікація суб'єктів національної системи захисту, визначення їх повноважень, відповідальності та механізмів взаємодії;

– створення умов для реалізації заходів зі зменшення ризиків, моніторингу загроз і ліквідації наслідків кризових ситуацій;

– запровадження системи раннього виявлення загроз критичній

інфраструктурі;

– розвиток державно-приватного партнерства для залучення суб'єктів господарювання та громадян до процесу забезпечення безпеки критичної інфраструктури;

– активізація міжнародної співпраці у напрямі підвищення стійкості об'єктів;

– створення умов для швидкого відновлення функцій критичної інфраструктури у разі їх порушення або знищення.

Отже, стратегічна мета державної політики у цій сфері полягає у формуванні цілісної системи інституційних, правових, організаційних, ресурсних, інженерно-технічних та інформаційно-аналітичних заходів, що забезпечуватимуть захист критичних об'єктів від широкого спектра загроз. Серед основних проблем державного регулювання у сфері захисту критичної інфраструктури в Україні слід виокремити: затяжну інституційну невизначеність щодо структури системи захисту й реагування на надзвичайні ситуації, а також відсутність цілісної та узгодженої нормативно-правової бази, яка б чітко розмежовувала повноваження державних органів. Зазначимо також неузгоджене використання термінології, як-от: «критична інфраструктура», «національна інфраструктура», «критично важливі об'єкти» чи «життєво важлива інфраструктура», що породжує правову та інституційну невизначеність.

Водночас, критичну інфраструктуру варто розглядати як структурний елемент національної інфраструктури, який забезпечує ключові функції життєдіяльності держави. Аналіз міжнародних законодавчих підходів до визначення поняття «критична інфраструктура» дозволяє стверджувати, що в його основі лежить ціннісна тріада: «людина – суспільство – держава». Це означає, що йдеться про об'єкти, безпека яких є фундаментально важливою для збереження соціальної стабільності, економічної безпеки та національного суверенітету. Водночас, певні інфраструктурні об'єкти можуть мати символічну цінність, адже їх руйнування може викликати соціальну та емоційну дестабілізацію в суспільстві, порушити відчуття національної ідентичності та вплинути на загальносуспільну психологічну стійкість.

1.3. Теоретико-методичні основи забезпечення захисту критичної інфраструктури

У процесі гарантування державою сталого життєзабезпечення та безпеки суспільства особливого значення набуває мінімізація вразливості критично важливих систем, що зумовлює актуальність наукового обґрунтування напрямів державної політики у сфері захисту об'єктів критичної інфраструктури. Продовжуючи цю наукову думку, варто звернутися до положення, запропонованого вченими С. В. Бєлаєм, І. В. Євтушенко та В. В.

Мацюком, згідно з яким «державна політика у сфері захисту критичної інфраструктури повинна бути спрямована на формування комплексу організаційних, нормативно-правових, інженерно-технічних, експлуатаційних, наукових та інших заходів, що сприяють забезпеченню безпеки та стійкості критичної інфраструктури» [5, с. 344].

Відтак, дослідження державної політики у цій сфері потребує окреслення спектру загроз, наявність яких і обумовлює потребу в її розбудові. У цьому контексті доцільно звернути увагу на Європейську програму захисту критичної інфраструктури [292], у якій члени Комісії Європейських Спільнот наголошують на ключових загрозах, що можуть пошкодити, знищити або вивести з ладу об'єкти критичної інфраструктури. Серед таких небезпек визначаються: терористичні акти, стихійні лиха, недбалість, виробничі аварії, хакерські атаки, злочинна діяльність і зловмисні дії [292].

Таким чином, стратегічний вектор державної політики має бути зосереджений на забезпеченні безперебійного функціонування критичної інфраструктури з метою захисту життя, здоров'я і майна населення від загроз порушення її роботи. У цьому аспекті доцільно розглядати безпеку об'єктів критичної інфраструктури через призму їхньої інфраструктурної адаптивності та керованості як складову сучасної парадигми державного управління. Вважаємо, що в цьому контексті необхідне впровадження політики «експлуатаційної ефективності» – раціоналізації розподілу та використання державних ресурсів безпеки з метою локалізації та нейтралізації потенційних джерел загроз. При цьому важливо робити акцент не стільки на ефективності окремих елементів системи, скільки на стратегії міжсистемної та міжсекторальної взаємодії [293].

Звернемо увагу на обґрунтування типології загроз для критичної інфраструктури. Починаючи з 1990-х років, у наукових колах Європи та США спостерігається активне вивчення поняття «захист критичної інфраструктури», що надалі отримало відображення у численних наукових працях та нормативно-правових актах багатьох країн. Захист критичної інфраструктури, як відомо, передбачає передусім протидію загрозам.

У чинному законодавстві України термін «загроза» визначається в Законі України «Про національну безпеку» як «явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України» [62]. У контексті захисту критичної інфраструктури Д. Г. Бобро трактує загрозу як «наявні та потенційно можливі явища та чинники, що створюють небезпеку сталому функціонуванню об'єктів критичної інфраструктури та можуть призвести до негативних наслідків» [11, с. 85]. Це визначення вважаємо обґрунтованим, оскільки воно акцентує на забезпеченні стійкості функціонування об'єктів.

Подібне трактування міститься й у «Зеленій книзі» ЄС із захисту критичної інфраструктури, де загрози визначаються як «будь-які обставини

або події, що можуть порушити стале функціонування або знищити критичну інфраструктуру чи будь-який її елемент, а також будь-які спроби та наміри завдати шкоди критичним активам» [292, с. 55]. Аналогічну позицію займає і О. П. Єременчук, який пропонує розглядати загрози об'єктам критичної інфраструктури як «наявні або потенційно можливі явища і чинники, що можуть завдати шкоди такому об'єкту (фізичному або у кіберпросторі), вивести його з ладу або порушити стійкість функціонування відповідно до призначення, чим створюють небезпеку життєво важливим національним інтересам України» [48, с. 108].

Таким чином, підтримуючи позиції як вітчизняних учених, так і європейських експертів, визначаємо забезпечення стійкості функціонування об'єктів критичної інфраструктури як ключовий пріоритет державної політики у цій сфері.

Більшість дослідників [1, с. 55; 2, с. 512; 5, с. 343] вважає, що США стали першопрохідцями у формуванні й реалізації концепції критичної інфраструктури та її захисту. Ця держава й надалі утримує провідні позиції у зазначеній сфері завдяки впровадженню ефективних державних управлінських підходів, розвиненій інформаційно-аналітичній підтримці процесу прийняття рішень, використанню інноваційних технологій та широкому спектру інструментів і методів забезпечення безпеки.

Узагальнюючи розглянуті визначення, простежується концентрація на дослідженні загроз і ризиків, що можуть дестабілізувати роботу критичної інфраструктури на різних ієрархічних рівнях. Нормативно-правова база США конкретизує ці загрози залежно від їх джерел, зокрема як: «природні або техногенні явища, дії фізичних осіб або суб'єктів, що містять потенційну шкоду для життя, інформації, операцій, довкілля та/або власності» [46, с. 137].

В умовах динамічного та нестабільного макросередовища, яке породжує широкий спектр загроз і викликів для державної політики безпеки, актуалізується необхідність активної участі державних інституцій у процесі виявлення, прогнозування та нейтралізації таких загроз. Перелік основних із них представлений у Стратегії національної безпеки України (2020) [256], а також у ст. 19 Закону України «Про національну безпеку» [62] і ст. 24 Закону України «Про критичну інфраструктуру» [180]. До базових загроз, що постають перед об'єктами критичної інфраструктури, відносять: воєнні загрози, розвідувально-підривну діяльність, тероризм, кіберзагрози, економічні загрози, витік державної таємниці, надзвичайні ситуації, технічні аварії та збої, а також кризові явища. Д. М. Павлов пропонує доповнити цей перелік такими викликами, як гібридні війни, сепаратизм, техногенний тероризм і ворожа колаборація [180, с. 147].

Звертаючи увагу на потребу врахування актуальних умов, пов'язаних із воєнним станом в Україні, слід наголосити на необхідності інтеграції цих чинників у процес розробки державної стратегії захисту критичної інфраструктури. У цьому контексті науковці, аналізуючи пошкодження

інфраструктурних об’єктів у період збройних дій, окреслюють дві основні категорії впливів:

– по-перше, навмисні дії, що мають на меті дестабілізувати або припинити функціонування інфраструктури;

– по-друге, непрямі або ненавмисні впливи, які виникають внаслідок бойових дій, зокрема у випадку неточних ударів.

Відповідно до класифікації П. П. Богуцького, рівень деструктивного впливу поділяється на такі форми: зупинка функціонування через фізичне захоплення об’єктів з метою завдання шкоди або отримання переваг; окупація з подальшим використанням інфраструктури; демонтаж складових частин з метою їх продажу; перешкоджання відновленню об’єктів; та повне фізичне знищення, що несе економічні та соціально-політичні наслідки [15, с. 280]. У контексті гібридних загроз уразливість критичної інфраструктури проявляється через низку факторів, зокрема, дискредитацію державної спроможності гарантувати безпеку, психологічний тиск, економічні втрати, атаки дронів і артилерії, кібератаки та приховані диверсійні дії з елементами тероризму [1, с. 242]. Такі методи підриву життєзабезпечення та саботажу інфраструктурної спроможності виконувати свої функції розглядаються як елемент гібридної війни, спрямованої на психологічне виснаження населення та політичний тиск на уряд. Відповіддю на ці виклики має стати інституціоналізація систем безпеки. Вітчизняні дослідники [100, с. 18], звертаючись до філософського розуміння безпеки, підкреслюють її універсальність, яка охоплює всі рівні існування – особистий, соціальний та державний.

Історичні витоки концепції безпеки простежуються у працях мислителів античності, таких як Платон, Арістотель, Епікур, Ціцерон та Лукрецій, які розглядали її як стан душевного спокою, досяжного лише за умов захищеності від зовнішніх загроз [321, с. 54]. У «Політологічному енциклопедичному словнику» безпека трактується як сукупність дій, спрямованих на виявлення, нейтралізацію та запобігання загрозам, здатним завдати шкоди особі, суспільству чи державі, блокувати прогрес і позбавити цінностей [189, с. 47]. Сучасна наукова думка зосереджується на трьох вимірах безпеки: концептуальному – що поєднує онтологічні та епістемологічні підходи; практичному – який визнає безпеку базовою потребою; та ціннісному – де акцент зроблено на гносеології та культурі безпеки. Наукове розуміння безпеки здебільшого формулюється як еклектичний стан, що передбачає сукупність запобіжних і реагуючих заходів [100]. Польський дослідник А. Д. Родфельд зауважує, що поняття безпеки є динамічним і змінюється залежно від національного та глобального контексту [345, с. 15]. М. Гладиш додає, що національні уявлення про безпеку не завжди збігаються з глобальними, а дії однієї держави можуть сприйматися як агресивні її сусідами [25, с. 30], що підтверджує і Б. Посен [337, с. 18]. Вітчизняні вчені трактують захист критичної інфраструктури як цілісний комплекс нормативно-правових, технологічних та організаційних

заходів, спрямованих на забезпечення її безпечного функціонування [79, с. 11], з чим погоджується також С. С. Теленик, акцентуючи на пріоритетності стійкості [258, с. 183].

Досвід США, зафіксований у Директиві з національної безпеки, демонструє, що захист критичної інфраструктури передбачає зменшення ризиків через фізичні та кіберзаходи [300]. О. П. Єременчук підкреслює, що така система має включати широку сукупність заходів – від організаційних до технічних – що сприяють підвищенню стійкості об'єктів [46, с. 37].

Закон України «Про критичну інфраструктуру» [60] визначає її захист як комплекс дій, здійснюваних на всіх етапах функціонування, спрямованих на запобігання та мінімізацію загроз [62]. Попри актуальність цього визначення, воно недостатньо враховує участь недержавних суб'єктів – власників і операторів – які володіють більшістю інфраструктурних об'єктів. Відтак, доцільним є розширення кола відповідальних за межі державних структур через ефективну міжвідомчу координацію. Підтвердженням цього є Національна стратегія Канади, яка покладає основну відповідальність за регенерацію інфраструктури саме на її власників [313, с. 8].

У цьому зв'язку пропонується авторська дефініція поняття «захист критичної інфраструктури» як скоординованої діяльності всіх залучених сторін із реалізацією комплексу дій, спрямованих на забезпечення стійкості, запобігання та ліквідацію наслідків загроз, а також відновлення функціональності об'єктів задля запобігання людським втратам і національним ризикам [283]. Це визначення змінює акцент державної безпекової політики з реагування на загрози на їхню попереджувальну нейтралізацію, одночасно забезпечуючи баланс відповідальності між державними структурами та приватними суб'єктами.

Доцільно підкреслити, що впродовж тривалого часу в українському правовому полі відсутній єдиний централізований інститут, відповідальний за формування та реалізацію державної політики у сфері захисту критичної інфраструктури. Наразі охорона таких об'єктів здійснюється фрагментарно, за участі окремих органів сектору безпеки, зокрема Міністерства оборони України, Державної служби з надзвичайних ситуацій (ДСНС), Служби безпеки України (СБУ), Міністерства закордонних справ (МЗС) та Міністерства охорони здоров'я (МОЗ). При зазначених структурах функціонують відповідні центри оперативного реагування, такі як Ситуаційний центр Головного командного пункту Збройних сил України, Ситуаційний центр ДСНС та Антитерористичний центр при СБУ, який координує взаємодію органів виконавчої влади з питань запобігання та припинення терористичних актів. Водночас відсутність чіткої міжвідомчої координації їх дій і ресурсів породжує низку організаційних проблем. Крім того, деякі повноваження у цій сфері мають також інститути боротьби з тероризмом, органи цивільного захисту, суб'єкти регулювання енергетичного сектору, ринку енергоресурсів та кібербезпеки. У цьому контексті заслуговує на увагу ефективна модель захисту критичних секторів, реалізована у США, де за безпеку окремих

напрямів відповідають спеціалізовані галузеві установи, зокрема департаменти внутрішньої безпеки, енергетики, сільського господарства, охорони здоров'я, а також берегова охорона та управління безпеки транспорту [256, с. 362].

Отже, однією з ключових передумов ефективної реалізації державної політики у сфері захисту критичної інфраструктури є потреба в розробці та актуалізації нормативно-правових актів, що регламентують державну систему захисту об'єктів, із акцентом на підвищення їхньої стійкості та впровадження превентивних заходів. Кожна стратегічна інституція держави в межах власної компетенції фіксує перелік потенційних загроз для підпорядкованих їй інфраструктурних об'єктів, а також володіє відповідними ресурсами для їхнього захисту як у мирний період, так і в умовах збройної агресії. Відповідно до позиції науковців Д. С. Бірюкова та С. І. Кондратова [9, с. 110], ефективна діяльність інституту захисту критичної інфраструктури повинна ґрунтуватися на системному аналітичному підході, що передбачає:

– ідентифікацію критичних секторів на різних рівнях управління;
– визначення відповідних ризиків;
– аналіз їхньої уразливості;
– оцінку ймовірності порушень або знищення;
– впровадження заходів запобігання через створення системи захисту інфраструктури.

У підсумку, значущість функціонування стратегічного державного інституту у сфері захисту критичної інфраструктури обґрунтовується кількома положеннями: такі об'єкти є критично важливими для функціонування держави та суспільства, особливо у кризовий час; інфраструктура виступає інструментом у геополітичній конкуренції; та має ознаки об'єктів підвищеної небезпеки як на національному, так і глобальному рівнях.

Аналіз різноманітних наукових підходів дає підстави стверджувати про критичну важливість виявлення та попередження ризиків у системі управління безпекою критичної інфраструктури. Такий підхід передбачає виконання на загальнодержавному рівні низки завдань, серед яких ключовим є розробка та інтеграція відповідних превентивних заходів у документи державного планування. Головною метою цих дій є зниження ймовірності виникнення нових ризиків і мінімізація вже наявних шляхом реалізації комплексного спектру заходів, охоплюючи національний, регіональний і місцевий рівні. У цьому контексті визначальними виступають: глибоке розуміння природи ризиків, вдосконалення інституційно-правових механізмів ризик-менеджменту, інвестування в запобіжні заходи та посилення потенціалу реагування на ризики.

Цю тезу підтверджують наукові дослідження колективу авторів під керівництвом С. І. Азарова, які пропонують чотиристадійну модель розвитку надзвичайних ситуацій на об'єктах критичної інфраструктури. Перша стадія – накопичення факторів ризику – відбувається у джерелі небезпеки, і цей процес може тривати тривалий період – від кількох діб до десятиліть. Друга – ініціація надзвичайної ситуації, тобто момент запуску деструктивного

сценарію, коли фактори ризику досягають критичної межі та набувають незворотного характеру. Третя – перебіг самої надзвичайної ситуації, у ході якої відбувається вивільнення енергії або речовин, що чинять вплив на довкілля, суспільство та технічні об'єкти. Четверта – стадія затухання, яка охоплює період від локалізації загрози до усунення її безпосередніх і опосередкованих наслідків [1, с. 276].

У межах державної політики захисту критичної інфраструктури важливим є також глибоке розуміння поняття «ризик», яке виступає міждисциплінарною категорією та застосовується у природничих, соціальних, технічних і економічних науках. Для безпеки інфраструктурних об'єктів доцільно класифікувати ризики за такими видами: соціальні, професійні, техногенні, екологічні, військові тощо. Таким чином, ризик можна визначити як «міру цілком певних небезпек» [104, с. 5].

Під ризиком слід розуміти ймовірність або частоту настання небезпек певного характеру, обсяг можливих збитків або комбінацію цих характеристик. На думку В. В. Вітлінського та Г. І. Великоіваненка, ризик є ситуацією невизначеності з наявністю конфлікту та множинних альтернатив, жодна з яких не гарантує однозначно позитивного результату [22, с. 68]. Л. І. Донець акцентує на необхідності прийняття управлінського рішення у ситуації аморфності, коли існує можливість кількісної та якісної оцінки імовірностей як успіху, так і невдачі [42, с. 212]. І. М. Посохов у свою чергу підкреслює, що ризик є обов'язковою умовою будь-якої дії з потенційно несприятливим результатом [190, с. 105].

Узагальнюючи наукові позиції, можна сформулювати таке визначення ризику в управлінні безпекою критичної інфраструктури: це ймовірність виникнення аварійної ситуації, небезпеки, катастрофи чи іншої деструктивної події, що ускладнює функціонування об'єктів критичної інфраструктури за умов невизначеності та потреби прогнозування альтернатив розвитку ситуації.

У процесі формування протоколів технологічної безпеки та аналізу ризиків особлива увага приділяється системному врахуванню й дослідженню диференційованих факторів, що впливають на рівень ризику, в межах так званого ризик-аналізу. Наукове трактування поняття «аналіз ризику» полягає в розгляді його як процесу ідентифікації небезпек та оцінки ризику для окремих осіб, груп населення, об'єктів критичної інфраструктури та інших потенційно вразливих цілей [237, с. 123]. На основі різних підходів поняття ризику у сфері управління безпекою критичних об'єктів може бути витлумачене як імовірність реалізації небезпеки, аварії, надзвичайної ситуації або катастрофи під час виконання інфраструктурою своїх функцій за умов невизначеності та потреби прогнозування альтернатив [285, с. 125].

Багатогалузевий характер критичної інфраструктури та її інтеграція у численні сфери суспільного життя обумовлює складність управління ризиками в цій царині. Особливість критичного ризик-аналізу полягає в тому, що він включає потенційні негативні наслідки, спричинені аварійністю

технічних систем або помилками персоналу. Результати такого аналізу мають ключове значення для обґрунтування управлінських рішень щодо розміщення і проєктування інфраструктурних об'єктів, що, у свою чергу, актуалізує потребу в запровадженні ефективного ризик-менеджменту. В. О. Мусієнко визначає ризик-менеджмент як процес прийняття управлінських рішень, спрямованих на зниження ймовірності реалізації негативних наслідків та мінімізацію можливих втрат [118, с. 102].

Вчені Н. С. Скопенко та І. В. Євсєєв-Северин обґрунтовують необхідність інтеграції ризик-менеджменту в систему захисту критичної інфраструктури, вказуючи не лише на важливість мінімізації наслідків, але й на запобігання їхньому виникненню шляхом розробки превентивних заходів [237, с. 125]. Важливим є і погляд науковців С. П. Потеряйка, К. Г. Бєлікова, О. С. Твердохліба, які пропонують включити до системи управління ризиками чотири ключові механізми: правовий, організаційний, структурно-функціональний та прогнозування [221, с. 44]. Саме останній, за їхніми словами, становить сукупність методів, норм і важелів, що дозволяють органам управління оцінювати ефективність безпекових структур і приймати обґрунтовані рішення у коротко-, середньо- та довгостроковій перспективі [221, с. 45].

Отже, доцільно розглядати критичний ризик-менеджмент як невід'ємний елемент державної політики у сфері захисту інфраструктури. Його сутність полягає у реалізації комплексу заходів, спрямованих на мінімізацію потенційних загроз стабільності функціонування об'єктів, недопущення надзвичайних ситуацій і планування дій з локалізації можливих наслідків. Оскільки управління ризиками в умовах невизначеності неможливе без чіткої аналітичної основи, необхідно враховувати чинники економічного, соціального та правового характеру, а також використовувати методи прогнозування. Державна політика в цьому напрямі має орієнтуватися на оцінку альтернативних сценаріїв, враховуючи ризики та прогнозуючи їхні наслідки. Це передбачає виконання багатокритеріальних завдань перед ухваленням управлінських рішень. Оцінка ризику є центральною віссю для формування ефективної моделі ризик-менеджменту, що потребує розробки адаптивних алгоритмів моделювання аварійних процесів з метою підготовки персоналу до дій у реальних умовах.

Для опису ризикових сценаріїв як просторово-часових процесів на критично важливих об'єктах І. Г. Фадєєва та О. І. Гринюк пропонують використовувати три критерії: чітка ідентифікація події, яка є джерелом загрози; визначення ймовірності її настання; та рівень потенційної мінімізації наслідків [273, с. 215]. Методологічно такий підхід оформлюється у вигляді послідовного алгоритму дій: опис поведінки систем, її пояснення, прогнозування, управління, а також конструювання систем із заданими характеристиками поведінки [1, с. 230]. Ця схема створює основу для розробки науково обґрунтованих заходів безпеки на основі адміністративно-правових інструментів у ситуаціях невизначеності.

О. О. Терещенко наголошує, що самі по собі ризики не є головною проблемою – критичною є саме їхня неконтрольованість, що виникає через нестачу інформації та затримки в управлінських рішеннях. Учений зазначає, що контроль за ризиками забезпечується шляхом впровадження внутрішнього аудиту та комплексної системи ризик-менеджменту [260]. У свою чергу М. Ф. Гончар пропонує відокремлювати ризик-менеджмент – як практику реагування на звичайні та незначні відхилення, – від стрес-менеджменту, який реалізовується в умовах критичних та екстремальних ситуацій, коли об'єкти інфраструктури зазнають значних відхилень від очікуваних траєкторій розвитку [30].

Прислухаючись до теоретичних положень, викладених О. Є. Кузьміним, О. Г. Мельником і М. Є. Адамівим, слід зазначити, що в умовах критичного дефіциту часових та інформаційних ресурсів, необхідних для прийняття обґрунтованих управлінських рішень, суттєво зростає ризик неадекватного реагування на зміни у функціонуванні об'єктів критичної інфраструктури. Вчені пропонують вихід із такої ситуації у вигляді впровадження антисипативного управління, яке базується на прогнозуванні ризиків як мікро-, так і макросередовища [103, с. 73]. Таке управління спрямоване на підготовку об'єктів до потенційно дестабілізуючих подій, здатних спричинити аномальні або екстремальні відхилення у їхній роботі. З огляду на це, особливої актуальності набуває проактивний підхід до ризик-менеджменту підприємств, орієнтований на недопущення розвитку кризових явищ.

Характерними особливостями сучасного державного управління безпекою критичної інфраструктури є важливість інформаційного забезпечення прогнозування ризикових подій у середньо- та довгостроковій перспективі, а також обмеженість часу для прийняття ефективних поточних управлінських рішень. Серед поширених методологічних підходів до оцінки та прогнозування ризиків науковці виокремлюють: скринінгові методи на основі лінійних дискримінантних функцій; моделі, побудовані на нечіткій логіці та нейромережах; імовірнісні моделі множинного вибору; інтегральні моделі на основі факторного аналізу, таксономічних індикаторів, адитивних або мультиплікативних згорток [89, с. 90].

Недостатність або повна відсутність статистичних даних про розвиток загроз для інфраструктурних об'єктів ускладнює застосування формалізованих моделей, побудованих на суворих припущеннях. Враховуючи це, доцільно застосовувати апарат нечіткої логіки для моделювання ризикових ситуацій у межах логіко-аналітичного підходу, що дозволяє ефективно управляти безпекою інфраструктури в умовах невизначеності. Теорія нечіткої логіки була предметом досліджень С. В. Козловського [92], О. В. Кочеткова, Т. О. Гаур, В. М. Машіна [100], А. В. Матвійчука [115] та ін. Цей підхід передбачає виділення ключових факторів стійкості, формалізацію їх взаємозв'язків, визначення лінгвістичних оцінок та оптимізацію параметрів моделі [115, с. 185].

У практичній площині, коли цілі, обмеження та наслідки не визначені чітко, доцільно застосовувати також апарат теорії ймовірностей, методи прийняття рішень, управління та інформаційні підходи. Це означає, що працівник змушений приймати інтуїтивні рішення, що містять припущення та елементи випадковості.

У цьому контексті слушною є позиція С. І. Ніколаюка, який розглядає кластерний аналіз як форму нечіткого аналізу, коли множина даних розбивається на кластери за відповідними функціональними ознаками [136, с. 285]. У ситуації з великою кількістю як об'єктивних, так і суб'єктивних факторів, що впливають на надзвичайну ситуацію, можливо побудувати алгоритм, який дозволить працівнику критичного об'єкта аналізувати ситуацію на основі раніше сформульованих критеріїв. Така алгоритмізація є ефективною за умов стабільного середовища, з обмеженою кількістю значущих вихідних даних і мінімізацією випадкових факторів.

Л. В. Дранишников і Є. О. Сугаль обґрунтовують концепцію «прийнятного ризику», згідно з якою повна безпека є недосяжною, а отже доцільно орієнтуватися на досягнення відносної безпеки шляхом встановлення аварійно-допустимого рівня ризику. Такий рівень має відповідати економічним, соціальним та технологічним наслідкам певної діяльності і узгоджуватись із принципами державної політики у сфері захисту критичної інфраструктури. При цьому ймовірність реалізації загроз і обсяг можливих збитків складно точно оцінити [43, с. 64]. З урахуванням цього варто звернутися до досліджень В. В. Гордіної, яка пропонує доповнити класичну систему управління ризиками інструментом ризик-контролінгу. Його основною функцією є надання інформаційно-аналітичної підтримки ризик-менеджменту з метою забезпечення комплексного управління [31, с. 33] (рис. 1.8.).

До ключових функцій ризик-контролінгу, за визначенням В. В. Гордіної, належать такі завдання:

– прогнозування потенційних ризиків і встановлення цільових орієнтирів показників;

– здійснення контролю за динамікою ризиків;

– підготовка аналітичної звітності щодо стану ризикових чинників для об'єктів критичної інфраструктури з подальшим інформуванням керівних структур;

– побудова ефективної системи виявлення, аналізу й оцінювання ризиків;

– забезпечення координації всіх етапів процесу управління ризиками як усередині окремих елементів системи, так і між ними;

– проведення консультацій з питань ризик-менеджменту [31, с. 33].

Для забезпечення точності оцінки та прогнозування ризиків, що становить головну мету системи ризик-контролінгу, І. Г. Фадєєва розробила каскадну нечітку модель Мамдані-типу. Ця модель дозволяє оцінити ймовірність виникнення ризиків у діяльності підприємств

нафтогазовидобувного сектору, що докладно описано в її науковій роботі [305, с. 260]. Основною перевагою запропонованого підходу є здатність встановлювати складні, неочевидні та нелінійні взаємозв'язки між вхідними та вихідними змінними, які часто не піддаються класичному формалізованому опису.

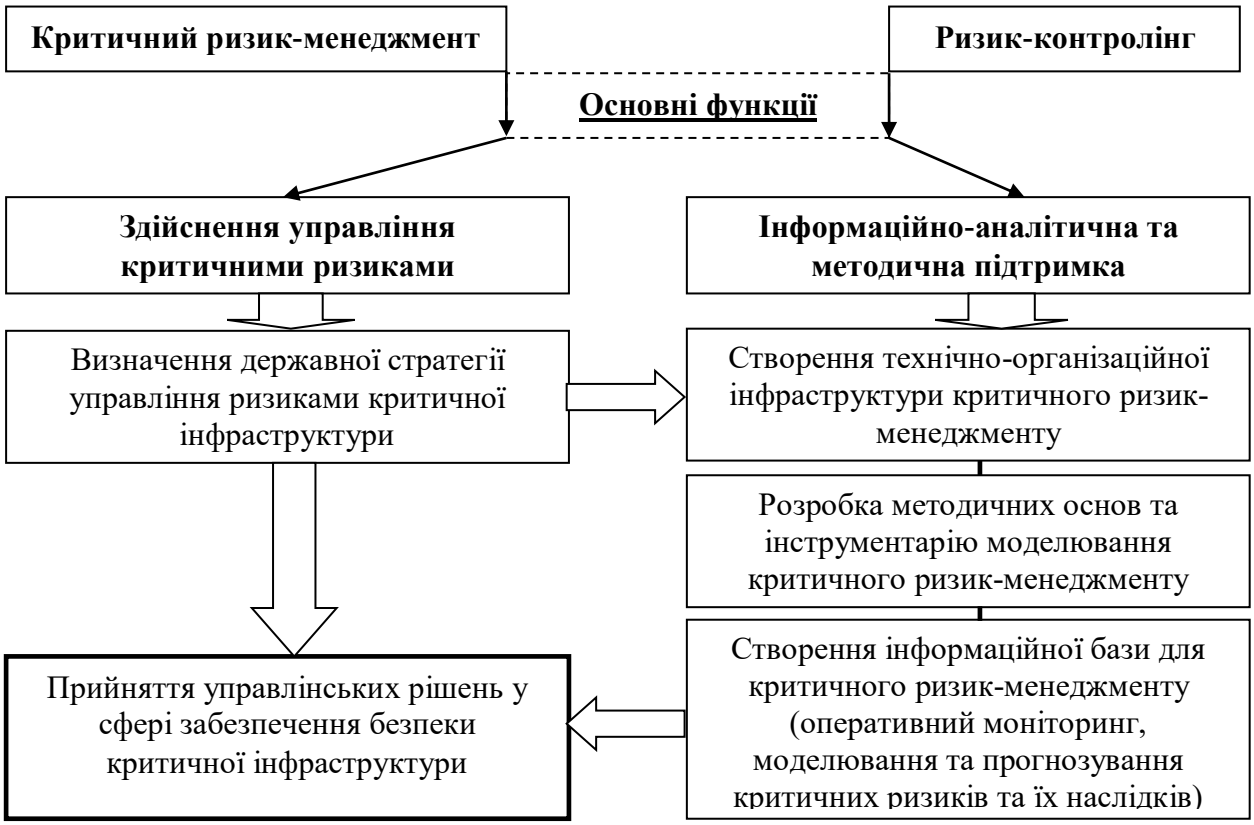


Рис. 1.8. Механізм прийняття управлінських рішень у сфері забезпечення безпеки критичної інфраструктури на основі критичного ризик-менеджменту

Джерело: сформовано автором з використанням [31],[273]

Ключовим поняттям у контексті цієї моделі є так звані ризикоутворюючі фактори – тобто ті процеси, явища або умови, які безпосередньо або опосередковано сприяють виникненню ризиків у функціонуванні об'єктів критичної інфраструктури (табл.1.1).

Таблиця 1.1 – Характеристика ризиків для об'єктів критичної інфраструктури

Вид ризику	Опис ризику
Ризики зниження ефективності захисту	Потенційна можливість зниження ефективності захисту об'єктів критичної інфраструктури
Ризики виникнення потенційних загроз	Можливість виникнення потенційних загроз для об'єктів критичної інфраструктури
Ризики нанесення збитків	Можливість нанесення потенційних збитків для об'єктів критичної інфраструктури або порушення умов їх нормального функціонування

Джерело: сформовано на основі [98]

Для формування висновків у системах нечіткої логіки пропонується низка алгоритмічних процедур, що базуються на структурованому підході до обробки даних через послідовність етапів. Серед таких етапів виокремлюють: створення бази даних нечітких регламентів висновку; фазифікацію вхідних змінних; синтез підумов нечітких умов та відповідних правил дії; композицію та активізацію підвисновків; акумулювання висновків із нечітких умов; та, нарешті, декомпозицію вихідних змінних.

Науковці О. В. Кочетков, Т. О. Гаур і В. М. Машін визначають оцінку ризику як процес, у ході якого встановлюється величина потенційних збитків у кількісній або якісній формі [98, с. 99]. Зростання складності та невизначеності зовнішнього середовища, його динамічність, турбулентність і низька передбачуваність обумовлюють необхідність упровадження сучасних управлінських моделей, зокрема стратегічного планування. Такі моделі мають забезпечити розробку стратегій розвитку об’єктів критичної інфраструктури на основі всебічного аналізу як зовнішніх умов, так і внутрішнього потенціалу підприємства.

Ключовим етапом у цьому процесі є визначення місії та стратегічних цілей інфраструктурного об’єкта. Цей етап, водночас концептуально важливий і практично складний, характеризується високим ступенем невизначеності, потребує спеціалізованих знань, експертної інтерпретації даних та прийняття рішень, що мають нечіткий, розмитий характер. Саме якісне виконання цієї процедури значною мірою визначає ефективність формування державної політики у сфері безпеки критичної інфраструктури та забезпечує її подальшу практичну реалізацію.

Одним із найактуальніших викликів сучасності є необхідність збору, концентрації та оперативної обробки релевантної інформації. Це ускладнюється просторовою розосередженістю об’єктів критичної інфраструктури. У зв’язку з цим доцільним є використання геоінформаційних систем і технологій, які надають змогу здійснювати просторово-часовий аналіз взаємозв’язків між об’єктами, враховуючи як зовнішній вплив, так і внутрішні процеси в межах кожного з них.

Ефективним інструментом у такому випадку виступає нечітке моделювання, яке дозволяє працювати з недостатніми або нечіткими знаннями про систему. Воно передбачає використання знаннєво-орієнтованих моделей, таких як продукційні правила, семантичні мережі, фрейми та формальні логічні структури. Застосування цих методів дає змогу створювати адаптивні, гнучкі та релевантні управлінські рішення для підтримки стабільності та безпеки критичної інфраструктури.

1.4. Сучасні наукові парадигми формування державної політики у сфері захисту критичної інфраструктури

Сучасний етап розвитку суспільства супроводжується зростанням кількості масштабних катастроф, серед яких природні лиха (цунамі, землетруси, повені, виверження вулканів), терористичні акти, техногенні аварії, військові конфлікти, кібератаки тощо. Ці події актуалізують потребу у зміцненні здатності суспільства до протидії таким загрозам та ефективного відновлення після їх настання. У зв'язку з цим державна політика має зосереджуватися на розробці дієвих механізмів зниження вразливості ключових елементів економічної, екологічної та соціальної систем. Йдеться, передусім, про захист критичної інфраструктури як одного з базових елементів національної безпеки.

У цьому контексті доречно погодитися з науковою позицією П. П. Богуцького, який визначає національну безпеку як стан захищеності національних інтересів від реальних та потенційних загроз, при цьому воєнні загрози виступають найнебезпечнішими [16, с. 10]. У випадку України, сучасні військові виклики становлять загрозу не лише для територіальної цілісності та суверенітету, але й безпосередньо впливають на безпеку життя громадян, що унеможливлює абстраговане або нейтральне ставлення до інших наслідків збройних дій. У глобальному вимірі такі явища становлять ризик для всього людства. У зв'язку з цим особливої ваги набуває необхідність наукового осмислення парадигм, що формують основу державної політики у сфері захисту критичної інфраструктури. Це дозволяє не лише сформулювати теоретичні засади, але й обґрунтувати концептуальні положення відповідної політики в межах загальної стратегії національної безпеки. Важливо, що саме наука, з її методологічною різноманітністю та світоглядними підходами, має передувати практичній реалізації заходів у цій сфері.

Для розуміння логіки та наукової аргументації ключових складових державної політики захисту критичної інфраструктури, які формуються під впливом трансформацій безпекового середовища, доцільно звернутися до поняття «парадигма» у тлумаченні Томаса Куна. Ця концепція, адаптована також у працях Р. К. Мертона [324, с. 28] та Ф. М. Рудича [233, с. 68], є інструментом формування інтегрованих наукових підходів і сприяє побудові системного бачення досліджуваного явища. Як зазначає М. Цюрупа, парадигма дозволяє об'єднати конкретні гіпотези в єдиний дослідницький каркас та спрямовувати пошук відповідей на складні питання, зокрема – у сфері безпеки. У нашому випадку це надає можливість сформувати ефективний інструментарій дослідження стратегій державної політики на основі наукового скептицизму й колективного аналізу [277, с. 124].

Особливо важливою є сфера аналізу сучасних наукових парадигм, що формують підґрунтя політики захисту критичної інфраструктури. Саме від

успішної ідентифікації науково обґрунтованої парадигми залежить ефективність як формування, так і реалізації відповідної політики. Завданням цього дослідницького процесу є узагальнення наявних наукових позицій щодо основ державної політики у сфері захисту критичної інфраструктури. Це, у свою чергу, створить підґрунтя для генерування авторських пропозицій щодо її удосконалення на основі фундаментального наукового пізнання.

Аналізуючи концепцію формування наукових парадигм, слід визнати визначальний внесок Томаса Куна, який стверджував, що рушієм наукового поступу виступає не абстрактна логіка, а сама людина, як учасник наукового співтовариства. Він підкреслював, що розвиток знань відбувається не лише шляхом їх кількісного накопичення, а внаслідок глибинних якісних змін – переходу від однієї парадигми до іншої. У його моделі науковий прогрес реалізується через чергування фаз «нормальної» і «революційної» науки, а не поступове доповнення знань [322, с. 188]. Парадигми, таким чином, змінюються відповідно до ступеня їхньої зрілості, здатності до формалізації, рівня експериментального підтвердження і традицій певної наукової галузі.

У класичній філософії поняття «парадигма» трактується як концептуальна модель постановки проблем, методів їх розв’язання і способів інтерпретації результатів досліджень, яка домінує протягом певного історичного періоду [238, с. 427]. У сучасному дискурсі цей термін часто ототожнюється з такими поняттями як «теорія», «концепція», «доктрина», «модель», «уявлення», «система поглядів». По суті, парадигма відображає наше уявлення про події, процеси, майбутнє, тобто формує інтелектуальне поле управлінських підходів.

Спираючись на ідеї Куна, варто виокремити дві ключові вимоги до парадигми у сфері захисту критичної інфраструктури: по-перше, вона має бути безпрецедентною, щоб об’єднати наукову спільноту навколо себе; по-друге, відкритою для інтерпретацій і розвитку, залишаючи нерозв’язані питання для наступних поколінь дослідників [322, с. 145]. Узагальнення наведених підходів дозволяє визначити ознаки парадигми у сфері державної безпеки як багатовекторність, фундаментальність, предметну конкретність, системність, здатність до реплікації, суб’єктність, прийнятність для наукової спільноти, еволюційність, практичність та об’єктивність.

Особливу увагу варто зосередити на дослідженні парадигм безпекознавства. У цьому контексті показовим є історичний приклад інтервенції США до Панамського каналу (1904 р.), під час якої президент Т. Рузвельт вперше вжив термін «національна безпека» як аргумент захисту державних інтересів. Науковці визначають суть безпеки як стан надійного захисту життєво важливих інтересів у політичній, економічній, соціальній, екологічній та військовій сферах [250, с. 288].

У післявоєнний період безпека асоціювалася виключно з військовими загрозами (1945–1954), у біполярному світі вона мала оборонний характер (1954–1991), а після 1991 року почалася трансформація до багатовимірної парадигми, що включає інформаційну, екологічну, соціальну та інші

компоненти [111, с. 180]. В умовах поліполярного світу та цифрової трансформації парадигма безпеки набуває нової якості – вона інтегрує базові цінності буття людини, стає визначальним чинником збереження антропо-соціо-культурного середовища. А. Д. Пілько справедливо окреслює сучасну безпекову парадигму як стиль мислення, що охоплює весь спектр – від стратегій державного управління до бачення безпеки окремим громадянином [188, с. 334].

З огляду на це, обґрунтування нової парадигми державної політики у сфері захисту критичної інфраструктури стає не лише актуальним, а й необхідним. У межах теоретичного аналізу простежується дуальність розуміння безпеки критичної інфраструктури: з одного боку – як стану захищеності, а з іншого – як відсутності загроз. Відповідно, перше розуміння орієнтоване на захист від критичних впливів, а друге – на усунення джерел небезпек, тобто ризиків [111, с. 185].

В. А. Ліпкан окреслює чотири основні підходи до трактування безпеки: статистичний (безпека як стан), апофатичний (як відсутність загроз), діяльнісний (як сукупність заходів) та пасивний (як дотримання нормативів) [110, с. 345]. У свою чергу В. М. Пасічник наголошує на зв'язку безпеки з потребами людини, спираючись на ієрархію А. Маслоу – безпека як стабільність, захист, впевненість [182]. Він також закликає відмовитися від «реактивної» парадигми – реагування на вже реалізовану загрозу – на користь «проактивної» політики, орієнтованої на раннє виявлення загроз і превентивні заходи.

Слушною видається позиція В. Ліпкана, який пропонує включити до нової парадигми безпеки символічні, метафізичні та консенсуальні елементи, що забезпечують цілісне бачення системи національної безпеки [110, с. 234]. Безпека, за такого підходу, інтегрується з філософією буття, стає ядром концепції держави, управління та політики. Актуальним також є підхід Р. Валіхновського, який обґрунтовує потребу розробки нової гуманітарної парадигми безпеки, що враховує взаємозалежність соціальних, політичних, економічних та екологічних криз у глобалізованому світі [17, с. 245]. Мова йде про модель, яка має бути побудована у світлі сучасного соціального знання щодо причин, наслідків, взаємозв'язку та взаємообумовленості світоглядно-ціннісних, політичних, економічних, соціальних, техногенних, екологічних та інших криз і кризових явищ різного рівня, які, на думку переважної частини фахівців, експертів та аналітиків, мають тенденцію щодо загострення в сучасних умовах глобалізації.

У межах безпекознавчого дискурсу поняття парадигми варто розглядати як сукупність теоретико-методологічних передумов, що визначають спрямованість наукових досліджень у конкретний історичний період. Парадигма формує підґрунтя для постановки наукових проблем, виступаючи зразком і моделлю їх вирішення. У соціальному контексті кожна модель суспільного устрою породжує власне бачення безпеки, яке після здобуття загального визнання оформлюється у вигляді парадигмального підходу.

Оскільки будь-яка діяльність у сфері безпеки є продуктом людської активності, її змістовне наповнення відображає домінуючі моделі поведінки – тобто парадигми, які визначають усталене розуміння як теоретичних, так і практичних аспектів забезпечення безпеки.

Професор Г. Ситник акцентує увагу на необхідності формування загальнонаукової, так званої «класичної» парадигми, орієнтованої на дослідження управлінських аспектів національної безпеки [236, с. 27]. Центральним положенням цієї парадигми є розгляд національної безпеки як інтегральної категорії, що поєднує безпеку особистості, суспільства та держави. Її оптимальний рівень досягається за умови дотримання державою тріади: наявність ефективного управління, захист національних інтересів і нейтралізація загроз. Відтак державна політика безпеки повинна ґрунтуватися на результатах, отриманих у межах цієї парадигми, і бути спрямованою на створення умов для стабільного функціонування соціуму, збереження його цілісності та потенціалу держави до самозахисту.

С. А. Мушникова інтерпретує парадигми управління безпекою як набір фундаментальних понять, метафізичних категорій і критеріїв, відповідність яким необхідна для визнання наукових пояснень [119, с. 132]. Вона вводить поняття трансдисциплінарної безпекової парадигми, що спирається на філософсько-наукову основу для інтеграції знань і створення ефективних комунікаційних практик між суб'єктами безпеки. У контексті формування державної політики захисту критичної інфраструктури така парадигма передбачає:

– усунення суперечностей у тлумаченні поняття «захист критичної інфраструктури»;

– міждисциплінарну взаємодію наукових спільнот у процесі аналізу безпекової політики;

– відмову від суто формалізованих підходів на користь інноваційних моделей міжгалузевої кооперації;

– використання плюралістичного знання для комплексного вирішення проблем безпеки.

Трансдисциплінарна парадигма є інтегративною й поєднує фрагменти реальності у єдину модель, долаючи протиставлення різних концептуальних підходів. Вона апелює до принципів синергетики, прагнучи описати складну реальність у її багатовимірності [134, с. 144]. У цьому сенсі трансдисциплінарна парадигма управління безпекою критичної інфраструктури постає як інтегративний трикутник, вершинами якого є:

1. Філософія – для осмислення фундаментальних змін у світовому порядку;

2. Соціально-гуманітарні науки – для аналізу суспільних змін і їхнього впливу на структури безпеки (соціологія, політологія, психологія тощо);

3. Управління (менеджмент) – як механізм наукового обґрунтування рішень у сфері безпеки.

Таким чином, трансдисциплінарна парадигма формує новий

міждисциплінарний інструментарій управління безпекою критичної інфраструктури, що поєднує підходи, методи і концепти з різних сфер знання, сприяючи системному і комплексному вирішенню завдань у сфері національної безпеки. Проілюструємо зміст даної парадигми на рис. 1.9.

Рис 1.9. Трансдисциплінарна парадигма управління у сфері захисту критичної інфраструктури

Джерело: узагальнено автором з використанням [119], [120]

Трансдисциплінарна безпекова парадигма може слугувати ефективним комунікативним механізмом, що забезпечує інтеграцію соціогуманітарних, філософських і управлінських підходів для впровадження інноваційних продуктів і технологій у практику державного управління у сфері захисту критичної інфраструктури. У перспективі така парадигма передбачає формування нового типу управлінця – фахівця, який поєднує трансдисциплінарне мислення з якостями науковця, здатного до системного аналізу, міжгалузевої кооперації та розв'язання багаторівневих задач, що виникають у процесі функціонування критичної інфраструктури. Такий керівник повинен не лише глибоко розуміти свою галузь, а й уміти ефективно співпрацювати в мультидисциплінарних командах – ознака, що властива трансдисциплінарному науковому середовищу [120, с. 449].

У логіці подальшого розвитку трансдисциплінарного підходу С. А. Мушникова пропонує поліпарадигмальну модель управління безпекою як наступний рівень інтеграції. Ця модель доповнює попередню, включаючи до своєї структури різноманітні дослідницькі парадигми, які взаємодіють на

принципах доповнюваності та узгодженості. Така міжпарадигмальна взаємодія дозволяє зменшити ризики фрагментарності знань, підвищити якість прийняття рішень та адаптувати управлінські практики до складної реальності сучасного безпекового середовища (рис. 1.10.).

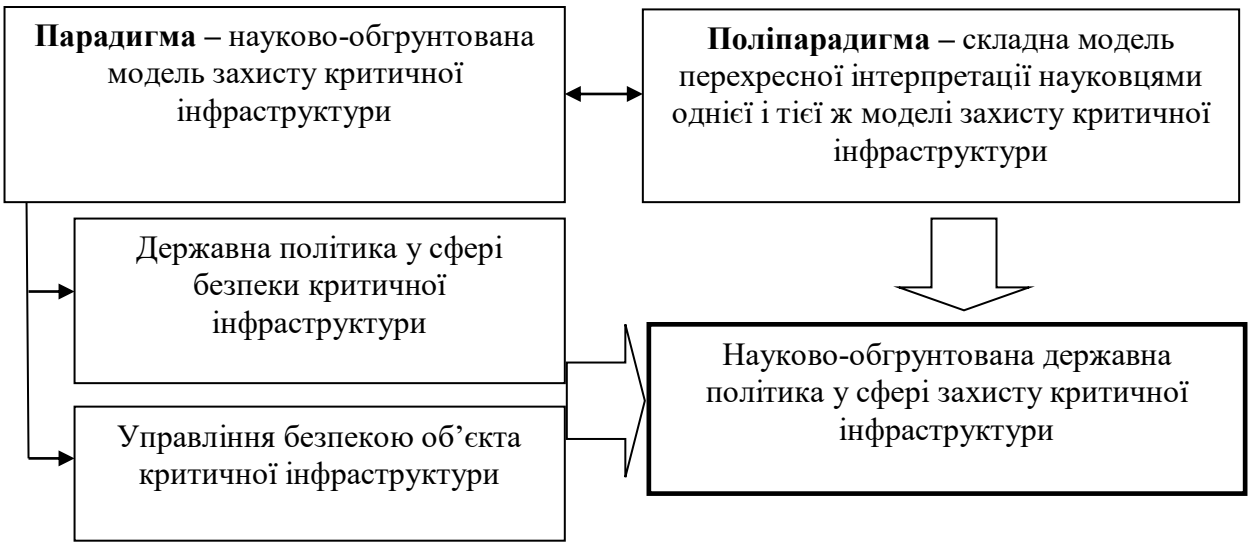


Рис. 1.10. Формування поліпарадигмальної моделі формування державна політики у сфері захисту критичної інфраструктури

Джерело: узагальнено автором з використанням [119], [120]

Вважаємо доцільним розглянути інтеграцію наукових парадигм – зокрема трансдисциплінарної та поліпарадигмальної – у сферу формування та реалізації державної політики у галузі безпеки критичної інфраструктури. Такий підхід, по-перше, дозволяє врахувати широкий спектр наукових підходів, а по-друге, сприяє комплексному і різносторонньому осмисленню та впровадженню безпекових заходів. У цьому контексті С. А. Мушникова підкреслює, що поліпарадигмальна модель не є новою парадигмою чи інноваційною системою, а слугує інструментом забезпечення системного підходу до наукового обґрунтування управлінських рішень [120, с. 450].

Це твердження відкриває перспективу для поглибленого аналізу можливостей поєднання трансдисциплінарної парадигми з поліпарадигмальною моделлю у контексті ієрархії стратегій управління в сфері захисту критичної інфраструктури. Така інтеграція дозволить не лише концептуалізувати багаторівневість сучасного безпекового середовища, а й закласти основу для ефективної реалізації державної політики на цьому напрямі.

Варто звернути увагу на напрацювання фахівців Національного інституту стратегічних досліджень, які в аналітичній доповіді «Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури в Україні» окреслили актуальні виклики й запропонували нові підходи. Зокрема, йдеться про необхідність модернізації інформаційно-аналітичних та ситуаційно-кризових центрів, формування кадрового потенціалу і створення аналітичних спільнот як постійно діючих

концептуальних осередків безпеки [13]. Такі ініціативи цілком узгоджуються з трансдисциплінарною парадигмою, яка дозволяє сформувати ефективні механізми взаємодії та управління в умовах складних систем, що функціонують за принципами нелінійної динаміки – як це передбачає, зокрема, критичний ризик-менеджмент на основі нечіткої логіки.

Цей науковий напрям підтримується і С. С. Телеником, який, застосовуючи макросистемний підхід до вивчення державної політики захисту критичної інфраструктури, посилається на екологічну теорію розвитку Урі Бронфенбреннера [352]. Вона передбачає ієрархічну структуру систем (мезо-, екзо-, макро-), що дозволяє враховувати як прямі, так і зворотні зв'язки у процесі державного управління [257, с. 223]. Такий підхід дозволяє розглядати захист критичної інфраструктури не ізольовано, а як частину загальної системи національної безпеки.

На завершення варто зазначити позицію професора Г. Ситника, який закликає до переходу на новий рівень наукової парадигми – системно-синергетичної, що знайшла відображення у цивілізаційному підході до дослідження соціальних процесів. Цей підхід вимагає використання сучасних методологій комплексного аналізу як основи для побудови ефективної, адаптивної системи державного управління у сфері безпеки критичної інфраструктури [236, с. 28]. Учений обґрунтовує потребу забезпечення безпеки на всіх рівнях через врахування низки взаємопов'язаних факторів, що визначають напрямок сталого та безпечного розвитку. Серед них особливе значення мають: стабільність у реалізації концепції сталого розвитку, що забезпечує гармонійний баланс між екологічними, соціальними, економічними та політичними чинниками; необхідність одночасного врахування культурно-історичних характеристик національного розвитку та факторів міжнародної безпеки; конфліктність і динаміка змін між загальнолюдськими, національними, груповими та індивідуальними інтересами, що спричиняє непередбачуваність суспільно-політичних трансформацій; глобалізаційні процеси й розвиток інформаційних технологій, які ускладнюють контроль держави над соціальними взаємодіями.

Таким чином, поліпарадигмальна модель державної політики у сфері захисту критичної інфраструктури передбачає урахування вищезгаданих факторів, а також дії загроз і ризиків. У статичному аспекті ця модель являє собою сукупність мікросистем, а в динамічному – формування інституцій, здатних до колективного виконання завдань. Як приклад, С. С. Теленик наводить взаємодію СБУ та МВС за надзвичайних умов, що утворює мезосистему. Подібною мезосистемою можуть бути окремі сектори критичної інфраструктури – водопостачання, транспорт чи енергетика, які об'єднують підсистеми на рівні галузей [257, с. 115].

З позицій інституціоналізму державна політика у сфері безпеки критичної інфраструктури розглядається як складна політико-правова, техніко-організаційна система. За Г. Ситником, вона включає: сукупність

суб'єктів безпеки (органи влади, громадськість, ЗМІ); арсенал інструментів (політичних, воєнних, економічних); нормативну базу (закони, стратегії, програми); множину джерел загроз (фізичних і юридичних осіб); перелік факторів національної безпеки (зовнішні впливи, міжнародні інституції); та, безпосередньо, об'єкти критичної інфраструктури [236, с. 28].

Сучасна парадигма державної політики має бути зосереджена на посиленні інституційної ефективності захисту критичної інфраструктури. Як наголошує О. П. Єременчук, реалізація цього завдання передбачає алгоритм дій, адаптований до особливостей кожного об'єкта [48, с. 87]. До цього алгоритму входить:

– ідентифікація загроз і визначення їх інтенсивності (природного, техногенного, криміногенного походження);
– аналіз уразливості інфраструктурного об'єкта;
– оцінка його стійкості до негативних впливів;
– визначення ключових ризиків;
– категоризація об'єкта за рівнем захищеності;
– розробка сценаріїв реагування;
– формування цілей і засобів захисту;
– реалізація спільних державних і приватних заходів;
– безперервна адаптація регулятивного середовища залежно від ситуації.

Таким чином, концепція забезпечення безпеки критичної інфраструктури має ґрунтуватися на адаптивних, динамічних, науково обґрунтованих підходах із фокусом на інтеграцію управлінських, технологічних та міжінституційних рішень.

Актуальними для формування сучасної безпекової парадигми є дослідження О. П. Постельжука, Л. І. Валюха, Г. Я. Невинної та Р. Ю. Михальчука, які наголошують на необхідності урахування військово-економічного та інформаційно-комунікаційного потенціалу Російської Федерації як стратегічного противника [220, с. 110]. Така позиція цілком обґрунтована: цілеспрямована і довгострокова безпекова політика має за мету мінімізувати вплив Росії через інфільтрацію її агентурних структур у державні управлінські процеси, що сприяє системному ослабленню України. Ці загрози стали очевидними у 2014 році та на початку 2022 року, коли Україна не змогла ефективно протистояти вторгненню диверсійно-розвідувальних груп та окупаційних військ, які, крім прямих дій, здійснювали удари по об'єктах критичної інфраструктури, підриваючи соціально-економічну та логістичну стабільність [220, с. 109]. У цьому контексті новітню безпекову парадигму варто будувати на глибокому лінгвістичному й ідейно-політичному аналізі оборонних доктрин України. Як зазначає М. Цюрупа, у період з 1993 по 2021 рік українська оборонна стратегія характеризувалась миролюбною спрямованістю, без агресивних чи превентивних установок, що дозволяє кваліфікувати Україну як державу з неагресивною політикою [277, с. 123].

Таким чином, сучасні безпекові реалії України вимагають переосмислення та оновлення підходів до захисту критичної інфраструктури в контексті зміни парадигми національної безпеки. Особливої уваги заслуговує пропозиція Д. М. Павлова щодо розширення державно-приватного партнерства у цій сфері. Зважаючи на те, що значна частина об'єктів критичної інфраструктури перебуває у приватній власності [179, с. 72], ефективна взаємодія між державою та бізнесом потребує належного правового забезпечення [180, с. 146]. Це положення знайшло відображення у Стратегії національної безпеки України «Безпека людини – безпека країни» [265], де підкреслюється важливість побудови ефективної системи безпеки критичної інфраструктури на засадах чіткого розподілу відповідальності між суб'єктами та державно-приватного партнерства.

У контексті розбудови сучасної моделі державної політики заслуговують на увагу також теоретичні розробки П. П. Богуцького, який пропонує впровадження військово-правової парадигми взаємодії громадянського суспільства з сектором безпеки та оборони. Така модель передбачає створення правових механізмів участі громадських інституцій і громадян в оборонних процесах, а також контроль за виконанням відповідних функцій силами оборони, оборонно-промисловим комплексом та іншими структурами, що забезпечують суверенітет і територіальну цілісність держави [15, с. 115]. Таким чином, ефективне впровадження новітньої парадигми безпеки має спиратися на міжсекторальну взаємодію, залучення громадянського суспільства, реформування стратегічного планування та посилення правового регулювання у сфері захисту критичної інфраструктури.

Актуальним у межах дослідження безпекової політики також вважаємо науковий доробок О. М. Суходолі, який підкреслює, що основою парадигми захисту критичної інфраструктури мають стати: визначення, аналіз та оцінка ефективності методів і засобів впливу однієї системи на іншу, а також розробка інструментів запобігання, стримування, нейтралізації або пом'якшення наслідків такого впливу. Окрему увагу приділено розробці механізмів, що сприяють підвищенню рівня готовності, своєчасному реагуванню та швидкому відновленню функціонального режиму критичних систем. У межах наукової концепції вчений формує ідею національної стійкості як ключової складової безпеки держави, де системи критичної інфраструктури виступають її основними детермінантами. Він виділяє сім ключових тригерів забезпечення національної стійкості: безперервність урядування та державних послуг, управління переміщенням населення, допомога потерпілим, енергетична безпека, продовольча та водна стійкість, стійкість комунікаційних систем, а також транспортної інфраструктури [251, с. 67].

Проблему інфраструктурної вразливості в умовах глобальної конкуренції піднімає і Г. Ю. Зубко, який акцентує на прагненні окремих держав контролювати інфраструктурні системи інших країн, що, зокрема,

проявляється у діях Росії [83, с. 38]. У цьому контексті парадигма національної стійкості повинна корелюватися із новою соціально-економічною парадигмою сталого розвитку. Цю думку підтримує і професор Г. Ситник [236, с. 29], який вказує на необхідність гармонізації екологічних, соціальних, економічних та політичних взаємовідносин як умови реалізації потреб у безпеці.

Поняття сталого розвитку було введене Міжнародною комісією з навколишнього середовища та розвитку (Комісія Брунтланд) у 1987 році і трактується як розвиток, що задовольняє поточні потреби без шкоди для майбутніх поколінь [131, с. 75]. Із цієї позиції варто згадати і позицію В. Є. Хаустова та Ш. А. Омарова, які, враховуючи потреби безпеки майбутніх поколінь, пропонують модель розвитку з акцентом на зниження виробництва, помірне споживання ресурсів, органічне землеробство та відповідальне енергоспоживання [274, с. 269]. Серед цілей сталого розвитку ООН, що корелюють із безпековою політикою в частині інфраструктури, варто виділити: розвиток стійкої інфраструктури, зниження нерівності в доступі до неї, ефективне використання об'єктів інфраструктури для збалансованого розвитку, а також їх повну інтеграцію у процес реалізації національних інтересів [172].

А. Д. Пілько та Т. П. Гарда у своїх дослідженнях пропонують дві основні інтерпретації безпеки критичної інфраструктури у контексті сталого розвитку: як систему меж і параметрів, що забезпечують збалансовану динаміку розвитку територіальних систем; і як модель, де соціальний розвиток має пріоритет над іншими формами (економічною, військовою, екологічною, науково-технічною) [187, с. 114].

Важливим є також інституційне підґрунтя для реалізації зазначених ідей. Як слушно зазначено у висновках, ефективне впровадження науково обґрунтованих стратегій можливе лише за наявності як формальних, так і неформальних інститутів, які мають суспільне визнання. Таким чином, ключову роль у формуванні стійкої державної політики у сфері захисту критичної інфраструктури відіграють не лише наукові концепції, але й ціннісні орієнтири, що поділяються елітами та суспільством загалом.

За підсумками проведених досліджень, слушною видається пропозиція вітчизняних науковців [114, с. 434] щодо векторів модернізації державної політики у сфері захисту критичної інфраструктури. Зокрема, модернізація має здійснюватися за такими напрямами:

– формування комплексної нормативно-правової бази щодо безпеки критичних об'єктів;

– гармонізація національного законодавства з актами ЄС і впровадження відповідних стандартів, зокрема в частині державно-приватного партнерства;

– створення інституту-координатора державної політики у сфері критичної інфраструктури з механізмами моніторингу;

– впровадження профілактичних заходів безпеки, зокрема охорони й

самозахисту об’єктів; налагодження міжнародної співпраці.

Дослідження дозволило виявити актуальні проблеми політики України у цій сфері, серед яких:

– нормативно-правова неузгодженість функціоналу суб’єктів безпеки;

– слабкість інституційних механізмів забезпечення стійкості інфраструктури до загроз зовнішнього і внутрішнього характеру;

– відсутність узгодженості у формуванні регіональних моделей захисту населення в надзвичайних ситуаціях;

– наявність прогалин у системі протидії загрозам стабільності роботи критичних об’єктів.

У цьому контексті доцільно реалізувати заходи в межах новітньої парадигми державної політики, що передбачає активізацію моніторингу, паспортизацію об’єктів, ефективну міжвідомчу координацію, посилення державно-приватного партнерства та міжнародної співпраці. Реалізація вказаних заходів дозволить зменшити ризик виникнення надзвичайних подій і знизити їх негативні наслідки. Водночас вважаємо за доцільне розробити чіткий, уніфікований алгоритм дій для власників, операторів і залучених суб’єктів безпеки, з подальшим нормативним закріпленням на державному рівні, що створить передумови для цілісної, прогнозованої та відповідальної політики у сфері захисту критичної інфраструктури.

РОЗДІЛ 2
СУЧАСНІ ОРГАНІЗАЦІЙНО-ПРАВОВІ ТА УПРАВЛІНСЬКІ АСПЕКТИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

2.1. Інституційно-правові аспекти реалізації державної політики у сфері захисту критичної інфраструктури

Процес становлення сучасної державної політики у сфері захисту критичної інфраструктури України передбачає інтеграцію різноспрямованих елементів, що стосуються інституційного оформлення, легітимації та забезпечення її правової валідності. Особливої актуальності набуває осмислення прихованих аспектів правової адаптації державної політики в умовах воєнного стану. Такий підхід дозволяє не лише краще усвідомити сутність інституційно-правових характеристик політики безпеки, а й розробити ефективні механізми її адміністративно-правового регулювання.

Як відомо, усе, що пов'язано з державною політикою виходить від уповноважених державою суб'єктів, насамперед її органів влади. Таким чином, обов'язковою ознакою державної політики варто розглядати владний характер її інститутів, що інспірується правоздатністю та загальнообов'язковістю генерованих ними нормативно-правових актів [235, с. 120].

Логіко-семантичний аналіз стрижневих компонентів атрибутиву інституційно-правових аспектів державної політики дозволяє зафіксувати синергетичну дуальність її ключових тригерів – механізму державного управління та механізми правового регулювання [261, с. 345]. Звернемось до Великого тлумачного словника сучасної української мови, який визначає «механізм» як внутрішню будову, систему, сукупність станів і процесів, з яких складається певне явище [20, с. 665]. Опираючись на вихідні постулати та принципи державного управління, С. І. Крук , пролонгуючи змістовне наповнення попередньої дефініції, пропонує суб'єктно-об'єктні відносини, що виникають під час реалізації державної політики у сфері захисту об'єктів критичної інфраструктури, трактувати у формі правовідносин через необхідність їх державного врегулювання та легітимації [101, с. 77]. Цей процес передбачає імплементацію ряду заходів, зокрема:

1) ідентифікації базових векторів державної політики, стратегічного планування та прогнозування у сфері захисту критичної інфраструктури;

2) пошук, виявлення, профілактика та ліквідація загроз та ризиків безпеки об'єктів критичної інфраструктури;

3) суб'єктна корекція та координування діяльності органів державної влади у сфері забезпечення захисту критичної інфраструктури;

4) визначення обсягу та рівня необхідної ресурсної бази у сфері забезпечення захисту критичної інфраструктури та її

забезпечення [102, с. 72].

Усі згадані заходи та правовідносини, що виникають у процесі реалізації державної політики в сфері захисту критичної інфраструктури, мають на меті протидію з боку органів державної влади різноманітним ризикам, загрозам і небезпекам. Ця діяльність реалізується шляхом застосування орієнтованого на безпеку державного управлінського інструментарію, що базується на дотриманні принципів публічності, легітимності та результативності, ефективність яких обумовлена функціональністю механізму правового регулювання. Слушною видається позиція С. І. Бевза, який визначає механізм правового регулювання як «сукупність засобів, за допомогою яких забезпечується вплив права на суспільні відносини» [4, с. 44]. До цього варто додати положення, викладені у Великому енциклопедичному юридичному словнику, згідно з якими термін «правове регулювання» означає «один із основних засобів державного впливу на суспільні відносини з метою їх упорядкування в інтересах людини, суспільства і держави» [19, с. 335]. Аналогічну думку висловлюють науковці Ю. С. Шемшученко та С. В. Бобровник, які вказують, що «...правове регулювання є одним із основних засобів державного впливу на суспільні відносини з метою їх упорядкування в інтересах людини, суспільства і держави» [281, с. 40]. Отже, ключовим у контексті реалізації державної політики захисту критичної інфраструктури є акцент на взаємозв'язку людини, суспільства і держави. Це положення знаходить своє підтвердження і в Конституції України, де в ст. 3 зазначено, що «людина, її життя і здоров'я, честь і гідність, недоторканість і безпека визнається в Україні найвищою соціальною цінністю» [99], а у ст. 43 гарантується право кожного на «належні, безпечні і здорові умови праці» [99].

Реалізація інституційно-правового регулювання в державному механізмі неможлива без використання відповідного державного інструментарію, який передбачає створення або санкціонування правових норм у межах певних форм юридичного впливу. Науковці В. Колпаков та О. Кузьменко, досліджуючи механізми інституційно-правового регулювання, виокремлюють такі державно-правові механізми: механізм правового регулювання, механізм дії права, механізм правотворчості, механізм соціального управління, механізм правового впливу, механізм державного управління, а також механізм забезпечення правових режимів [93, с. 156].

Таким чином, підсумовуючи викладене, інституційно-правове регулювання можна розглядати як одну з форм правового впливу, здійснюваного органами державної влади за допомогою інституційних засобів правової дійсності, які реалізують регуляторну функцію права. Механізм інституційно-правового регулювання, відповідно, є комплексом взаємопов'язаних інструментів, спрямованих на досягнення цілей правового регулювання. Узагальнення наукових підходів дозволяє

сформулювати власне бачення інституційно-правового регулювання у сфері державної політики захисту об'єктів критичної інфраструктури. У цьому контексті механізм інституційно-правового регулювання слід визначити як систему організаційно-управлінських і правових заходів, реалізованих державними інститутами, що забезпечують цілеспрямований адміністративний вплив (з орієнтацією на максимізацію безпеки) на суспільні відносини, спрямовані на мінімізацію ризиків, загроз та небезпек щодо об'єктів критичної інфраструктури, при цьому ґрунтуючись на пріоритетах людини, суспільства і держави [244, с. 215]. Основу такого механізму становлять об'єктивні взаємозв'язки між процесами саморозвитку й саморуху інституційних засобів правової дійсності. Тому система забезпечення безпеки критичної інфраструктури повинна бути адаптивною, динамічно змінюваною відповідно до змін у безпековому середовищі як на мікро-, так і на макрорівні, а також у глобальному геополітичному контексті [40, с. 83].

Проведений аналіз нормативно-правової бази, що формує фундамент інституційно-правового механізму реалізації державної політики у сфері захисту критичної інфраструктури, дозволив систематизувати коло ключових інституцій, які визначають архітектоніку безпекової парадигми функціонування об'єктів критичної інфраструктури.

Інституційні підходи до організації системи захисту критичної інфраструктури інтегровані в безпекову модель держави та формалізовані в Законі України «Про національну безпеку України» № 2469-VIII від 31.03.2023 р. [62]. Відповідно до положень ст. 4 цього Закону, пріоритетні напрями державної політики у сфері національної безпеки та оборони охоплюють забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки та інших ключових напрямів [62]. Поряд із цим, ст. 34 Кодексу цивільного захисту України визначає необхідність реалізації комплексу інженерних заходів із захисту територій, включно з тими, що належать до об'єктів критичної інфраструктури [90].

У Стратегії забезпечення державної безпеки, затвердженій Указом Президента України від 16.02.2022 р. № 56/2022 [267], критична інфраструктура розглядається як один із центральних елементів системи забезпечення національної безпеки, захисту державного суверенітету, конституційного ладу та територіальної цілісності країни. Документ наголошує на високому рівні загроз цій інфраструктурі (п. 19), що зумовлені тимчасовою окупацією окремих територій України та триваючими гібридними впливами з боку іноземних суб'єктів розвідувально-диверсійної діяльності, спрямованої на її дестабілізацію [267].

У пункті 24 цієї Стратегії виокремлено комплекс ключових завдань державної політики, серед яких: розвиток спроможностей суб'єктів системи державної безпеки щодо впровадження превентивних заходів на

об’єктах критичної інфраструктури, посилення контррозвідувального режиму, активізація протидії терористичним та організованим злочинним угрупованням, які можуть бути спрямовані на захоплення або руйнування важливих об’єктів, технологічне укріплення інституцій державної безпеки, впровадження новітніх апаратних і спеціальних засобів, підвищення професійної кваліфікації фахівців із безпеки, модернізація нормативно-правової та організаційної бази, налагодження ефективної взаємодії з інститутами громадянського суспільства, а також розвиток міжнародного співробітництва у сфері безпеки та впровадження національної системи стійкості [267].

Аналізуючи роль органів державної влади в інституційно-правовому механізмі реалізації державної політики, О. Л. Хитра [275, с. 78] зазначає, що архітектура національної безпеки, за змістом розділів IV–VI Конституції України, включає такі ключові інститути як Верховна Рада України, Президент України та Кабінет Міністрів України. Закон України «Про критичну інфраструктуру» № 1882-IX розширює коло суб’єктів, уповноважених на формування та впровадження політики у сфері її захисту, дозволяючи ідентифікувати спектр базових інституцій, які функціонують у даному безпековому сегменті:

1. Президент України. Правовий статус Президента у сфері захисту критичної інфраструктури регламентований у розділі V Конституції України, зокрема ст. 102 визначає його гарантом державного суверенітету, територіальної цілісності України, додержання Конституції України, прав і свобод людини і громадянина [96]. Президент України забезпечує національну безпеку України (п.1 ст.106), очолює Раду національної безпеки і оборони України (РНБО) (п.18 ст.106) та особисто формуючи її склад [72], є гарантом адміністрування процесу реагування на кризові ситуації, що загрожують національній безпеці [96]. Отже, повноваження Президента України в сфері захисту критичної інфраструктури можна розмежувати на повноваження: орієнтовані на профільний суб’єктний сегмент; диференційовані за сферами впливу; повноваження із досягнення загальнодержавної мети.

2. Рада національної безпеки та оборони (РНБО). Цей безпековий інститут є координаційним органом з питань національної безпеки і оборони при Президентові України [72]. РНБО України координує і контролює діяльність органів виконавчої влади у сфері національної безпеки і оборони (ч1 ст.107 Конституції України) [96], може подавати Президенту свої пропозиції, що стосуються важливих стратегічних питань із захисту критичної інфраструктури та приймає відповідні рішення [72].

3. Кабінет Міністрів України (КМУ). Даний інститут є найвищим органом в ієрархії органів виконавчої влади. Згідно ст.2 Закону України №794-VII від 27.02.2014 р. «Про Кабінет Міністрів України» [59] до його основних завдань у сфері захисту критичної інфраструктури належать:

– забезпечення державного суверенітету та економічної самостійності

України;

– розроблення і виконання загальнодержавних програм у сфері захисту критичної інфраструктури;

– здійснення заходів щодо забезпечення національної безпеки та обороноздатності України [59].

Отже, Кабінет Міністрів України слід вважати ключовим інститутом, відповідальним за формування та реалізацію в країні державної політики у сфері захисту критичної інфраструктури, організацію та забезпечує національну систему захисту критичної інфраструктури потрібними ресурсами, силами та засобами для її функціонування [231].

4. Верховна Рада України (ВРУ). До її повноважень у сфері захисту критичної інфраструктури входить прийняття законів, визначення засад внутрішньої і зовнішньої політики, затвердження Державного бюджету України, затвердження загальнодержавних програм захисту, заслуховування щорічних та позачергових послань Президента України про внутрішнє і зовнішнє становище України, контроль за діяльністю Кабінету Міністрів України, затвердження рішень про одержання Україною від іноземних держав, банків і міжнародних фінансових організацій макрофінансової допомоги, затвердження указів Президента України про введення надзвичайного чи воєнного стану в окремих місцевостях, про оголошення окремих місцевостей зонами надзвичайної ситуації, надання згоди на обов'язковість міжнародних договорів України та їх денонсація, затвердження переліку об'єктів права державної власності, що не підлягають приватизації, визначення правових засад вилучення об'єктів права приватної власності [96].

5. Функціональні органи у сфері захисту критичної інфраструктури. Відповідають за забезпечення роботи окремих державних систем захисту та реагування, долучаються до реагування на кризові ситуації з метою гарантування безпеки та стійкості критичної інфраструктури, формують перелік об'єктів критичної інфраструктури, готують пропозиції щодо включення інфраструктурних об'єктів до Реєстру, здійснюють оцінку загроз і ризиків критичній інфраструктурі у відповідних сферах та надають операторам і власникам об'єктів консультації щодо наявності таких загроз і ризиків, а також протоколи дій щодо їх нейтралізації, приймають участь у оцінюванні загроз та ризиків критичній інфраструктурі на національному рівні, генерують пропозиції щодо загальнодержавних та секторальних проєктних загроз і ризиків, здійснюють організацію комунікації та інформаційного реверсу між суб'єктами національної системи захисту критичної інфраструктури, проводять моніторинг рівня безпеки об'єктів критичної інфраструктури за сферами їх діяльності [60].

6. Секторальні органи у сфері захисту критичної інфраструктури. Відповідальні за формування та реалізацію державної політики у довірених їм сегментах критичної інфраструктури. Створюють у своєму

складі структурних підрозділів відповідальних за безпеку критичної інфраструктури, акумулюють, систематизують та аналізують дані щодо об'єктів критичної інфраструктури та особливостей їх функціонування, здійснюють разом із їх операторами категоризацію таких об'єктів за ввіреними їм секторами, створюють секторальні каталоги об'єктів та відправляють інформацію до Реєстру. Окрім цього, розробляють та затверджують на секторальному рівні: проєктні загрози критичній інфраструктурі, вимоги до захисту критичних об'єктів за категоріями, плани коінтеграції функціональних органів, регламенти і норми захисту критичної інфраструктури у відповідних секторах, проектні загрози критичній інфраструктурі на об'єктовому рівні, погоджують паспорти безпеки об'єктів критичної інфраструктури за профільними секторами, здійснюють інспекцію стану захищеності критичних об'єктів, займаються розробкою рекомендацій до врахування проєктних ризиків та загроз критичній інфраструктурі національного рівня та щорічної їх оцінки на загальнодержавному рівні, координують процес підготовки, навчання та тренування персоналу, щодо забезпечення захисту та стійкості секторів критичної інфраструктури, формують щорічний звіт по стану забезпечення безпеки критичної інфраструктури у відповідному секторі, долучаються до реагування на кризові ситуації, що загрожують безпеці та стійкості об'єктів критичної інфраструктури, а також до створення належних умов виконання розвідувальними, правоохоронними та контррозвідувальними органами своїх функцій щодо захисту критичної інфраструктури [60].

7. Уповноважений орган у сфері захисту критичної інфраструктури України. Відповідає за «формування та реалізацію державної політики у сфері захисту критичної інфраструктури, координацію діяльності суб'єктів національної системи захисту критичної інфраструктури…» [60]. Також, відповідно до його повноважень, систематизує пропозиції інститутів національної системи захисту критичної інфраструктури, створює та веде Реєстр об'єктів, організовує здійснення оцінки захищеності об'єктів критичної інфраструктури та оцінює загальний стан їх захищеності, здійснює моніторинг загроз критичній інфраструктурі на загальнодержавному рівні та оцінює загрози національній безпеці із залученням функціональних та секторальних органів. Окрім цього Уповноважений орган проводить щорічну оцінку національного рівня загроз і ризиків критичній інфраструктурі, візує проєктні загрози й ризики на секторальному рівні, узагальнює пропозиції щодо регламентування вимог до забезпечення стійкості та захисту секторів критичної інфраструктури. В межах реалізації інституційних повноважень розробляє та затверджує Проєктні загрози критичній інфраструктурі національного рівня, що містять дані з обмеженим доступом, надсилає пропозиції Кабінету Міністрів України щодо формування Національного плану захисту та забезпечення стійкості критичної інфраструктури, форми,

змісту та порядку розробки, паспорта безпеки та планів заходів щодо захисту критичної інфраструктури загальнодержавного рівня, готує пропозиції до проєктів стратегічних документів щодо забезпечення стійкості та безпеки, здійснення захисту критичної інфраструктури, приймає участь у розробці нових галузей знань, програм підвищення кваліфікації та навчання, навчальних програм з питань забезпечення захисту та стійкості критичної інфраструктури. Також Уповноважений орган узагальнює висновки та рекомендації для власників (операторів) об'єктів щодо зміни їх цільового призначення, права власності чи режиму роботи, формує бази даних щодо загроз і вразливостей критичної інфраструктури, підтримує функціональність системи інформаційного обміну між суб'єктами національної системи захисту критичної інфраструктури, координує роботу секторальних органів, налагоджує співпрацю із іноземними державами та міжнародними організаціями, гарантує виконання і дотримання зобов'язань по захисту критичної інфраструктури згідно підписаним міжнародним договорам [60].

8. Державна служба захисту критичної інфраструктури та забезпечення національної системи стійкості України (ДЗКІ). Ідентифікується як центральний орган виконавчої влади із спеціальним статусом, діяльність якого спрямовується і координується Кабінетом Міністрів України і який опікується забезпеченням національної системи стійкості та формуванням та реалізацією державної політики у сфері захисту критичної інфраструктури. Положення «Про Державну службу захисту критичної інфраструктури та забезпечення національної системи стійкості України» [217] ДЗКІ визначено як «уповноважений орган у сфері захисту критичної інфраструктури України» [217]. Отже, констатуємо факт, що ці дві організації усособлюють один інститут. Законом України № 2684-IX від 18.10.2022 р. «Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України» [51] установлено, що «…під час дії воєнного стану, а також протягом 12 місяців після його припинення чи скасування повноваження уповноваженого органу у сфері захисту критичної інфраструктури України, передбачені цим Законом, здійснюються Державною службою спеціального зв'язку та захисту інформації України» [51]. Зауважимо, що фактично дана установа (Держспецзвязку) перейняла зазначені повноваження лише через 4 місяці, відповідно до Постанови КМУ № 167 від 24.02.2023 р. «Про внесення змін до Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України» [199], яка внесла відповідні зміни до Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України. Однак зміни було внесено лише через 3 місяці Наказом Адміністрації державної служби спеціального зв'язку та захисту інформації України № 467 від 31.05.2023 р. «Про затвердження Змін до Положення про територіальний орган Адміністрації Державної

служби спеціального зв'язку та захисту інформації України» [123]. Зміни стосувалися основних завдань територіального органу, які було розширено діяльністю із реалізації державної політики у сфері захисту критичної інфраструктури, які безпосередньо здійснюють боротьбу з тероризмом, забезпечення здійснення Адміністрацією Держспецзв'язку функціонального управління національною системою захисту критичної інфраструктури, участь Держспецзв'язку у координуванні роботи міністерств та операторів критичних об'єктів з питань забезпечення захисту критичної інфраструктури [159]. Серед напрямків роботи було додано участь у межах регіону у координації діяльності місцевих органів виконавчої влади у сфері захисту критичної інфраструктури, взаємодію в регіоні операторів критичної інфраструктури та функціональних органів з питань забезпечення захисту об'єктів, участь у регіональній організації здійснення оцінки захищеності об'єктів критичної інфраструктури, участь у проведенні в межах регіону оцінки загроз критичній інфраструктурі на загальнодержавному рівні та моніторингу загроз національній безпеці в результаті дій загроз критичній інфраструктурі, участь у підготовці щорічного моніторингу загроз і ризиків критичній інфраструктурі національного рівня та ін. [123].

Організація налагоджує співробітництво із міжнародними установами та контролює виконання зобов'язань, взятих відповідно до міжнародних договорів, проводить із залученням секторальних і функціональних органів моніторинг загроз критичній інфраструктурі та національній безпеці на загальнодержавному рівні внаслідок впливу загроз критичній інфраструктурі, розробляє та затверджує Проєктні загрози критичній інфраструктурі, направляє Кабінету Міністрів України пропозиції стосовно удосконалення:

– форми, порядку розробки та змістовного наповнення паспорта безпеки об'єктів критичної інфраструктури;

– Національного плану захисту та забезпечення стійкості критичної інфраструктури;

– форми, порядку розроблення та змістовного наповнення національних планів заходів щодо захисту об'єктів критичної інфраструктури.

У 2020 році Держспецзв'язку перейняла функцію зі створення каталогу та Реєстру об'єктів критичної інформаційної інфраструктури [217].

9. Оператор критичної інфраструктури. Законом України «Про критичну інфраструктуру» [60] даний інститут ідентифіковано як «юридична особа будь-якої форми власності та/або фізична особа-підприємець, що на правах власності, оренди або на інших законних підставах здійснює управління об'єктом критичної інфраструктури та відповідає за його поточне функціонування» [60]. Їх також Законом включено до складу національної системи захисту критичної

інфраструктури на яку покладено обов'язки розробки та провадження державної політики у сфері захисту критичної інфраструктури.

Разом із Секторальними органами оператори також проводять категоризацію об'єктів інфраструктури у своїх секторах, формують секторальні переліки об'єктів критичної інфраструктури, подають інформацію до Реєстру, забезпечують захист об'єктів критичної інфраструктури, розробляють і подають на затвердження до відповідних секторальних та функціональних органів паспорт безпеки, розробляють, оновлюють та гарантують виконання об'єктових планів щодо забезпечення стійкості й безпеки критичної інфраструктури, здійснюють моніторинг ризиків на об'єктах, організовують заходи оперативного реагування на фізичні атаки чи протиправні дії що націлені на дестабілізацію, пошкодження або знищення об'єктів критичної інфраструктури, проводять навчання, тренінги, підготовку та тестування працівників, відповідальних за безпеку, охорону та захист об'єктів критичної інфраструктури [60].

Окрім зазначених вище інститутів суб'єктний склад національної системи захисту критичної інфраструктури налічує й інші органи, як: Центральна виборча комісія, Апарат Ради національної безпеки і оборони України, Національний банк України, Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг, Національна комісія, що здійснює державне регулювання у сфері інформатизації та зв'язку, Національна комісія з цінних паперів та фондового ринку, Фонд державного майна України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Збройні Сили України й інші військові формування, а також інші органи влади із спеціальним статусом та які залучаються до формування та реалізації державної політики у сфері цивільного захисту, місцеві органи виконавчої влади, органи місцевого самоврядування, функціональні та секторальні органи, інші міністерства, правоохоронні та розвідувальні органи, суб'єкти контррозвідувальної й оперативно-розшукової діяльності, установи, підприємства та організації незалежно від форми власності, що провадять діяльність із забезпечення стійкості та безпеки критичної інфраструктури [60].

Зазначимо також, що спектр суб'єктів реалізації державної політики у сфері безпеки критичної інфраструктури не обмежується виключно державними інститутами, а акумулює в собі ще й приватних суб'єктів господарювання, а також окремих осіб – надавачів послуг, пов'язаних із національними інформаційними ресурсами. Слушною тут вважаємо пропозицію Г. Ю. Зубка що стосується удосконалення нормативно-правової бази досліджуваної сфери. Пропозиції стосуються регламентування та чіткої фіксації у нормативних документах спектру завдань і відповідних повноважень зазначених суб'єктів на основі затвердження відповідних положень [80, с. 170]. Доречною також буде

розробка концепції міжсекторальної взаємодії та синергії сил зацікавлених сторін на основі механізму державно-приватного партнерства.

Загальну архітектуру суб'єктного складу державної політики у сфері безпеки критичної інфраструктури структуровано Законом України «Про критичну інфраструктуру» [60] на рівні управління, серед яких встановлено:

I. Загальнодержавний рівень – реалізується Кабінетом Міністрів України, Національним банком України, уповноваженим органом у сфері захисту критичної інфраструктури України, інститутами державної влади відповідно до транспарентності повноважень, іншими центральними органами виконавчої влади та державними органами.

II. Регіональний та галузевий рівні – здійснюється центральними та місцевими органами виконавчої влади, відповідальними за функціонування окремих державних систем захисту та реагування, відповідальними за формування, забезпечення та реалізацію державної політики у захисту об'єктів критичної інфраструктури по секторах.

III. Місцевий рівень – реалізується органами місцевого самоврядування (в межах повноважень), а також місцевими органами виконавчої влади, а в умовах воєнного стану – військово-цивільними адміністраціями.

IV. Об'єктовий рівень – здійснюється безпосередньо операторами критичної інфраструктури.

Відповідно до Закону «Про критичну інфраструктуру» [60], державна політика у сфері захисту критичної інфраструктури передбачає мобілізацію безпекових заходів нормативно-правового, організаційного, інженерно-технічного, інформаційно-аналітичного, ресурсного та методологічного характеру у єдиний комплекс.

Зазначимо, що у системі складових гарантування національної безпеки Г. Ю. Зубко пропонує ідентифікувати інфраструктурну значущість автономних державних систем захисту критичної інфраструктури, серед яких:

1. Єдина державна система цивільного захисту (ЄДСЦЗ) – захисна інфраструктурна значущість;
2. Єдина система реагування, запобігання, й припинення терористичних актів та мінімізації їх наслідків (ЄСЗРПТА) – антитерористична інфраструктурна значущість;
3. Державна система фізичного захисту (ДСФЗ) – фізична інфраструктурна значущість;
4. Національна система кібербезпеки (НСК) – кібербезпекова інфраструктурна значущість;
5. Державна служба забезпечення національної системи стійкості та захисту критичної інфраструктури України (ДСЗКІ) – стійкісна інфраструктурна значущість [217];

6. Система національної безпеки (СНБ) – безпекова інфраструктурна значущість;

7. Система територіальної оборони (СТРО) – оборонна інфраструктурна значущість;

8. Система правоохоронних органів (СПО) – правоохоронна інфраструктурна значущість [82, с. 40].

Особливої уваги вимагає вивчення інституційно-правових засад функціонування Національної системи кібербезпеки (НСК), що обумовлено пріоритетністю підвищення кібербезпеки та безпеки даних відповідно до найкращих практик. Даний напрям захисту критичної інфраструктури регулюють наступні нормативно-правові акти:

1. Закон України № 2163-VIII. від 05.10.2017 р. «Про основні засади забезпечення кібербезпеки України» [68], ст. 8 якого визначає предикат Національної системи кібербезпеки як «…сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури» [68].

2. Указ Президента України від № 447/2021 26.08.2021 р. «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 р. «Про Стратегію кібербезпеки України» [268], що увів в дію рішення РНБО України від 14 травня 2021 р. та затвердив «Стратегію кібербезпеки України», яка визначає завдання, серед яких забезпечення захисту критичної інформаційної інфраструктури від кібератак та серед проблем визнає недостатню убезпеченість від кіберзагроз об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів.

3. Закон України № 3475-IV від 23.02.2006 р. «Про Державну службу спеціального зв'язку та захисту інформації України» [56], що визначає статус, основні завдання, принципи та особливості функціонування Державної служби спеціального зв'язку та захисту інформації України.

4. Наказ Адміністрації Держспецзв'язку від 10.06.2008 № 94, яким утверджено «Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [125].

5. Постанова КМУ № 1772 від 16.11.2002 р. «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних

системах», якою затверджено «Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах», що прийнята з метою підвищення рівня захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних системах [208].

6. Постанова КМУ № 373 від 29.03.2006 р. «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» [212], якою затверджено «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» Правила визначають загальні вимоги та організаційні засади забезпечення захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах [212].

7. Наказ Адміністрації Держспецзв'язку № 660 від 02.12.2014 р. «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» [126], яким затверджено «Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [126], що регламентував правові та організаційні засади проведення оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах державних органів, органів місцевого самоврядування, військових формувань та підприємств, установ і організацій критичної інфраструктури.

8. Наказ Адміністрації Держспецзв'язку № 20 від 15.01.2016 р. «Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті» [127], яким затверджено «Порядок сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті», що визначає організаційні засади даного процесу.

9. Постанова КМУ № 563 від 23.08.2016 р. «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» [210], якою затверджено «Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» [210], яким регламентовано механізм створення переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави.

10. Постанова КМУ № 518 від 19.06.2019 р. «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» прийнята відповідно до ч.2 ст.6 Закону України «Про основні засади забезпечення кібербезпеки України» та регламентує

організаційно-методологічні, технічні та технологічні умови кіберзахисту об’єктів критичної інфраструктури, що є обов’язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об’єктів критичної інфраструктури [201].

11. Постанова КМУ № 1295 від 23.12.2020 р. «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» [191], що затвердила Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки та визначила відповідальним за функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки Державний центр кіберзахисту Державної служби спеціального зв’язку та захисту інформації.

12. Наказ Міністерства енергетики України № 417 від 15.12.2022 р. «Про Вимоги з кібербезпеки паливно-енергетичного сектору критичної інфраструктури» [128] виданий відповідно до п.14 Загальних вимог до кіберзахисту об’єктів критичної інфраструктури з метою реалізації державної політики захисту об’єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури. Затверджені вимоги визначають заходи кіберзахисту об’єктів критичної інформаційної інфраструктури, що експлуатуються на об’єктах критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури для досягнення конкретного цільового стану кібербезпеки.

13. Постанова КМУ № 257 від 24.03.2023 р. «Деякі питання проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури», що прийнята у відповідності до ч.3 ст. 6 Закону України «Про основні засади забезпечення кібербезпеки України» та ввела в дію Порядок проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури, що визначає механізм організації та проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури та вимоги до його проведення [197].

14. Постанова КМУ № 1175 від 14.10.2022 р. «Деякі питання подання інформації у сфері захисту критичної інфраструктури» [196], що прийнята відповідно до ч.2 ст.19 та п.4 ч.4 ст.21 Закону України «Про критичну інфраструктуру» та затвердила форму річного звіту про виконання секторальним органом повноважень та форму річного звіту про виконання оператором критичної інфраструктури повноважень.

15. Постанова КМУ № 1174 від 14.10.2022 р. «Про затвердження Регламенту обміну інформацією між суб’єктами національної системи захисту критичної інфраструктури» [215], що прийнята відповідно до ч.4 ст.13 Закону України «Про критичну інфраструктуру» та затвердила Регламент інформаційного обміну між суб’єктним складом національної системи захисту критичної інфраструктури, яким визначено механізм

інформаційного реверсу між суб'єктами, залученими до захисту критичної інфраструктури з метою забезпечення її захисту та стійкості.

16. Указ Президента України № 56/2022 від 16.02.2022 р. «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки»« [267], яким утверджено Стратегію забезпечення державної безпеки, яка зафіксувала перелік загроз об'єктам критичної інфраструктури у сфері інформаційної та кібербезпеки (п.19) та основних завдань державної політики (п.24), серед яких у пріоритеті подальший розвиток і посилення спроможності національної системи кібербезпеки, оптимізація координації її суб'єктів з метою ефективної протидії кіберзагрозам у сучасному безпековому середовищі, створення ефективної системи обміну інформацією між суб'єктами забезпечення державної безпеки та запровадження дієвих механізмів доступу суб'єктів забезпечення державної безпеки до державних електронних інформаційних ресурсів та автоматизованих інформаційних і довідкових систем, реєстрів, банків (баз) даних [267].

Реалізація державної політики у інших сферах захисту критичної інфраструктури інспірує необхідність інституційно-правових заходів реалізовуваних органами державної влади в межах яких розроблено та введено у дію низку законодавчих, нормативних документів та методичних регламентів, що закладають основу для безперебійності функціонування об'єктів критичної інфраструктури. Відзначимо основоположні інституційно-правові зміни, серед яких:

1. Постанова КМУ «Про внесення змін до переліку секторів критичної інфраструктури» № 455 від 09.06.2023 р. [198] доповнила позицію «Харчова промисловість та агропромисловий комплекс» у графі «Тип основної послуги» пунктом «виробництвом ветеринарних препаратів та експлуатацією елеваторів»;

2. Постанова КМУ № 1109 від 09.10.2020 р. «Деякі питання об'єктів критичної інфраструктури» [78] є однією із найважливіших нормативних актів, прийнята відповідно до ч.1 ст.8, ч.3 ст. 9 та ч.4 ст.10 Закону України «Про критичну інфраструктуру» та розроблена з урахуванням вимог законодавства ЄС – Директиви Європейського Парламенту та Ради (ЄС) 2016/1148 від 06.07.2019 р. «Про заходи високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» [35], Директиви Ради 2008/114/ЄС від 08.12.2008 р. «Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту» [36]. Постанова одночасно урегулювала цілий ряд інституційно-правових аспектів у напрямку реалізації державної політики у сфері захисту критичної інфраструктури, а саме ввела в дію Порядок віднесення об'єктів до критичної інфраструктури, Методику категоризації об'єктів критичної інфраструктури та Перелік секторів критичної інфраструктури, який гармонізовано з відповідним переліком, наведеним у Директиві ЄС

2016/1148 [36].

3. Постанова КМУ «Деякі питання об’єктів критичної інформаційної інфраструктури» № 943 від 09.10.2020 р. прийнята відповідно до абзацу 1 ч.3 ст.4 Закону України «Про основні засади забезпечення кібербезпеки України» та вводить в дію Порядок формування переліку об’єктів критичної інформаційної інфраструктури та Порядок внесення об’єктів критичної інформаційної інфраструктури до державного Реєстру об’єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування [192].

4. Наказ Адміністрації державної служби спеціального зв’язку та захисту інформації України № 23 від 15.01.2021 р. «Про затвердження Методичних рекомендацій щодо категоризації об’єктів критичної інфраструктури» [124]. Даний нормативний акт став логічним доповненням Методики категоризації об’єктів критичної інфраструктури (п.5), затвердженої постановою КМУ № 1109 від 09.10.2020 р. [193] та розроблена на виконання вимог ст.6 Закону України «Про основні засади забезпечення кібербезпеки України» [68]. Присвоєння об’єктам інфраструктури статусу критичного проводиться за сукупністю відповідних критеріїв, що ідентифікують їх соціальну, економічну, політичну та екологічну значимість для забезпечення безпеки громадян, оборони країни, суспільства, правопорядку, надання життєво-важливих послуг, свідчать про існування для них ризиків та загроз, перспективи виникнення деструктивних ситуацій, людський фактор чи природні лиха, припинення функціонування, тривалість робіт для ліквідації негативних наслідків та повної регенерації потужностей штатного режиму. Визначено предикат рівня критичності як «відносної міри важливості об’єктів критичної інфраструктури, якою враховується вплив раптового припинення функціонування або функціонального збою на безпеку постачання, забезпечення суспільства важливими товарами і послугами» [124] Для визначення категорії об’єкта критичної інфраструктури уповноважені органи у своїх секторах разом з операторами критичної інфраструктури проводять бальну оцінку критичності кожного об’єкта критичної інфраструктури за допомогою форм із секторальними та міжсекторальними критеріями визначення рівня негативного впливу. Зазначені критерії враховують важливість об’єкта критичної інфраструктури на основі аналізу потенційної шкоди, яку суспільство, навколишнє середовище, економіка та національна безпека держави можуть зазнати внаслідок порушення або припинення функціонування об’єкта інфраструктури. Важливість об’єктів інфраструктури оцінюється за допомогою низки секторальних та міжсекторальних критеріїв [193].

5. Постанова КМУ № 818 від 04.08.2023 р. «Деякі питання паспортизації об’єктів критичної інфраструктури» [195] затвердила «Порядок розроблення та погодження паспорта безпеки на об’єкт критичної інфраструктури» [195], що передбачає ч.4 ст.12 Закону України

«Про критичну інфраструктуру» [60].

6. Постанова КМУ № 821 від 22.07.2022 р. «Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури» [209] затвердила форму Акту оцінки стану захищеності об'єкта критичної інфраструктури, що складається у результаті проведення моніторингу рівня безпеки даних об'єктів, відповідно вимог ч.4 ст. 23 Закону України «Про критичну інфраструктуру» [60].

7. Постанова Правління НБУ № 151 від 30.11.2020 р. «Про затвердження Положення про визначення об'єктів критичної інфраструктури в банківській системі України» [219] що встановила критерії та порядок віднесення банків України до об'єктів критичної інфраструктури, а також порядок ведення переліку таких об'єктів в банківській системі України та переліків об'єктів критичної інформаційної інфраструктури в банках, обсяги та порядок подання банками інформації, необхідної для ведення реєстру об'єктів критичної інформаційної інфраструктури.

8. Постанова КМУ № 415 від 28.04.2023 р. «Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього» [207] Положеннями переважної більшості зазначених інституцій передбачено формування та ведення Реєстру об'єктів критичної інфраструктури, однак Уряд ухвалив відповідну Постанову лише 8 квітня 2023 року, чим виконав вимоги ст.11 Закону України «Про критичну інфраструктуру», прийнятого у 2021 році [60]. Цей документ регламентував процедуру включення об'єктів та формування і ведення Реєстру, а також внесення до нього інформації про ці об'єкти. Постанова регламентує умови доступу до даних Реєстру, що має на меті «..узгодження дій суб'єктів національної системи захисту критичної інфраструктури» [207]. Аналіз нормативного акту дозволив відзначити наступні ключові положення:

I. Визначено поняття «власник об'єкта критичної інфраструктури» як «юридична особа будь-якої форми власності або фізична особа-підприємець, якій на праві власності належить об'єкт критичної інфраструктури». Варто акцентувати увагу, що у даному формулюванні регламентовано лише приватну форму власності, однак у «Порядку розроблення та погодження паспорта безпеки на об'єкт критичної інфраструктури» [195] дана умова розширена і включає також інші речові права – господарське відання та оперативне управління.

II. Адміністратором, власником та держателем Реєстру визначено державу в особі Уповноваженого органу у сфері захисту критичної інфраструктури України (Держспецзв'язку), який проводить облік, узагальнення, систематизацію, аналіз та надання інформації, а інформацію ідентифіковано у якості державного ресурсу.

III. Користувачами Реєстру є суб'єкти національної системи захисту критичної інфраструктури.

IV. До Реєстру вносяться відомості про секторальний орган, який подає інформацію, оператора критичної інфраструктури, документ, на підставі якого ідентифіковано та категоризовано об'єкт критичної інфраструктури, об'єкт критичної інфраструктури, погодження (перегляд) паспорта безпеки на об'єкт критичної інфраструктури.

V. Дані про об'єкти критичної інфраструктури, що внесені до Реєстру, є публічними та безкоштовними, окрім інформації з обмеженим доступом. Зауважимо, що війна в Україні внесла певні корективи до даного регламенту і частину даних про критичну інфраструктуру було закрито в інтересах національної безпеки. Так, НКРЕКП внесла зміни до своєї Постанови № 349 від 26.03.2022 р. «Щодо захисту інформації, яка в умовах воєнного стану може бути віднесена до інформації з обмеженим доступом, у тому числі щодо об'єктів критичної інфраструктури» [218]. У документі визначено, що «під час дії воєнного стану в Україні та до останнього дня місяця, наступного за місяцем припинення або скасування воєнного стану, на веб-сайтах ліцензіатів повинен бути закритий доступ» [218]. Частково була прихована також інформація з приводу інших секторів – освітніх і медичних закладів, кадастру, системи життєзабезпечення та захисту населення. Такі обмеження є цілком виправдані й повністю відповідають національним інтересам та особливостям регулювання відносин у воєнний час.

VI. Інформація у Реєстрі розподілена на дві категорії доступу: відкриту (інформація про: секторальний орган, який подав інформацію, найменування, місцезнаходження, код ЄДРПОУ, форму власності, країну реєстрації, КВЕД основної діяльності оператора критичної інфраструктури, кінцевого бенефіціара, реєстровий номер об'єкта критичної інфраструктури, дату внесення інформації) та з обмеженим доступом (назва об'єкта критичної інфраструктури, категорія критичності, дата останнього оновлення інформації про об'єкт, дата затвердження паспорта безпеки, адреса місцезнаходження, кадастровий номер, найменування, місцезнаходження власника (суб'єкта управління) об'єкта, форма власності, країна реєстрації власника, сектор, підсектор, тип основної послуги, життєво важлива функція та послуга, яку надає об'єкт, назва секторального органу, який погодив паспорт безпеки, дата його погодження, дата погодження функціональними органами планів захисту від загроз, відомості про особу, відповідальну за організацію та забезпечення захисту об'єкта, додаткові відомості щодо об'єкта критичної інфраструктури.

VII. Секторальні органи подають окремо про кожен об'єкт критичної інфраструктури інформацію до Реєстру за формою. До повідомлення про внесення до Реєстру відомостей про об'єкт критичної інфраструктури додаються документи, що обґрунтовують розрахунок віднесення об'єкта критичної інфраструктури до однієї з категорій критичності, здійснений відповідно до Методики категоризації об'єктів критичної

інфраструктури [207]. Інформація про об’єкт критичної інфраструктури подається у місячний строк з моменту внесення об’єкта критичної інфраструктури до секторального переліку об’єктів критичної інфраструктури.

VIII. Об’єкт критичної інфраструктури виключається з Реєстру у зв’язку з невідповідністю такого об’єкта критеріям віднесення його до критичної інфраструктури [207].

Постановою КМУ № 415 визначено, що «оператори критичної інфраструктури протягом трьох місяців з дня внесення відомостей про об’єкт критичної інфраструктури до Реєстру об’єктів критичної інфраструктури забезпечують подання на погодження паспорта безпеки на об’єкт до відповідного державного органу, визначеного законодавством відповідальним за забезпечення формування та реалізацію державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури» [207].

Вкрай важливою процедурою у напрямку упорядкування інституційно-правових аспектів провадження державної політики у сфері захисту критичної інфраструктури стала розробка й погодження паспорта безпеки об’єкту критичної інфраструктури. Порядок паспортизації було затверджено Постановою КМУ «Деякі питання паспортизації об’єктів критичної інфраструктури» № 818 від 04.08.2023 р., що вимагає ч.4 ст.12 Закону України «Про критичну інфраструктуру». Цей Порядок визначає вимоги до його розробки оператором критичної інфраструктури та його складових, а також механізм погодження секторальними і функціональними органами у сфері захисту критичної інфраструктури [195]. Даний документ містить загальну характеристику об’єкта критичної інфраструктури, плани захисту та акти оцінки стану захищеності об’єкта критичної інфраструктури.

Акт оцінки стану захищеності об’єкта критичної інфраструктури складається за формою, визначеною в Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури, затвердженому Постановою КМУ № 821від 22.07.2022 р. [209], яка відповідає вимогам ч.4 ст. 23 Закону України «Про критичну інфраструктуру» [60]. Документ відображає результати моніторингу безпеки об’єктів критичної інфраструктури, що проводиться один раз на три роки функціональними й секторальними органами у сфері захисту критичної інфраструктури.

План захисту (як складову паспорта безпеки) розробляє оператор за кожною із проектних загроз національного, секторального та об’єктового (у разі наявності) рівня відповідно до форм планів захисту та рекомендацій з розроблення планів захисту, що затверджуються відповідними функціональними органами у сфері захисту критичної інфраструктури щодо кожної проектної загрози. Відповідно до зазначених проектних загроз визначаються функціональні органи.

Варто відзначити привенційну значимість зазначених інституційних

новелизацій, оскільки Реєстр дає уявлення про спектр критично важливих інфраструктурних об'єктів та їх характеристики, а Паспорт безпеки містить такі важливі атрибути, як плани захисту та акти оцінки стану захищеності таких об'єктів. Акт оцінки стану захищеності, включає критерії оцінки стану захищеності, їх показники та методику оцінки стану захищеності визначає уповноважений орган у сфері захисту критичної інфраструктури [195]. Вони підлягають обов'язковому погодженню відповідними функціональними органами, до яких, зокрема, належать МОЗ, Міноборони, Держспецзв'язку, ДСНС, Національна поліція. А у разі загроз диверсій, терористичних актів, актів кібертероризму підлягають обов'язковому погодженню СБУ, Національною гвардією, іншими державними органами [195].

Важливим кроком також є ідентифікація проєктних загроз та ризиків об'єкта критичної інфраструктури, що представляє собою оформлений за встановленим зразком протокол, який регламентує характеристики і властивості потенційних та реальних загроз об'єкту критичної інфраструктури, на зниження ризиків настання яких має бути орієнтоване функціонування системи захисту критичної інфраструктури, візує Уповноважений орган у сфері захисту критичної інфраструктури України. Органи державної влади, призначені відповідальними за роботу окремих державних сил реагування «формують пропозиції щодо національних та секторальних проектних ризиків і загроз» [60]. Проектні загрози критичній інфраструктурі секторального та об'єктового рівня розробляють та затверджують Секторальні органи.

Задля забезпечення функціонування зазначеної системи важливим є регламентація інформаційного забезпечення. Відповідно до ч.4 ст.13 Закону України «Про критичну інфраструктуру» [60] Кабінет Міністрів України Постановою № 1174 від 14.10.2022 р. затвердив «Регламент обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури» [215]. Даний нормативний акт регламентує інформаційну взаємодію, що забезпечується шляхом послідовного інформаційного реверсу між суб'єктами національної системи захисту критичної інфраструктури, що здійснюється відповідальними особами, визначеними такими суб'єктами, з використанням засобів електронних комунікацій, національної системи конфіденційного зв'язку, спеціального зв'язку, шифрувального зв'язку та інформаційно-комунікаційних систем [215]. Обмін інформацією здійснюється послідовно між операторами критичної інфраструктури та секторальними органами, між секторальними органами та уповноваженим органом а також між секторальними органами та КМУ. Регламентує також порядок передачі інформації в умовах кризової ситуації та об'єктах критичної інфраструктури та інформування про хід ліквідації кризової ситуації на об'єктах критичної інфраструктури. Однак, не достатньо врегульованим залишається інформаційний реверс між службами реагування на

надзвичайні ситуації та об'єктами критичної інфраструктури стратегічного значення інформація про які належать до категорії державної таємниці. Отже, описана інституційно-інформаційна система ведення Реєстру, паспортизації та фіксації проєктних загроз об'єктів критичної інфраструктури та обміну інформацією потрібна для виявлення джерел небезпеки та також оцінки здатності систем захисту критичної інфраструктури протистояти усім типам загроз, тим самим активізуючи дієвість національної системи захисту критичної інфраструктури.

2.2. Аналіз інституційної спроможності національної системи захисту критичної інфраструктури

У сучасних умовах глобалізаційних процесів у світі, питання збереження власної суверенності виходить на авангард політики національної безпеки будь якої незалежної держави. У даному ракурсі наукових досліджень варто відзначити позицію Г. Ю. Зубка, який наголошує на необхідності забезпечення інфраструктурної ідентичності, інфраструктурної спроможності та інфраструктурної значущості з метою забезпечення втілення національних інтересів. Вчений стверджує, що у сфері функціонування об'єктів критичної інфраструктури Україна повинна володіти могутнім та системним інфраструктурним комплексом у тандемі із ефективною функціональною державною політикою [83, с. 215].

Сучасні безпекові виклики в умовах гібридних загроз безпековій парадигмі створюють небезпеку для суверенітету та територіальної цілісності України. У таких умовах ключового значення набуває процес захисту критичної інфраструктури у якості детермінанти національної безпеки, що вимагає якісно нового рівня державного управління безпекою критичної інфраструктури. Це у свою чергу інспірує забезпечення належного рівня інституційної спроможності публічних інституцій, що полягає в ефективному виконанні покладених на них функцій на усіх державно-управлінських рівнях.

Проаналізуємо сутнісне наповнення інтенції національної системи захисту критичної інфраструктури, яка утверджена Законом України «Про критичну інфраструктуру» [60] як «сукупність органів управління, сил та засобів центральних і місцевих органів виконавчої влади (військово-цивільних адміністрацій – у разі утворення), органів місцевого самоврядування, операторів критичної інфраструктури, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури» [60]. Дане формулювання вважаємо оптимальним, оскільки воно передбачає залучення до національної системи захисту критичної інфраструктури військово-цивільних адміністрацій та операторів критичної інфраструктури.

Аналіз інституційної спроможності національної системи захисту критичної інфраструктури варто розпочати із трактування інституційного розвитку на рівні реалізації державної політики, який О. Г. Рось ідентифікує як системний розвиток організаційних структур публічної влади, оновлення форм і методів діяльності, механізмів і засобів їх взаємодії [232, с. 98].

Європейська Комісія відзначає, що зміцнення інституційної спроможності національної системи захисту критичної інфраструктури орієнтовано передусім на інститути (системи і структури), однак зміцнення спроможності індивідів (тобто штату інституцій) може бути так само важливим для зміцнення здатності інститутів діяти більш ефективно і результативно [304, с. 5].

Організація економічного співробітництва та розвитку (OECD) визначає інституційну спроможність як суму організаційних, структурних та технічних систем, а також індивідуальні компетенції, які створюють та впроваджують політику, що відповідає потребам громадськості [339, с.77]. Згідно з позицією Світового банку, підвищення інституційної спроможності охоплює три основні види діяльності: підвищення кваліфікації, удосконалення процедур та зміцнення організаційної функціональності [174]. Проаналізований спектр наукових розвідок у вивченні інституційної спроможності національної системи захисту критичної інфраструктури дає підстави даний процес визначати у фокусі на спроможності структурних, організаційних, технічних систем та окремих індивідів, що включає розвиток навичок і компетенцій на всіх рівнях здійснення державної політики захисту критичної інфраструктури крізь діоптрій процесних інституцій, що включає правила, процедури, засоби, інструменти, методи, організацію і ресурси.

Вважаємо раціональним акцент, стосовно впливу на інституційну спроможність індивідуальних компетенцій фахівців які ініціюють та провадять державну політику, що відповідає потребам громадськості. Дану позицію підтримує і О. А. Дмитренко [37, с.50], який, досліджуючи феномен інституційної спроможності, акцентує увагу на евентуальнісних детермінантах комплексного виконання інститутами захисту критичної інфраструктури своїх функцій. Окрім зазначеного вище рівня компетенції фахівців у цій галузі, учений вважає доцільним охопити також наявність ресурсів, характер та обсяги поставлених завдань, рівень оперативності прийняття рішень в умовах системних змін [38, с. 154]. Узагальнивши проаналізовані наукові доробки, інституційну спроможність національної системи захисту критичної інфраструктури можемо визначити як комплементарність внутрішньої системи профільних інститутів та відповідних інституцій, що детермінує їх здатність синхронно забезпечувати захист об’єктів критичної інфраструктури з метою безперебійності їх функціонування. Виходячи із вищезазначеного, а також, опираючись на дослідження учених [239, с. 65], [336, с. 10] варто

виокремити тріаду базових індикаторів інституційної спроможності системи національного захисту критичної інфраструктури:

Внутрішня синхронізація – передбачає взаємну узгодженість інститутів усередині системи захисту критичної інфраструктури, тобто вузькоспеціалізованих структур безпеки, операторів критичних об'єктів.

Зовнішня компліментарність – розглядається як взаємоузгодженість та відповідність інституційної системи захисту критичної інфраструктури із системою безпеки та оборони в цілому, а з одного боку, а з іншого боку, із національною інституційною системою публічного управління, а також узгодженість із розвитком світових тенденцій державної політики у сфері захисту критичної інфраструктури.

Конгруентність внутрішніх та зовнішніх складових інституційної системи – означає, що відносини всередині інститутів відповідають соціальним відносинам, які упорядковуються і підтримуються цими інститутами [336, с. 15].

Обґрунтування зазначених складових інституційної спроможності національної системи захисту критичної інфраструктури можна знайти у Концепції створення державної системи захисту критичної інфраструктури [230], пізніше його було доповнено Законом України «Про критичну інфраструктуру» [60]. Концепцією узагальнено поступальні кроки розвитку та удосконалення інституційної спроможності системи захисту критичної інфраструктури на національному, регіональному (галузевому), місцевому та об'єктовому рівнях, реалізація яких детермінує досягнення інституційної спроможності.

1.На національному рівні:

– визначення інституту, відповідального за формування та провадження державної політики у сфері захисту критичної інфраструктури;

– інтеграція засад державно-приватного партнерства у сферу захисту критичної інфраструктури, що посилить атавізм взаємодовіри, інформаційного обміну, інвестиційної мотивації у напрямку захисних заходів критичної інфраструктури;

– визначення повноважень, завдань та відповідальності державних органів у сфері захисту критичної інфраструктури, а також обов'язків, прав та відповідальності власників об'єктів критичної інфраструктури;

– організація взаємодії суб'єктів державної системи захисту критичної інфраструктури, обміну інформацією між ними про загрози критичній інфраструктурі, створення мережі ситуаційних центрів;

– створення системи підготовки та перепідготовки кадрів у сфері захисту критичної інфраструктури;

– затвердження переліку секторів критичної інфраструктури та визначення державних органів, що відповідатимуть за їх захист;

– визначення режимів функціонування державної системи захисту критичної інфраструктури та порядку їх ротації відповідно до змін у

безпековому середовищі;

– розробка і затвердження єдиної методології проведення оцінки загроз критичній інфраструктурі;

– розробка переліку об’єктів критичної інфраструктури;

– розробка методології та визначення критеріїв ідентифікації інфраструктурних об’єктів критичної інфраструктури, а також порядку їх паспортизації та категоризації;

– встановлення вимог до планування заходів щодо захисту критичної інфраструктури, включаючи аварійні плани, плани комунікації, плани регенерації об’єктів критичної інфраструктури, плани проведення здійснення навчань;

– здійснення категоризації та паспортизації об’єктів критичної інфраструктури;

– розробка та затвердження Національного плану стійкості та забезпечення захисту критичної інфраструктури.

2. На регіональному (галузевому) рівні:

– підготовка пропозицій щодо включення об’єктів інфраструктури до критичної інфраструктури;

– збір, аналіз та систематизація інформації про самі об’єкти критичної інфраструктури та їх функціонування;

– організація постійного обміну інформацією та моніторинг стану захищеності об’єктів критичної інфраструктури;

– розробка, у відповідно до законодавства, порядку реагування на кризові ситуації й загрози критичній інфраструктурі, а також забезпечити захист і стійкість критичної інфраструктури;

– здійснення превентивного інформування власників об’єктів критичної інфраструктури про загрози та надання їм експертної, інформаційно-консультативної та технічної допомоги;

– розробка стандартів та інших інституцій з питань захисту критичної інфраструктури у відповідних секторах;

– здійснення систематичних заходів державного нагляду, контролю та визначення стану захищеності об’єктів критичної інфраструктури;

– розробка і затвердження галузевих програм з протидії загрозам критичній інфраструктурі;

– проведення інспекцій об’єктів критичної інфраструктури з метою визначення їх рівня інформаційної та кібербезпеки;

– погодження та ведення обліку паспортів безпеки об’єктів критичної інфраструктури, а також карт ризику адміністративно-територіальних одиниць.

3. На місцевому рівні:

– розробка, затвердження і виконання локальних програм стійкості та забезпечення захисту критичної інфраструктури;

– розробка та погодження місцевих планів взаємодії суб’єктів

системи захисту об’єктів критичної інфраструктури та планів їх відновлення;

– розробка та виконання локальних програм із посилення стійкості громад до кризових ситуацій, пов’язаних із дизфункією об’єктів критичної інфраструктури;

– розробка та проєктування інженерно-технічних заходів захисту цивільного населення у містобудівній документації щодо безпечного розміщення та експлуатації об’єктів критичної інфраструктури.

4. На об’єктовому рівні:

– розробка та здійснення заходів із запобігання кризовим ситуаціям на об’єктах критичної інфраструктури;

– розробка та виконання об’єктових планів заходів щодо захисту і забезпечення стійкості об’єктів критичної інфраструктури;

– розробка, виконання та перегляд об’єктових програм протидії загрозам, а також програм забезпечення інформаційної безпеки та кібербезпеки;

– забезпечення виконання законних вимог конфіденційності інформації про об’єкти критичної інфраструктури;

– забезпечення відновлення функціональності об’єктів критичної інфраструктури в разі аварій та збоїв.

Передбачалося, що реалізація положень Концепції сприятиме досягненню інституційної спроможності національної системи захисту критичної інфраструктури, що визначатиметься:

– здатністю забезпечувати належний рівень захисту такої інфраструктури від усіх видів загроз;

– відпрацюванням ефективних механізмів реагування на кризові ситуації, та ліквідації їх наслідків, а також швидкому відновленню функціональності об’єктів критичної інфраструктури;

– налагодженням ефективної суб’єктної взаємодії інститутів, що входитимуть до складу національної системи захисту критичної інфраструктури та суспільства, місцевих громад, засобів масової інформації та профільних наукових установ;

– гармонізацією законодавства України та ЄС у сфері захисту критичної інфраструктури;

– розвитком міжнародного співробітництва України у сфері захисту критичної інфраструктури та світових систем безпеки.

Важливим кроком у досягненні інституційної спроможності національної системи захисту критичної інфраструктури є затвердження Розпорядженням КМУ № 825-р від 19.09.2023 р. «Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури» [228]. Він передбачає реалізацію стратегічного цільового пента-комплексу, а кожна із цілей передбачає відповідну еманацію архітектури її практичної реалізації у вигляді послідовних етапів. Проаналізуємо ключові положення зазначеної інституції:

Ціль 1 – передбачає правову регламентацію функціонування суб'єктів національної системи захисту критичної інфраструктури. Досягатиметься за рахунок уточнення завдань та повноважень інститутів національної системи захисту критичної інфраструктури шляхом модернізації нормативно-правової бази у сфері діяльності суб'єктів національної системи захисту критичної інфраструктури, фіксації вимог та забезпечення спостереження за рівнем захищеності об'єктів критичної інфраструктури за рахунок розроблення вимог щодо захисту об'єктів критичної інфраструктури та моніторингу і звітування щодо стану виконання вимог законодавства та з питань захисту критичної інфраструктури.

Ціль 2 – формування системи координування та інтеракції інститутів національної системи захисту критичної інфраструктури. Передбачає розробку порядку комунікації під час реагування на виникнення кризових ситуацій та їх загроз на критичній інфраструктурі за рахунок удосконалення протоколів взаємодії інфраструктури, та розробки планів співробітництва структурних підрозділів національної системи захисту критичної інфраструктури, забезпечення функціонування системи обміну інформацією за рахунок удосконалення регламенту інформаційного обміну між суб'єктами національної системи захисту критичної інфраструктури в разі порушення функціоналу об'єктів.

Ціль 3 – запровадження управління ризиками критичної інфраструктури. Передбачає періодичне проведення оцінки ризиків і загроз шляхом оцінки ризиків і загроз критичній інфраструктурі, управління рівнем захисту та розвиток у суб'єктів національної системи захисту критичної інфраструктури спроможностей реагувати на загрози, що виникають через їх проєктування.

Ціль 4 – посилення стійкості національної системи захисту критичної інфраструктури. Досягатиметься шляхом розробки механізмів співробітництва у проблемних ситуаціях на регіональному та секторальному рівнях, систематичного підвищення кваліфікації операторів критичної інфраструктури, локалізації наслідків надзвичайних ситуацій, удосконалення переліку спеціальностей та галузей знань, за якими проводиться підготовка здобувачів вищої освіти, новими позиціями сфери забезпечення захисту та стійкості критичної інфраструктури, ампліфікація стійкості суспільства до умов відсутності стабільних життєво-важливих послуг шляхом набуття територіальними громадами спроможностей підтримувати мінімальний рівень життєзабезпечення власними силами, та інтеграції механізму державної підтримки заходів з посилення стійкості населення у критичних ситуаціях

Ціль 5 – налагодження міжнародної співпраці. Передбачає розширення міжнародного співробітництва з іноземними державами та міжнародними організаціями у сфері захисту критичної інфраструктури

шляхом здійснення заходів колективної оборони [228].

Отже, зазначений документ дає підстави виокремити ряд ключових положень, що на наш погляд заслуговують особливої уваги щодо розвитку державної політики у сфері захисту критичної інфраструктури. Серед них:

– фіксація регламентів, норм та вимог до захищеності критичної інфраструктури;

– проєктування та дотримання планів заходів захисту і забезпечення стійкості, а також локалізації та ліквідації наслідків аварій;

– розробка та удосконалення кожні три роки планів інтеракції суб'єктів національної системи захисту критичної інфраструктури, розробка і затвердження секторальних планів співробітництва, планів взаємодії, відновлення, проведення навчань та тренувань і програм з протидії загрозам критичній інфраструктурі;

– проведення колективних тактико-спеціальних, командно-штабних навчань, спільних занять та тренувань із оборони, захисту, охорони, кібератак та припинення злочинних дій;

– удосконалення переліку спеціальностей та галузей знань, за якими проводиться підготовка здобувачів вищої освіти компетентностями щодо забезпечення захисту та стійкості критичної інфраструктури;

– розробка, затвердження та погодження зі стейкхолдерами програм навчання населення, місцевих планів взаємодії у кризовій ситуації та планів відновлення функціонування критичної інфраструктури.

Законом України «Про критичну інфраструктуру» [60] (ст.6.) також регламентовано основні принципи функціонування національної системи захисту критичної інфраструктури, дотримання яких сприяє досягненню нею інституційної спроможності. Серед них відзначимо забезпечення єдності методологічних засад, координованість, розвиток державно-приватного партнерства, гарантування безпеки, захисту та охорони інформації з обмеженим доступом, розширення міжнародного співробітництва.

Як стверджує G. D. Bhatt, поштовхом для розвитку та практичного удосконалення інституційної спроможності національної системи захисту критичної інфраструктури варто розглядати перегляд та врахування нових суспільно-економічних, безпекових та геополітичних реалій; використання сучасних форм і методів об'єктово-суб'єктної взаємодії; удосконалення виявлених прогалин у нормативно-правій базі [287, с. 122]. Цього можна досягнути за рахунок залучення до даного напрямку наукових установ та профільних закладів освіти.

Звернемо увагу на компетентності фахівців у галузі забезпечення впливу на інституційну спроможність індивідуальних компетенцій фахівців впливу на інституційну спроможність індивідуальних компетенцій фахівців. Результатами наукового пошуку M.Zollo та S.Winter визначають інституційну спроможність як результат

організованого навчання, через яке організація посилює свою здатність систематично генерувати і модифікувати операційну діяльність у напрямі підвищення управлінської ефективності [357, с. 3].

Отже, констатуючи результати проведеної наукової розвідки, варто зазначити, що одну із фундаментальних детермінант інституційної спроможності національної системи захисту критичної інфраструктури складає спектр компетенцій, якими володіють фахівці та оператори у даній галузі, а також наукова складова. Головними суб'єктами провадження державної політики у сфері захисту критичної інфраструктури являються органи публічної влади [283], котрі, як відомо, не проводять власних наукових досліджень, а знання, необхідні їм для реалізації даної діяльності, отримують лише в закладах вищої освіти та спеціалізованих установах підвищення кваліфікації, на основі чого формується їх рівень компетентності. Відзначимо, що рівень компетентності публічних службовців з питань захисту критичної інфраструктури обумовлюється наявністю відповідних освітньо-професійних та освітньо-наукових програм у закладах вищої освіти держави. Тому, варто припустити, що, що рівень інституційної спроможності національної системи захисту критичної інфраструктури напряму залежить від якості освіти та наявності й ефективності профільних науково-аналітичних центрів, що провадять практичні дослідження у цій сфері.

Відповідно має бути забезпечено взаємодію та співпрацю з науковими та навчальними установами у напрямі підвищення компетентності працівників органів публічного управління, тобто сформовано систему підготовки кадрів щодо захисту критичної інфраструктури. Нагадаємо, що Концепцією створення державної системи захисту критичної інфраструктури, схваленої Розпорядженням КМУ № 1009-р від 06.12.2017 р. [230], одним зі шляхів розв'язання зазначеної проблеми визначено «створення системи підготовки та перепідготовки кадрів у сфері захисту критичної інфраструктури» [230]. Окрім цього, Національний плану захисту та забезпечення безпеки та стійкості критичної інфраструктури [228] передбачає більш конкретизовані заходи, серед яких особливу увагу привертає посилення освітньої складової у забезпеченні спроможності системи забезпечення безпеки та стійкості критичної інфраструктури.

Прогалиною у компетентнісному векторі забезпечення інституційної спроможності національної системи захисту критичної інфраструктури вважаємо відсутність у Національному класифікаторі професій України [132] професії з питань державного управління у сфері захисту критичної інфраструктури та безпеки критичної інфраструктури вцілому. Аналізуючи зміст документу, констатуємо наявність професій із приналежністю до окремих секторів критичної інфраструктури:

соціальний захист населення (шифр 2446); цивільний захист (1120.1); захист інформації (1210.1); фізичний захист (сфера використання ядерної енергії) (1222.2); енергетична сфера (2143.2); електрохімічний захист (2146.2); захист інформації з обмеженим доступом (2149.2); захист секретної інформації (3439); радіаційний та хімічний захист (3439); газовий захист (5169); захист підземних трубопроводів (7241). Розділ 4.1 Класифікатора «законодавці», «вищі державні службовці», «менеджери» взагалі не представлений відповідними професіями з питань безпеки стратегічної інфраструктури. Також розділ 4.2 «професіонали» містить професії, пов'язані тільки з соціальним та цивільним захистом населення та захистом інформації, при цьому інші сектори критичної інфраструктури відсутні, що знижує інституційну спроможність національної системи захисту критичної інфраструктури.

Також варто звернути увагу на ст. 49 Закону України «Про Державну службу» [56], де передбачено наявність індивідуальних програм підвищення рівня професійної компетентності державного службовця, яка розробляється відомчою службою управління персоналом. Центральним органом виконавчої влади з провадження державної політики у сфері державної служби є Національне агентство України з питань державної служби, яке відповідно до покладених на нього завдань сприяє розвитку системи закладів освіти надає освітні послуги з підготовки, спеціалізації та підвищення кваліфікації державних службовців, а також організовує та координує підготовку здобувачів вищої освіти за освітнім ступенем магістра за спеціальністю D4 – «Публічне управління та адміністрування».

Ґрунтуючись на положеннях загальної теорії державного управління [44, с. 15], державну політику безпеки варто трактувати крізь діоптрій формотворчого виміру соціально-економічної системи, схильному до еклектичності внутрішніх зв'язків населення, об'єктів території, економіки, інфраструктури та управлінських інститутів [87, с. 190]. З огляду на вищезазначене, можна виділити ще один (найважливіший) вид інституційної здатності – стратегічну (багатофункціональну) здатність.

Аналізуючи сучасну структурно-функціональну характеристику вітчизняної державної політики у сфері захисту критичної інфраструктури, розглянемо спроможність ключового інституту – уповноваженого органу з питань захисту критичної інфраструктури України (Держспецзв'язку) [159]. Зробити це можемо на основі аналізу Звіту про відстеження результативності постанови КМУ № 1109 від 09.10.2020 р. «Деякі питання об'єктів критичної інфраструктури» [78] за підсумками 2022 року.

Згідно із даними, на листопад 2023 року було ідентифіковано, категоризовановано, утверджено та внесено до Реєстру:

– 159 об'єктів критичної інфраструктури паливно-енергетичного

сектору, відповідальний секторальний орган – Міністерство енергетики України;

– 5 об'єктів критичної інфраструктури відповідальний секторальний орган – Міністерством з питань стратегічних галузей промисловості України;

– 3 об'єкта критичної інфраструктури відповідальний секторальний орган – Міністерство охорони здоров'я України та Міністерство розвитку громад та територій України.

За останнім пунктом варто відзначити, що перелік наразі створений, проте, дані до Держспецзв'язку ще не подано. Окрім цього іншими секторальними органами у сфері захисту критичної інфраструктури перелік таких об'єктів досі не сформовано по своїх секторах (підсекторах). Отже, за результатами аналізу зазначеного Звіту, резюмуємо, що відомості відносно секторальних переліків об'єктів критичної інфраструктури надали до Адміністрації Держспецзв'язку лише чотири міністерства: Міністерство енергетики, Міністерство з питань стратегічних галузей промисловості, Міністерством розвитку громад та територій, Міністерство охорони здоров'я. Відносно перспектив інформаційного наповнення Реєстру об'єктів критичної інфраструктури у звіті Держспецзвязку вказано, що «на даний час продовжується робота над формуванням секторальних та зведеного переліків об'єктів критичної інфраструктури на основі наданої інформації від міністерств, центральних органів виконавчої влади, державних органів, операторів критичної інфраструктури, фізичних та юридичних осіб які є потенційно визначеними об'єктами критичної інфраструктури. Надається консультативна та методична допомога щодо ідентифікації, категоризації та віднесення об'єктів до об'єктів критичної інфраструктури» [78].

На сайті Держспецзв'язку [159] наголошується, що Адміністрацією перед Кабміном неодноразово ставилося питання щодо невиконання секторальними органами у сфері захисту критичної інфраструктури, завдань з ідентифікації та категоризації об'єктів визначеними Постановою по відповідним секторам (підсекторам). Даний факт можна вважати підтвердженням низької інституційної спроможності даних інститутів. Також уповноваженим органом з питань захисту критичної інфраструктури України встановлено, що оцінка результатів та ступеня досягнення визначених цілей із наповнення Реєстру об'єктів критичної інфраструктури проводитиметься з інтервалом у три роки після проведення повторного відстеження. Даний термін вважаємо за необхідне скоротити, з метою активізації даного процесу, оскільки наступні перевірки відбудуться не раніше 2026 року. Зауважимо, що відповідальність за безпеку об'єкта несе його оператор, а держава не має повноважень втручатися у безпеку приватних об'єктів критичної інфраструктури та може бути лише партнером у її забезпеченні [60]. У

такому випадку вважаємо, що оперативність ідентифікації та категоризації об'єктів інфраструктури як критично важливих сприятиме посиленню дієвості державної політики у сфері захисту критичної інфраструктури.

Зазначимо, що експліцитність інституційної спроможності національної системи захисту критичної інфраструктури імплікує комплементарність ряду паралельно функціонуючих систем:

1. Єдиної державної системи цивільного захисту (ЄДСЦЗ). Представляє собою об'єднання сил і засобів центральних та місцевих органів виконавчої влади, органів управління, виконавчих органів рад, підприємств, інших установ та організацій, котрі забезпечують реалізацію державної політики у сфері цивільного захисту. В межах ЄДСЦЗ центральними органами виконавчої влади у відповідних сферах суспільного життя створюються функціональні та територіальні підсистеми [206].

2. Єдина державна система запобігання, реагування та припинення терористичних актів і мінімізації їх наслідків (ЄСЗРПТА). Інституційну спроможність системи протидії тероризму в Україні регламентують Конституція та Закони «Про боротьбу з тероризмом» [52]. Силами протидії тероризму (СПТ) є, перш за все, спеціально уповноважені Урядом суб'єкти виконавчої влади у питаннях протидії тероризму і захисту населення, об'єктів критичної інфраструктури та територій від загроз терористичного характеру: СБУ, МВС, ДСНС. Одним із основоположних органів у цій системі є Служба безпеки України. Для цього у своїй структурі містить Антитерористичний центр (АТЦ), сформований у грудні 1998 року Указом Президента України № 1343/98 від 11.12.1998 р. «Про Антитерористичний центр» [272]. АТЦ регулює діяльність суб'єктів боротьби з тероризмом з метою протидії терактам та запобігання диверсіям на об'єктах критичної інфраструктури.

До компетенції названих сил входять завдання ліквідації та попередження наслідків, викликаних терористичними акціями на об'єктах критичної інфраструктури. запобігання терористичній діяльності на об'єктах критичної інфраструктури, у тому числі превенція терактів; сповіщення населення про загрози можливих терактів на об'єктах критичної інфраструктури; убезпечення об'єктів критичної інфраструктури від потенційних терористичних дій. Серед основних заходів варто зазначити:

– проведення комплексних перевірок антитерористичної захищеності (уразливості) об'єктів критичної інфраструктури та їх категорування за ступенем потенційної небезпеки;

– залучення до обов'язкової антитерористичної паспортизації об'єктів критичної інфраструктури в терористичному відношенні;

– підготовка списку об'єктів критичної інфраструктури особливо уразливих та небезпечних в терористичному плані;

– розробка та подання антитерористичної комісії на затвердження методичних рекомендацій щодо реагування на кризові ситуації, які виникають внаслідок диверсійно-терористичних актів на об'єктах критичної інфраструктури;

– залучення до розробки державних стандартів, нормативів та інших обов'язкових вимог відносно антитерористичної захищеності об'єктів критичної інфраструктури;

– коригування організаційних, режимних та оперативних заходів по організації антитерористичної захищеності об'єктів критичної інфраструктури на підставі розробки моделі загроз;

– організація систематичного проведення з персоналом і співробітниками охорони об'єктів відпрацювань порядку дій при виникненні загроз терористичних актів і в умовах їх настання.

3. Державна система фізичного захисту (ДСФЗ). Відповідно до Закону України № 2064-III від 19.10.2000 р. «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» [75] фізичний захист визначено як «діяльність у сфері використання ядерної енергії, спрямована на забезпечення захищеності ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання та на зміцнення режиму нерозповсюдження ядерної зброї» [75]. До об'єктів ДСФЗ включено ядерні об'єкти та установки, призначені для поводження з радіоактивними відходами, радіоактивні відходи, ядерні матеріали, радіоактивні матеріали, виявлені в незаконному обігу, інші джерела іонізуючого випромінювання [211]. Функціонування даної системи ґрунтується на результатах оцінки загроз вчинення диверсій.

До суб'єктів ДСФЗ належать: Державна інспекція ядерного регулювання України, центральні та місцеві органи виконавчої влади, Національна гвардія України, Національна академія наук України щодо фізичного захисту, СБУ, а також ліцензіати, які беруть участь у забезпеченні фізичного захисту.

4. Національна система кібербезпеки (НСК). Згідно ст.8 Закону України «Про основні засади забезпечення кібербезпеки України» [68] національна система кібербезпеки – «це сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури» [68].

Основними суб'єктами НСК є Держспецзв'язку, СБУ, НБУ,

Національна поліція України, розвідувальні органи, Міністерство оборони України та Генеральний штаб ЗСУ. Координатором реалізації цієї Стратегії є робочий орган РНБО України – Національний координаційний центр кібербезпеки [242].

Важливим кроком у ампліфікації інституційної спроможності Національної системи кібербезпеки стало рішення РНБО України від 14.05.2021 р. «Про Стратегію кібербезпеки України» [268], яку ввів у дію Указ Президента України №447 від 14.05.2021 р. 30 грудня 2021 року, розглянувши проект Плану реалізації Стратегії кібербезпеки України, який був поданий Національним координаційним центром кібербезпеки, РНБО його схвалила та Указом Президента України № 37/2022 від 01.02.2022 р. було введено в дію. Головним тезисом зазначеної інституції є пріоритет у посиленні спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному динамічному середовищі. Гібридну агресію російської федерації проти України у кіберпросторі визначено першочерговою загрозою для критичної інфраструктури. Кіберпростір визнано одним з можливих театрів воєнних дій у якому посилюється тенденція зі створення кібервійськ. До прямих завдань останніх віднесено «забезпечення захисту критичної інформаційної інфраструктури від кібератак», а також «проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об’єктів інфраструктури противника» [268].

Основними напрямами державної політики у напрямку забезпечення інституційної спроможності Національної системи кібербезпеки визначено: створення захищеного національного сегмента кіберпростору; запобігання втручанню у внутрішні справи України з боку інших країн, боротьба з кіберзлочинністю та кібертероризмом, укріплення обороноздатності в кіберпросторі, посилення стійкості кіберзахисту, дотримання міжнародних зобов’язань щодо боротьби з кіберзлочинністю та кібертероризмом [268].

Продовжуючи аналізувати інституційну спроможність національної системи захисту критичної інфраструктури, варто провести оцінку ефективності кіберзахисту критичних об’єктів. З цією метою звернемо увагу на інструмент вимірювання NCSI, який застосовують для оцінки потенціалу кібербезпеки країни ЄС на основі розрахунку Індексу національної спроможності кіберзахисту (НСК). Модель розроблено Академією електронного управління (eGA) [157]. Дана організація є спільною ініціативою Уряду Естонії, Інституту відкритого суспільства (OSI) та Програми розвитку Організації Об’єднаних Націй. Основні функції даного інституту полягають у висвітленні проблем кібербезпеки, які потребують уваги уряду, і в допомозі у розбудові національного

потенціалу кібербезпеки. NCSI – це інструмент для вимірювання та нарощування потенціалу національної кібербезпеки. NCSI вимірює готовність країн до запобігання реалізації фундаментальних кіберзагроз і готовність керувати кіберінцидентами, злочинами та масштабними кіберкризами. Фокус аналізу зосереджено на кіберпотужності національного рівня захисту об'єктів критичної інфраструктури та базується на ключових принципах:

– об'єднує результати всіх позитивно оцінених критеріїв;

– оцінка інституційної спроможності базується на чітко вимірних аспектах – законодавстві, організаційній спроможності, політиках захисту, форматах міжсекторальної співпраці, технологіях та їх ефективності;

– відстежується прогрес держави у порівнянні з іншими країнами;

– дозволяє порівняти розвиток кібербезпеки країн із глобальним цифровим розвитком;

– аналіз універсальний та сумісний із законодавством ЄС щодо кібербезпеки [157].

Індекс НСК включає оцінку 12 профілів національних спроможностей кібербезпеки, які організовані у три групи: загальні спроможності кібербезпеки, базові спроможності та спроможності управління інцидентами та кризами. Вони вимірюються за допомогою загалом 46 індикаторів, заснованих на фактичних даних, які включають законодавство, створені організації, формати співпраці, навчальні програми, тренування тощо [157]. Індекс розраховується у 5 кроків:

1. Визначення кіберзагроз національного рівня..
2. Визначення заходів та можливостей кібербезпеки.
3. Вибір важливих та вимірних аспектів.
4. Розробка показників кібербезпеки.
5. Групування показників кібербезпеки.

Відзначимо, що у десятку зі 176 країн із найвищою інституційною спроможністю кібербезпеки входять Греція, Чехія, Естонія, Іспанія, Литва, Франція, Фінляндія, Данія, Нідерланди та Німеччина.

Індекс НСК базується на квадро-комплексі вимірників спроможності державної політики у сфері кібербезпеки критичної інфраструктури:

1. Спроможність чинного законодавства – дієвість та повнота нормативно-правової бази (законів, постанов, наказів та ін.).

2. Спроможність діючих підрозділів захисту – ефективність існуючих організацій, департаментів, служб та ін.

3. Спроможність формату міжсекторальної співпраці – наявність та ліквідність створених комітетів, робочих груп та ін.

4. Спроможні результати – дієвість державної політики, заходів, технологій, веб-сайтів, програмного забезпечення та ін.

Загальну ієрархію набору показників розподілено на 3 категорії, 12 напрямків (табл.2.1) та 46 показників (Додаток А).

Таблиця 2.1 – Дані спроможності державної політики кіберзахисту об'єктів критичної інфраструктури України у 2023 році

Категорія спроможності	Напрямок спроможності	Бал спроможності	
		фактичне значення	максимальне значення
Загальні показники кібербезпеки	Розробка політики кібербезпеки	7	7
	Аналіз кіберзагроз та інформація	4	5
	Освіта та професійний розвиток	8	9
	Внесок у глобальну кібербезпеку	2	6
Базові показники кібербезпеки	Захист цифрових сервісів	1	5
	Захист основних послуг	6	6
	Електронна ідентифікація та довірчі послуги	9	9
	Захист персональних даних	4	4
Показники управління інцидентами та кризи	Реагування на кіберінциденти	4	6
	Управління кіберкризою	3	5
	Боротьба з кіберзлочинністю	9	9
	Військові кібероперації	1	6

Джерело: розраховано за даними [157]

Оцінка індексу НСК показує відсоток, який країна отримала від максимального значення показників. Максимальна оцінка NCSI завжди дорівнює 100 (100%), незалежно від того, додано чи видалено індикатори.

$$\text{Індекс НСК} = \frac{\sum \text{балів спроможності} * 100\%}{\sum \text{Максимальне значення балів спроможності}} \qquad (2.1.)$$

Окрім оцінки Індексу НСК, таблиця індексів також показує рівень цифрового розвитку (РЦР) шляхом обрахунку Індексу РЦР, який розраховується відповідно до індексу розвитку інноваційних комп'ютерних технологій (Індекс ІКТ) та індексу стійкості мереж (Індекс СМ). Індекс РЦР – це середній відсоток, який країна отримала від максимального значення обох індексів (СМ+ІКТ).

$$\text{Індекс РЦР} = \frac{\text{Індекс СМ (\%)} + \text{Індекс ІКТ(\%)}}{2} \qquad (2.2.)$$

Ще один індикатор – різниця між Індексом НСК та індексом РЦР (табл. 2.2).

Вказаний індекс показує зв'язок між спроможністю кіберзахисту критичної інфраструктури та рівнем цифровізації суспільства. Позитивний показник показує, що розвиток кібербезпеки відповідає або випереджає рівень цифрового розвитку, що демонструє спроможність кіберзахисту. Негативний результат показує, що цифрове суспільство країни є більш розвиненим, ніж сфера кібербезпеки, що ставить під загрозу спроможність кіберзахисту критичної інфраструктури

Таблиця 2.2 – Світовий рейтинг спроможності державної політики кіберзахисту об’єктів критичної інфраструктури на основі Індексу НСК у 2023 році

Місце в рангу	Країна	Індекс НСК	Індекс РЦР	Різниця
1.	Бельгія	**94,81**	74.07	20.74
2.	Литва	**93,51**	67,34	26.17
3.	Естонія	**93,51**	75,59	17.92
4.	Чехія	**90,91**	69.21	21.70
5.	Німеччина	**90,91**	80.01	10.90
6.	Румунія	**89,61**	59,84	29.77
7.	Греція	**89,61**	64.02	25.59
8.	Португалія	**89,61**	68,46	21.15
9.	Великобританія	**89,61**	79,96	9,65
10.	Іспанія	**88.31**	72.21	16.10
24.	**Україна**	**75,32**	**55,96**	**19.36**

Джерело: сформовано за даними [157]

Проведений аналіз показників спроможності національної системи захисту критичної інфраструктури в Україні на основі Індексу НСК у 2023 році, дозволило виявити наступні проблеми:

– освітні програми підготовки спеціалістів в країні не включають компетенції з кібербезпеки/комп’ютерної безпеки об’єктів критичної інфраструктури, а також відсутні спеціальності орієнтовані на захист об’єктів критичної інфраструктури вцілому;

– в Україні не розміщено жодного представництва регіональної або міжнародної організації з кібербезпеки, та безпеки об’єктів критичної інфраструктури;

– Україна не брала участі у співфінансуванні або співорганізації жодного проєкту з розбудови потенціалу захисту критичної інфраструктури для іншої країни за останні 3 роки;

– відсутність компетентного наглядового органу за результативністю державної політики у сфері захисту критичної інфраструктури;

– Урядом не розроблено Плану врегулювання кризових ситуацій на випадок масштабних кіберінцидентів та аварій на об’єктах критичної інфраструктури, не врегульовано законодавством порядок залучення волонтерів у сферу кібербезпеки та захисту критичної інфраструктури;

– Збройні Сили України не проводили в країні навчання з кібероперацій або навчання з компонентом кібероперацій протягом останніх 3 років;

– не прийнято закон про створення та функціонування у системі Міністерства оборони України кібервійськ;

– у національній системі захисту критичної інфраструктури відсутні підрозділи кібероперацій, Збройні сили України досі не мають підрозділу кібервійська та кіберкомандування, який би спеціалізувався на плануванні та

проведенні кібероперацій і спільних навчань з кіберполіцією із проведення кібероперацій;

– не сформовано перелік об'єктів критичної інформаційної інфраструктури та повільно проходить наповнення Реєстру об'єктів критичної інфраструктури;

– не розроблено дієву модель міжсекторальної співпраці у сфері захисту критичної інфраструктури та залучення стейкхолдерів на основі державно-приватного партнерства;

– брак фінансування, що не дозволяє державним інститутам у повній мірі займатися розробкою дієвих систем кіберзахисту, що вимагає залучення аутсорсу;

– відсутність державного мультиплексу, що в умовах війни не дозволяє в повній мірі контролювати медіа простір;

– відсутність державної інстанції, відповідальної за аналіз, обробку даних про інциденти (кризи) на об'єктах критичної інфраструктури та її структурування з метою обміну досвідом та створення програм міжсекторального співробітництва у сфері стійкості та захисту критичної інфраструктури.

Проведений аналіз інституційно-правових особливостей національної системи захисту критичної інфраструктури підтвердив необхідність сфокусувати увагу на проблемі обширності суб'єктного складу, що детермінує низьку скоординованість режимів роботи, процедур і планів реагування на різні комплекси ризиків і загроз у сфері захисту критичної інфраструктури. Окрім цього, визначені у планах і положеннях процедури й механізми інтеракції між суб'єктами національних систем безпеки і кризового реагування є недостатньо відтренованими та апробованими у прецедентах масштабних та системних кризових явищ. Це можна пояснити слабкою розвинутістю до цього часу в країні практики міжвідомчих та міжсекторальних тренувань і навчань на рівнях, вищих ніж об'єктовий. Напрацьована база інституції у напрямку посилення інституційної спроможності передбачає застосування більш виваженого підходу до нормопроектувальної діяльності із використання сучасної юридичної техніки та залученням до даних питань фахівців-юристів. Зокрема розробка вимог та комплексний моніторинг рівня захищеності об'єктів критичної інфраструктури надасть можливість досягти повноти та всебічності інституційної спроможності у виконанні вимог нормативно-правової бази, що детермінує цілісність і системність державної політики у цій сфері. При цьому, вважаємо доцільним посилити увагу до превентивних заходів забезпечення стійкості критичної інфраструктури та доповнити ними Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури. Тобто організаційно-правова структура Національний плану матиме на меті протидію усім видам загроз та ризиків і стане вагомим елементом сучасної національної системи захисту критичної інфраструктури.

2.3. Аналіз сучасної парадигми державної політики у сфері захисту критичної інфраструктури в умовах воєнного стану

Нинішня державна політика у сфері захисту об'єктів критичної інфраструктури в умовах воєнного стану виступає не окремою проблемою, а є органічною складовою вирішення комплексного завдання: формування системної державної парадигми політики національної безпеки, в рамках якої чільне місце посідає питання функціонування монолітної системи безпеки критичної інфраструктури в умовах військової агресії рф. Підтвердження даного судження можемо віднайти у Концепції створення державної системи захисту критичної інфраструктури [230], де прямо відзначалася необхідність інтеграції системного підходу в напрямок розв'язання проблеми на загальнодержавному рівні.

Акцентуємо увагу, що в умовах воєнного стану дієвість національних векторів державної політики у сфері захисту об'єктів критичної інфраструктури в Україні в теоретичному плані не вивчено. В такому випадку для створення раціональних структур управління вкрай важливим є осягнути складність і глибину актуальних проблем України в період воєнного стану та підвищених ризиків терактів на об'єктах критичної інфраструктури і врахувати їх при конструюванні архітектури майбутньої державної безпекової політики. При цьому, як зазначає А. В. Бєлоусов, необхідним є «зважений погляд на стан суспільства, його можливості та перспективи, ресурси, резерви, потенціал і джерела зростання» [6, с. 230].

Нагадаємо, що у зв'язку з російською військовою агресією, Президент України, на підставі ч.1 п.20 ст.106 Конституції України [96] та Закону України «Про правовий режим воєнного стану» [71] 24 лютого 2022 року підписав Указ, яким запровадив воєнний стан. Воєнний стан – це «особливий правовий режим, що вводиться в країні або в окремих її місцевостях у разі збройної агресії чи загрози нападу, небезпеки державній незалежності України, її територіальній цілісності та передбачає надання відповідним органам державної влади, військовому командуванню, військовим адміністраціям та органам місцевого самоврядування повноважень, необхідних для відвернення загрози, відсічі збройної агресії та забезпечення національної безпеки, усунення загрози небезпеки державній незалежності України, її територіальній цілісності, а також тимчасове, зумовлене загрозою, обмеження конституційних прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб із зазначенням строку дії цих обмежень» [71].

Варто зазначити, що прояви російської агресії систематично ігнорує міжнародні конвенції, у тому числі породжує аномію у сферах критичної інфраструктури [247]. До прикладу, в умовах війни більша частина об'єктів критичної інфраструктури знаходиться під захистом Додаткового протоколу до Женевських конвенцій від 12.07.1949 р.. Документ не містить власне формулювання терміну «критична інфраструктура», однак у ньому

зазначено, що «будь які цивільні об'єкти не повинні бути об'єктом нападу або репресалій» [39]. Окрім цього, документ забороняє знищувати або піддавати нападу чи виводити з ладу об'єкти, потрібні для виживання цивільного населення. Окрім цього, у Додатковому протоколі утверджено чіткий перелік споруд і установок, які заборонено піддавати нападам, оскільки вони містять приховану небезпеку (атомні електростанції, греблі, дамби). Отже, можемо зробити висновок, що оскільки об'єкти критичної інфраструктури в Україні цілком підпадають під юрисдикцію даного документу. Однак офіційні дані підтверджують, що за одну зі стратегічних цілей ворог обрав саме об'єкти цивільної критичної інфраструктури, розташовані у глибокому тилу у вигляді електропідстанцій, об'єктів гідроенергетики, теплової генерації та ін.. Дані факти спричинили примусове переміщення та знищення цивільного населення. Станом на травень 2023 р. приблизно 6,2 мільйона людей покинули Україну як біженці, а 5,4 мільйона осіб перебувають усередині країни в статусі внутрішньо переміщених осіб. Окрім цього, у вересні 2022 року російська влада провела референдуми на тимчасово окупованих територіях Донецької, Луганської та Херсонської і Запорізької областей. В рамках незаконної анексії, було захоплено ряд критично важливих інфраструктурних об'єктів [148].

З початку війни в Україні росія повністю зруйнувала більш ніж 700 об'єктів критичної інфраструктури, завдаючи найбільше атак, спрямованих на знищення енергетичної інфраструктури шляхом систематичних групових ракетних ударів з рубежів пуску над Каспійським морем, акваторії Чорного моря, а також військової авіації, застосовуючи широкий арсенал ракет (Х-101, Х-555, Іскандер, Циркон, Онікс, Калібр, Торнадо, С-300 та ін.), а також бойових безпілотних дронів-камікадзе «Shahed 136» та Mohajer 6 [161].

Авіаудари по енергетичним потужностям України почалися 10 жовтня. Наймасовіший обстріл об'єктів енергосистеми України ворог здійснив 15 листопада 2022 р., випустивши по території України близько 100 ракет. При цьому окремі із них було спрямовано на інфраструктуру АЕС. Зафіксовано перше загальнонаціональне відключення електроенергії. Це при тому, що завдяки відпрацюванню ППО вдається знищувати близько 80% запущених росією ракет та дронів [165]. Перші удари по енергосистемі спричинили дефіцит потужності на рівні 20%, а вцілому на початок 2023 року енергетичний сектор зазнав зниження функціональності на 61%. Таким чином довоєнна потужність у 36 Гігават (ГВт) знизилася до 13,9 ГВт. Окрім цього, близько 10 ГВт знаходиться на територіях під тимчасовим військовим контролем російської федерації, 6 ГВт з яких надходить із Запорізької АЕС. У таких умовах оператори були змушені обмежувати постачання електроенергії, щоб забезпечити роботу системи [165]. За оцінками Світового банку [174] та ПРООН [173], понад 12 мільйонів українців постраждали внаслідок пошкодження джерел енергії , що призводить до нормування електроенергії та опалення.

Подальші атаки на критичну інфраструктуру вплинули на роботу трьох

атомних електростанцій (у Нетішині, Южноукраїнську та Вараші). Додатково, знаходячись під окупацією, під постійним ризиком аварії функціонує найбільша в Європі атомна електростанція – Запорізька. Встановлені факти «інфраструктурного тероризму» становлять загрозу не лише для постачання електроенергії [148], але, у разі руйнування 15 реакторів українських АЕС, населення України, а також і Європи опиниться в умовах глобальної ядерної катастрофи, в десятки разів потужнішої ніж аварія у квітні 1986 року на Чорнобильській АЕС.

Наступною за масштабом деструктивною ситуацією у критичній інфраструктурі України, став підрив 6 червня.2023 р. дамби Каховської ГЕС в Херсонській області. Це призвело до масового затоплення території країни на площі близько 180 км². Висота рівнів води сягала 5-6 метрів. Даний інфраструктурний об'єкт був джерелом питної води для 700 тис. людей та зрошувальних систем 584 тис га с.-г. угідь на півдні України [148]. Даний терористичний акт спричинив хвилю додаткових пошкоджень інших об'єктів критичної інфраструктури (комунального сектора, сільського господарства та ін..). Прямі збитки від підриву Каховської ГЕС оцінюються у більш ніж 2 млрд дол. США із яких на критичну інфраструктуру припадає близько 950 млн дол. США [148].

Підрив Каховської ГЕС завдав додаткових збитків енергетиці у $586 млн, за рахунок безповоротної втрати ще 334,8 МВт потужностей. Таким чином, загальні збитки енергетиці сягнули $624 млн. Збитки, завдані транспортній інфраструктурі, сягнули $311 млн. За оцінками KSE Institute [148], понад 290 км доріг постраждали від повені. Знищення посівів сільськогосподарських культур, поголів'я худоби та риби завдали збитків агросектору на $25 млн. Орієнтовна сума збитків, завданих навколишньому середовищу, оцінюється у $1,5 млрд. Міністерства захисту довкілля та природних ресурсів [166].

З початку війни в Україні пошкоджень зазнали 18 аеропортів і цивільних аеродромів, 344 мости та мостові переходи, а також понад 25 тисяч кілометрів автомобільних шляхів. Сфера освіти, за оцінками KSE Institute [148], на початок вересня 2023 р. отримала збитків близько 10.1 млрд дол США. Загальна кількість пошкоджених та зруйнованих освітніх об'єктів вже перевищила 3,5 тис. із яких – понад 1,7 тис. закладів середньої освіти, більше 1,0 тис. – дошкільної та 586 – вищої освіти. Зруйновано або пошкоджено 1223 медзаклади, з них – 384 лікарні та 352 амбулаторії. На вересень 2023 року зруйновано або пошкоджено війною близько 167,2 тис житлових об'єктів із яких 19,1 тис. багатоквартирних та 147,8 тис. приватних будинків, а також 350 гуртожитків. Найбільше пошкоджених об'єктів критичної інфраструктури зафіксовано у Донецькій, Харківській, Луганській, Запорізькій, Херсонській Дніпропетровській, Одеській та Миколаївській областях. Дані регіони найбільше постраждали з точки зору прямої шкоди цивільній та критичній інфраструктурі та економічних наслідків.

За підсумками 2022 року, за оцінками Світового банку, ВВП України

скоротився на 29,2%, а рівень бідності зріс на 24,1%. Станом на 01.09.2023 р. загальна сума прямих задокументованих збитків, завдана критичній інфраструктурі України становила до $151,2 млрд., що більше на $700 млн, порівняно з червнем 2023 року [174].

Можемо дійти висновку, що всупереч міжнародним правилам війни, знищуючи цивільну критичну інфраструктуру України, агресор намагається маніпулювати морально-психологічним станом цивільного населення. Формуючи, тим самим, внутрішній страх потенційних проблем (відсутність взимку електроенергії, тепла, питної води, медичного обслуговування транспортного сполучення та ін.), намагається доповнити комплекс активних бойових дій та змусити українську владу прийняти свої умови.

Аналізуючи сучасну парадигму державної політики у сфері захисту критичної інфраструктури в умовах воєнного стану, варто звернути увагу на працю О. Ю. Кондратенка, який досліджуючи зовнішню геоекономічну політику щодо України акцентує увагу на намірах рф спрямувати військову агресію, на підрив суверенітету та незалежності України, а також перетворення її на «буферну зону» безпеки відносно євроатлантичних інститутів [94, с. 15]. В. А. Ліпкан, аналізуючи дані умови, звертає увагу також на ідеологічне просування деструктивного простору політикою країни-агресора наративи концепції «failed state» [113, с. 272]. Дане припущення у своїх дослідженнях ще у 2000 році висвітлив З. К. Бжезінський, який резюмував що «…більша частина сучасної російської політичної еліти вважає Україну неправомірно утвореною державою; не лише незаконним, а й неприроднім державним утворенням...» [7, с.14]. Отже, можна зробити висновки, що спроба військової експансії рф території незалежної України було лише питанням часу. У даному випадку варто навести аргумент важливості забезпечення стійкості критичної інфраструктури, а саме думку Г. Ю. Зубка [86, с. 80], який, вивчаючи тематику інфраструктурної війни, наголошує, що руйнування критичної інфраструктури супротивника відкриває шлях до встановлення домінування над країною. Ці прояви генерують нові стратегічні виклики у сфері державної політики захисту критичної інфраструктури та закладають науковий дискурс щодо можливостей, інтелектуальних спроможностей, технічних засобів та власних сил і ресурсів спроможних інспірувати підвалини протидії інформаційним та ідеологічним загрозам.

Аналізуючи ретроспективу формування сучасної парадигми державної політики у сфері захисту критичної інфраструктури слід узагальнити аксіоматичні припущення стосовно фатальних стратегічних прорахунків, які були допущені у безпековій політиці незалежної України:

1. Прийняття без'ядерного статусу. Ще в Декларації про державний суверенітет 16 липня 1990 року [32] передбачалося, що Україна прагне позбутися ядерної зброї. 14 січня 1994 року було підписано Тристоронню заяву Президентів України, США та Росії (Леонідом Кравчуком, Біллом Клінтоном і Борисом Єльциним), у якій було проголошено про те, що «всі

ядерні боєзаряди будуть виведені з території України до Росії для цілей їх наступного розукомплектування у якомога коротший можливий час» [262]. 5 грудня 1994 року у Будапешті , між Україною, Росією, Великою Британією та США було укладено Меморандум про гарантії безпеки у зв'язку з приєднанням України до Договору про нерозповсюдження ядерної зброї. Документ передбачав гарантії безпеки для України у зв'язку з набуттям нею неядерного статусу [117].

2. Позиція нейтралітету та позаблоковий статус. Окрім без'ядерного статусу, Україна вирішила заявити ще й про нейтральність, позаблоковість і багатовекторність. Це все було виписано в Конституції 1996 року [96], а додатково у Законі України «Про засади внутрішньої і зовнішньої політики» № 2411-VI від 01.07.2010 р. було прописано що «Україна як європейська позаблокова держава здійснює відкриту зовнішню політику і прагне співробітництва з усіма заінтересованими партнерами, уникаючи залежності від окремих держав, груп держав чи міжнародних структур» [58]. Головними причинами запровадження позаблокового статусу України В. Т. Шатун [280] вбачає:

– низьку результативність політики України у євроінтеграційному векторі;

– політичний та економічний тиск росії;

– вплив проросійського політичного лобі на безпекову політику України;

– низька політична дієздатність і конкурентоспроможність української управлінської еліти;

– низький рівень суспільної підтримки курсу на євроатлантичну інтеграцію через брак і недоліки інформаційної політики держави.

3. Демілітаризація та штучна деградація обороноздатності суб'єктів системи забезпечення національної безпеки та захисту критичної інфраструктури.

4. Трансформація корупції на системоутворюючий чинник функціонування системи державної влади [83, с. 180].

5. Підписання «Угоди між Україною і Російською Федерацією про статус та умови перебування воєнної бази Чорноморського флоту Російської Федерації на території України» [264], що укладалася на 20 років.

6. Не були вирішені питання розмежування між Росією та Україною акваторії Азовського моря та проведення лінії державного кордону в Керченській протоці.

Саме ці прогалини у державній політиці національної безпеки на нашу думку сприяли стратегічному дисбалансу військових сил у геопросторовому позиціонуванні України як незалежної держави та детермінували формування стратегічних загроз для критичної інфраструктури.

Український стратегічний шлях передбачає її повноцінне приєднання («повернення») до західної цивілізації, інтеграцію до європейських та євроатлантичних структур. У геоекономічному контексті, попри всі

труднощі, стратегічний курс України на вступ до ЄС покликаний забезпечити її економічне піднесення до рівня розвиненої високотехнологічної держави з достойним рівнем життя населення. Війна з росією фактично вирішує декілька важливих тактичних завдань у воєнній сфері:

1) знищення значних арсеналів застарілої радянської зброї;

2) знищення зброї країни-агресора;

3) постачання Україні в особливо великих розмірах надсучасної зброї за стандартами НАТО;

4) навчання персоналу щодо ефективного оперування сучасною зброєю, організацію підготовки, перепідготовки і підвищення кваліфікації щодо оперування сучасною зброєю;

5) оволодіння технікою і навичками ведення бою за стандартами НАТО.

Одним зі складників сучасної парадигми державної політики у сфері захисту критичної інфраструктури в умовах правового режиму воєнного стану є напрямки протидії агресії рф. До таких напрямків варто віднести:

– мілітарний дискурс для України на порядку денному міжнародної спільноти;

– персональні та економічні санкції проти росії;

– політика «стримування» росії західним державам на чолі зі США що проявляється допомогою Україні фінансами, новітніми технологіями, військовим спорядженням та ін. [29, с. 73];

– ефективна стратегія інформаційної війни та забезпечення поширення у світі правдивої інформації про події, що відбуваються нині в країні;

– досягнення сумісності Збройних Сил із збройними силами держав – членів НАТО, розвиток спроможностей щодо отримання допомоги від іноземних партнерів та її надання іншим державам озброєння України та підготовка військових відповідно до стандартів НАТО [224, с. 345];

– створення дієвої системи територіальної оборони з використанням кращого досвіду країн з розвинутою територіальною обороною; розвиток військово-патріотичного виховання;

– забезпечення ефективності оборонного менеджменту, професійності та вмотивованості персоналу сил оборони, чисельності воєнного резерву, розвинутої військової інфраструктури, логістики та запасів матеріальних засобів;

– активні навчання й тренування представників інститутів державної влади, сил безпеки та оборони, зокрема за участі іноземних держав та НАТО, щодо комплексного реагування на різні загрози [224, с. 337].

Аналізуючи державну політику в сфері захисту критичної інфраструктури в умовах правового режиму воєнного стану, сліз зазначити, що задля посилення захисту критичної інфраструктури, військове командування у тандемі з військовими адміністраціями може змінювати охорону об’єктів життєзабезпечення населення та критичної інфраструктури, а також запроваджувати особливий режим їх роботи, вводити трудову

повинність для осіб не задіяних в оборонній сфері (з метою виконання робіт оборонного характеру для захисту критичної інфраструктури), ініціювати заборону діяльності громадських об'єднань, політичних партій та інших об'єднань якщо вона може порушити стійкість критичної інфраструктури [71].

У таких умовах порядок особливого режиму та роботи об'єктів критичної інфраструктури затверджуються Кабінетом Міністрів України. Однак, відзначимо, що у теорії державного управління не існує універсального інституційного шаблону, що визначало б стандартний алгоритм захисту критичної інфраструктури. Саме тому, завданням Уряду є формування власних автентичних протоколів, опираючись на аналіз поточної ситуації в країні крізь призму базових показників:

- основи конституційного ладу країни;
- каталог прогнозних і поточних критичних ризиків і загроз;
- кон'юнктура та структура економіки;
- етнічна культура нації та суспільно-політичний стан в країні;
- загальний інституційний досвід у державному управлінні.

Прислухаємось до наукового підходу вчених Д. С. Бірюкова та С. І. Кондратова [10, с. 76] стосовно архітектури державної політики захисту критичної інфраструктури, де вчені пропонують розвивати вектор державної політики у сфері захисту критичної інфраструктури у світлі дуальної моделі:

1. Модель, що базується на принципах стимулювання, саморегулювання та добровільності дотримання стандартів. Дана модель опирається на політику ліберального управління, та посилює участь стейкхолдерів інфраструктурних об'єктів, яким надається можливість докласти зусиль до процесу захисту критичної інфраструктури. Такі зусилля можуть бути як у дорадчій так і фізичній формі.

2. Модель, що базується на принципах обов'язковості та відповідальності. Головний зміст передбачає обов'язковість виконання правових норм в рамках державної політики у сфері захисту критичної інфраструктури та супроводжується санкціями відносно операторів об'єктів критичної інфраструктури за порушення вимог безпеки.

Варто акцентувати увагу на поширеній у іноземних країн практиці інституційної інтеграції у державну політику комбінацій окремих елементів обох зазначених моделей. Такі перспективи у розбудові парадигми державної політики захисту критичної інфраструктури в Україні на основі світового досвіду вивчав учений Д. Г. Бобро [12, с. 7]. Нам імпонує перелік ключових кроків, які виокремив учений у цьому напрямі:

1. Конструювання автентичної інституційно-правової бази та її регулярне удосконалення.

2. Ідентифікація координуючого органу, як, наприклад, у США – Департамент внутрішньої безпеки (Department of Homeland Security), до складу якого включено 22 федеральних агентства із загальною чисельністю персоналу близько 170 тис. осіб.

3. Напрацювання методичних вказівок до формування реєстру об’єктів критичної інфраструктури, а також оцінки ризиків та загроз.

4. Створення планів оперативного реагування та систематична переоцінка їх дієвості. Наприклад, у США цим займається National infrastructure simulation and analysis center (Національний центр аналізу та імітаційного моделювання інфраструктури) [150].

5. Організація підготовки кадрового потенціалу в сфері захисту критичної інфраструктури.

6. Налагодження оперативної співпраці, інформаційного обміну та вивчення кращих практик.

7. Розвиток державно-приватного партнерства [14].

Реалізація в Україні парадигми державної політики у сфері захисту критичної інфраструктури в умовах правового режиму воєнного стану неможлива без розподілу специфічних функцій управління між спеціальними державними органами.

Це частково викликано тим, що сьогодні Україна зіткнулася із гострою потребою оперативної адаптації векторів державної політики до умов протидії численним гібридним загрозам з боку країни агресора, котрі вона свідомо спрямовує на руйнацію суверенітету та територіальної цілісності держави. Аналізуючи досягнуті Україною успіхи у сучасній парадигмі державної політики у сфері захисту критичної інфраструктури, що формувалась в умовах воєнного стану, відзначимо створення власної архітектури комплексного аналітичного процесу забезпечення захисту об’єктів критичної інфраструктури, що включає:

– алгоритм ідентифікації секторів критичної інфраструктури;

– визначення спектру актуальних ризиків та загроз для об’єктів критичної інфраструктури;

– формування Реєстру об’єктів критичної інфраструктури;

– ідентифікацію суб’єктного складу із провадження державної політики у сфері захисту критичної інфраструктури;

– суттєву модернізацію інституційно-правового забезпечення державної політики у сфері захисту об’єктів критичної інфраструктури;

– розробку алгоритмів та протоколів вжиття відповідних заходів із усунення наслідків руйнувань об’єктів критичної інфраструктури

– формування системи захисту критичної інфраструктури.

Не зважаючи на позитивні зрушення, слушним вважаємо зауваження Г. Ю. Зубка [85, с. 170], який наголошує на певній інституційній недосконалості державної політики у розрізі забезпечення захисту об’єктів критичної інфраструктури саме в умовах воєнного стану в Україні. Учений акцентує увагу на її стратегічній розпорошеності та рандомності та локальній фрагментарності. Розділяємо позицію науковця, що дані проблеми виступають певним інституційним бар’єром до модернізації стратегії національної безпеки. Опираючись на даний аргумент, актуалізуємо квестію щодо розробки моделі ефективної взаємодії і міжсекторальної координації

суб'єктів державної політики в сфері захисту критичної інфраструктури. Дану позицію можна підсилити на прикладі успішного досвіду світових країн, де структурна дифузія систем реагування на загрози, ризики та небезпеки у сфері захисту критичної інфраструктури є пріоритетним елементом державної політики. Наприклад, нормативно-правова база США характеризує здатність таких систем взаємодіяти між собою терміном «функціональна сумісність» [164]. Даний предикат передбачає оптимальну здатність обладнання та персоналу окремих структур оперативно реагувати, отримувати та надавати послуги та організаційну підтримку при реагуванні на надзвичайні ситуації у сфері захисту об'єктів критичної інфраструктури, пріоритетно рівню їх критичності.

Категоризація критичності об'єкта критичної інфраструктури, є окремими важливим елементом державної політики, та визначається на основі аналізу рівня негативного впливу внаслідок порушення або припинення функціонування об'єкта інфраструктури [124].

Визначення рівня негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури (секторальні критерії) відбувається відповідно до рівня негативного впливу: катастрофічні наслідки (4 бали), критичні наслідки (3 бали), значні наслідки (2 бали), незначні наслідки (1 бал), надто малий (0 балів). Більшість показників ґрунтуються на однобічній кількісній характеристиці, що аналізує вплив порушення роботи критичного об'єкта на жителів відповідної території. Отже, це дає підстави стверджувати що дана методика розроблена відповідно до концепції людиноцентризму як антропологічної парадигми сучасної євроінтеграційної політики України. Відповідно до ідеології людиноцентризму або «людиноорієнтованої» ідеології, держава має «служити» інтересам громадян, тобто діяти заради і в ім'я приватних осіб шляхом всебічного забезпечення пріоритету їх прав, свобод та інтересів у публічній сфері [116, с. 161].

Аналіз реалізації адміністративно-правової доктрини людиноцентризму, проведений О. В. Гладкою свідчить, що людина володіє специфічним «соціальним тілом», яке базується на економічних, антропологічних, духовно-етичних, аксіологічних засадах, що свідчить про специфічну культуру людини і суспільства [26, с. 61]. Це підтверджується аналізом визначення рівня негативного впливу у разі знищення, пошкодження або порушення функціонування об'єкта критичної інфраструктури (міжсекторальні критерії), що диференційовані на категорії за Соціальною, суспільною Економічною, комунікативною та безпековою значущістю:

I. Соціальна значущість об'єкта критичної інфраструктури (заподіяння шкоди навколишньому природному середовищу, заподіяння шкоди життю та здоров'ю людей);

II. Суспільна значущість об'єкта критичної інфраструктури (припинення або порушення функціонування державних органів, негативний вплив на довіру людей до державних інституцій, шкода інтересам інших держав –

партнерів України);

III. Економічна значущість об'єкта критичної інфраструктури (заподіяння збитків об'єкту інфраструктури, заподіяння збитків державному та місцевим бюджетам);

IV. Комунікативна (негативний вплив на безперервне та стійке функціонування іншого об'єкта інфраструктури, що забезпечує надання таких самих або інших послуг);

V. Безпекова значущість об'єкта критичної інфраструктури (припинення або порушення функціонування пунктів управління або ситуаційного центру, що оцінюється в їх значущості, зниження показників державного оборонного замовлення).

В межах сучасної парадигми державної політики в сфері захисту критичної інфраструктури в умовах правового режиму воєнного стану важливим кроком стало упорядкування процесу формування переліку суб'єктів, відповідальних за формування й реалізацію державної політики та секторів критичної інфраструктури у відповідних секторах національної системи захисту критичної інфраструктури. Даний процес координує Кабінет Міністрів України, переглядаючи та змінюючи його виходячи визначених з критеріїв критичності. Ст. 4. Закону України «Про критичну інфраструктуру» [60] до життєво важливих послуг та функцій, порушення яких сприятиме виникненню негативних наслідків для національної безпеки України, визначає 17 позицій: урядування та надання найважливіших публічних послуг, охорона здоров'я, енергозабезпечення, , продовольче забезпечення, фармацевтична промисловість, водопостачання та водовідведення, виготовлення вакцин, інформаційні послуги, стале функціонування біолабораторій, транспортне забезпечення, електронні комунікації, фінансові послуги, оборона, правопорядок, державна безпека, здійснення правосуддя, цивільний захист населення та територій, тримання під вартою, служби порятунку, космічні технології та послуги, космічна і дослідницька діяльність, хімічна промисловість. Відповідно до зазначеного переліку, Постановою № 1109 визначено перелік секторів (підсекторів), основних послуг критичної інфраструктури, заключним у цей список було внесено агропромисловий комплекс у якості детермінанти продовольчого забезпечення держави. Таким чином станом на 1 листопада 2023 р. в Україні налічується 25 секторів критичної інфраструктури (Додаток Б) [78].

Важливим кроком у межах модернізації державної політики захисту критичної інфраструктури в умовах правового режиму воєнного стану стала спроба формування у системі Міністерства оборони України кібервійськ, що передбачено Указом Президента України №446 від 26.08.2021 р. «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави» [268]. Магістральною ціллю даної ініціативи стала необхідність захисту суверенітету держави, відсічі збройній агресії у кіберпросторі, забезпечення її обороноздатності та запобігання збройному конфлікту. Логічним завершенням процесу створення

кібервійськ має стати розробка законопроєкту «Про створення та функціонування у системі Міністерства оборони України кібервійськ». Однак станом на листопад 2023 року це питання ще залишається відкритим.

Звернемо увагу, що парадигми державної політики у сфері захисту критичної інфраструктури розвинених країн об'єднує актуалізація предикату стійкості критичної інфраструктури. Стійкість об'єкта критичної інфраструктури дослідники тлумачать як здатність ним виконувати задані функції не лише у нормальних умовах, але й запобігати виникненню на об'єкті аварій чи катастроф за настання надзвичайного стану [1, с. 234]. Тобто питання забезпечення стійкості критичної інфраструктури, є особливо актуальною в умовах воєнного стану, оскільки посилюється інтенсивність впливу надзвичайних ситуацій, що піддають критичну інфраструктуру ризику дестабілізації. С. І. Кондратов, О. М. Суходоля підтверджують дане припущення, наголошуючи, що проблемам забезпечення стійкості приділяється усе більше уваги відносно захисту. Таку діаметральність учені пояснюють тим, що в умовах війни, жодна відома система захисту не гарантує повноцінний захист від усього спектру загроз і небезпек [95, с. 20]. Відповідно стійкість критичної інфраструктури передбачає її здатність до готовності та акомодації відносно динамічних умов, а також здатність протистояти змінам і швидко регенерувати потужності після надзвичайних ситуацій. Отже, можна дійти висновку, що концепція стійкості є більш практичною та дієвішою. У даному напрямку Державна служба спеціального зв'язку та захисту інформації України вивчає директиви ЄС NIS 2 (EU 2022/2555) та RCE (EU 2022/2557) щодо стійкості критичної інфраструктури і співпрацює з країнами, які вже розпочали їх впровадження.

У законодавчо визначеному переліку С. І. Крук пропонує конкретизовані інформаційні, інформаційно-інструментальні загрози та загрози психологічні дії з території інших країн, спрямовані на порушення нормального функціонування систем державного і воєнного управління. Вітчизняне законодавство про безпеку має чітко розмежовувати повноваження державних органів, насамперед, органів сектору безпеки, забезпечувати міжвідомчу координацію, зокрема за умов тривалої агресії проти України [101, с. 77].

Фундаментальне значення в ідентифікації позиції та ролі парадигми державної політики в сфері захисту критичної інфраструктури в умовах правового режиму воєнного стану, закріплено Конституцією України, положення якої проектуються у Законі України від 21.06.2018 № 2469-VIII «Про національну безпеку України» [62]. Його зміст спрямований на посилення ролі органів державної влади у механізмі розвитку оборонно-промислового комплексу України, складовими якого є «державно-приватне партнерство» та «міжнародна консультативна, фінансова та матеріально-технічна допомога» [62]. Роль державної влади у сфері захисту критичної інфраструктури в умовах правового режиму воєнного стану актуалізує також п.2 ч.1 ст.1 Закону України «Про критичну інфраструктуру» [60] у якій

ідентифіковано послуги та функції, здійснення яких гарантується органами місцевого самоврядування та державної влади, суб'єктами господарювання, установами та організаціями будь-якої форми власності, переривання, збої або порушення надання яких спричиняє швидкі негативні наслідки для національної безпеки як атрибутив «життєво важливі функції та послуги». Тобто дані положення Закону спрямовані на створення національної системи забезпечення безпеки та стійкості функціонування критичної інфраструктури та здійснення життєво важливих функцій [60].

Зазначений аспект парадигми державної політики у сфері захисту критичної інфраструктури в умовах правового режиму воєнного стану урегульовується низкою механізмів та інструментів, описаними у попередніх розділах зокрема веденням Реєстру об'єктів критичної інфраструктури, паспортизацією об'єктів, розробкою планів захисту та планів взаємодії та ін. Такі заходи переважно орієнтовані на забезпечення безпеки конкретних об'єктів, що є складовою глобального завдання у векторі забезпечення стійкості критичної інфраструктури в умовах воєнного стану. Тобто в умовах воєнного стану активується потреба у досягненні стійкості шляхом забезпечення спроможності окремих операторів критичної інфраструктури. Секторальні органи влади розробляють та затверджують плани підтримання життєво важливих функцій та взаємодії у випадку дизфункції об'єктів критичної інфраструктури (п.4 ст.19), місцеві органи виконавчої влади забезпечують розроблення та затвердження програм підвищення стійкості територіальних громад, місцевих планів взаємодії у кризовій ситуації залучених суб'єктів, планів відновлення функціонування критичної інфраструктури (ст.20). Такі плани є своєрідною угодою між стейкхолдерами, котрі залучаються до процесу захисту критичної інфраструктури [60].

Аналізуючи в умовах воєнного стану особливості сучасної державної політики у сфері захисту критичної інфраструктури, корисним вважаємо дослідження Г. Ю. Зубка [80, с. 172], який, вивчав наукові аспекти реалізації державної інфраструктурної політики. Опираючись на доктринальні погляди вченого, відзначимо декілька основоположних припущень:

По-перше, в умовах правового режиму воєнного стану державна політики у сфері захисту критичної інфраструктури існує в концептуальному та діяльнісному аспектах і здійснюється Президентом, Урядом, інститутами, відповідальними за реалізацію політики захисту критичної інфраструктури.

По-друге, як процесу в умовах правового режиму воєнного стану державній політиці у сфері захисту критичної інфраструктури, притаманна етапність: від плану, курсу дій до практичної реалізації безпекових заходів.

По-третє, в умовах правового режиму воєнного стану державна політики у сфері захисту критичної інфраструктури концентрує в собі суспільно значущі інтереси і потреби.

По-четверте, в умовах правового режиму воєнного стану державна політики у сфері захисту критичної інфраструктури є багато суб'єктною.

Сформованість законодавчої бази в Україні передбачає механізми управління державою як у звичайних умовах, так і в умовах надзвичайного та воєнного стану. Це значною мірою гарантує безперервність урядування, що є одним із ключових напрямів забезпечення національної безпеки і стійкості. Крім того, ухвалений 2021 р. Закон України «Про основи національного спротиву» [66] заклав підвалини організації територіальної оборони, яка відіграла важливу роль у забезпеченні захисту держави у нинішній війні. Зокрема, у такий спосіб було реалізовано принцип субсидіарності, який є одним із ключових у сфері формування національної стійкості. Це дозволило суттєво підвищити ефективність реагування на воєнні загрози на місцевому рівні й налагодити належне координування на всіх рівнях [224].

Зокрема в роботах, присвячених аналізу різноманітних аспектів захисту критичної інфраструктури йдеться передусім про внутрішній аспект. На наш погляд, така позиція вельми дискусійна, оскільки Україна обрала курс на європейську та євроатлантичну інтеграцію, що передбачає розвиток в умовах глобалізації світової спільноти. Відповідно до цього, вектор державної політики захисту критичної інфраструктури має розвиватися й реалізовуватися в міжнародному і транснаціональному безпекових контекстах [86]. Тобто Уряд має встигнути вбудуватися в нову архітектуру світу, зберігаючи власні національні інтереси, контроль над власним інфраструктурним комплексом та національною ідентичністю, в тому числі й монополію та розвиток та провадження штучного інтелекту, водночас враховуючи глобалізаційні загрози, в тому числі і щодо ролі та впливу інфраструктури на формування парадигми національної безпеки. Погодимось із думкою В. А. Ліпкана, який стверджує, що «сучасна парадигма безпеки в Україні є наслідком деструктивних результатів агресії рф та аксіом її геополітики таких як агресія, анексія, тероризм, сепаратизм» [113, с. 271], що варто вважати основоположним системоутворюючими елементами адаптації державної політики захисту критичної інфраструктури. Слушною вважаємо пропозицію Г. Ю. Зубка, який пропонує політику України у цій сфері адаптувати за такими напрямами: зменшення інвестиційно-інноваційних ризиків; поліпшення економічних, правових та організаційних умов діяльності іноземних інвесторів; активізацію механізмів концесії, угод про розподіл продукції, лізингу; використання потенціалу інститутів спільного інвестування [81, с. 220]. Аналіз алгоритмів відпрацьованих дій суб’єктами реагування на кризові ситуації внаслідок руйнування енергетичної інфраструктури України, можемо узагальнити методичний підхід до розробки концепції забезпечення стійкості системи критичної інфраструктури (рис. 2.1).

Враховуючи напрацювання у цьому напрямку О. М. Суходолі [255] та у відповідності до визначених Законом України «Про критичну інфраструктуру» [60] режимів функціонування критичної інфраструктури можемо узагальнити базові заходи реагування в межах квадрокомлексу режимів на об’єктовому рівні:

1. Штатний режим – передбачає розробку превентивного плану захисту, зокрема, розробку паспорта безпеки, відпрацюванні заходів зі попередження загроз, планування заходів зі зниження ризиків, планування заходів із мінімізації потенційної шкоди; застосування заходів з підвищення технічної стійкості, навчання персоналу.

2. Режим готовності та запобігання – передбачає розробку планів оперативної готовності. Основним документом є Акт оцінки стану захищеності об'єкта критичної інфраструктури, на основі якого здійснюється розробка планів захисту об'єкта та протидії проектним загрозам, оцінка стану аварійної готовності, тренування персоналу.

3. Режим реагування – заходи реагування на подію з метою повернення до первинних параметрів функціонування. Розробляються плани реагування, аварійної ситуації, взаємодії на випадок диверсії, протидії кіберзагрозам, безперервності ведення виконання функцій.

4. Режим відновлення – повернення до штатного режиму функціонування та урахування помилок попередніх режимів. Передбачає розробку планів відновлення, диверсифікації, резервування, посилення майбутньої стійкості, нових технологічних можливостей.

Рис. 2.1 Концепція забезпечення стійкості системи критичної інфраструктури

Джерело: розроблено автором на основі [113],[255]

Слушною вважаємо також пропозицію О. М. Суходолі [255, с. 3], який розподіляє заходи державної політики у сфері забезпечення стійкості системи критичної інфраструктури під час реагування на загрози порушення функціонування критичної інфраструктури на заходи «аварійного реагування» (першочергові дії реагування по припиненню деструктивного впливу загроз) та заходи «пом'якшення впливу загроз» на функціональність критичних об'єктів та рівень їх функціональності.

Важливим тригером у формуванні ефективної парадигми державної політики у сфері захисту критичної інфраструктури в умовах правового режиму воєнного стану стало ухвалення Урядом 19 вересня 2023 року розробленого Адміністрацією Держспецзв'язку «Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури» [228]. Інституція визначає стратегічні цілі, завдання та заходи для суб'єктів національної системи захисту критичної інфраструктури, серед яких: уточнення завдань та повноважень суб'єктів захисту критичної інфраструктури, удосконалення законодавства, що регламентує їхню діяльність; забезпечення проведення моніторингу; проведення оцінки ризиків і загроз критичній інфраструктурі; визначення порядку взаємодії суб'єктів захисту у кризових ситуаціях; забезпечення функціонування системи обміну інформацією; посилення стійкості; розроблення програм щодо роботи з громадами та підтримки населення на випадок кризових ситуацій; налагодження міжнародної співпраці.

Отже, адекватна модель загроз об'єкта критичної інфраструктури (рис.2.2) має включати портрет потенційного порушника, модель об'єкта та модель обстановки. Зважаючи на зазначене, модель загроз можна представити відповідно до підходу «all hazards approach» враховуючи загрози диверсифікованого походження: природного, техногенного, соціально-політичного, військового, кібернетичного, диверсійного, економічного, терористичного та колаборантного. Завдячуючи процесу моделювання формується модель загроз, що включає перелік можливих небезпек для критичного об'єкта, що впливають на його стале функціонування [95, с. 20]. Варто акцентувати увагу, що 15 березня 2022 року Кримінальний кодекс України було доповнено статтею 111-1 «Колабораційна діяльність» [99], де розтлумачено інтенцію «колабораціонізм», відповідно, колабораційну загрозу можемо трактувати, як небезпеки, що походять від громадян держави, які співпрацюють із ворогом з метою забезпечення реалізації його інтересів та заподіяння шкоди.

Теорії взаємовідносин між вищими органами державної влади в умовах надзвичайних ситуацій, де чітко розмежовується характер загрози. Якщо ця загроза зовнішня – за її подолання чи попередження відповідає глава держави, якщо внутрішня – уряд. Тому конституційні приписи мають бути розкриті в нормах спеціальних законів, де повинна бути чітко відображена послідовність дій всіх органів влади та посадових осіб.

Якщо в умовах воєнного стану Президент стає ключовою фігурою в

прийнятті рішень, то в умовах надзвичайного стану чи надзвичайної екологічної ситуації повсякденне керівництво управлінням ресурсами та подоланням таких подій бере на себе уряд, а Президент здійснює тільки функцію запуску заходів, передбачених у таких випадках, а саме, оголошення відповідного стану. Для уникнення протистоянь між Президентом та Прем'єром служить єдина площадка для прийняття рішень – Рада національної безпеки та оборони.

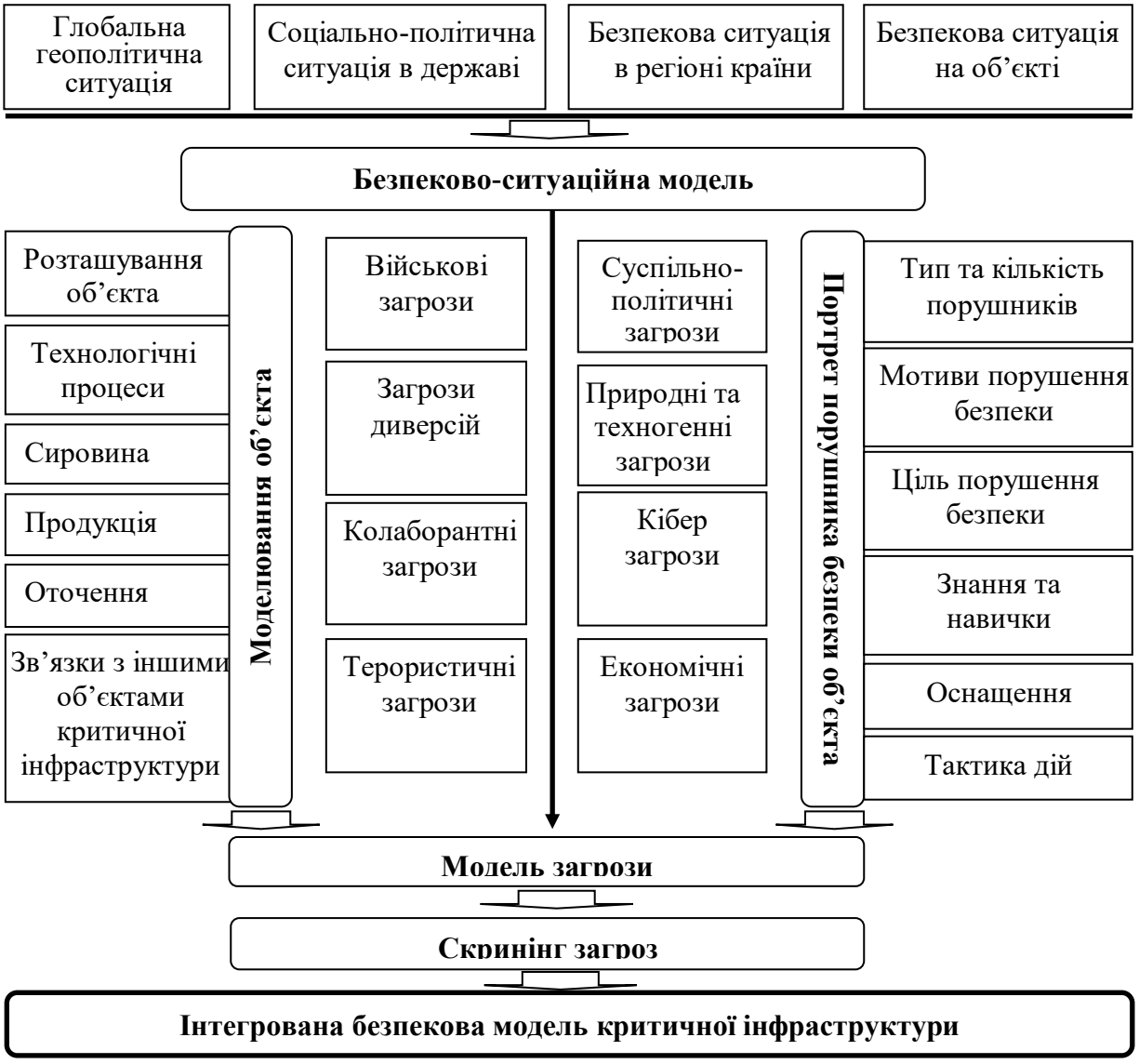


Рис. 2.2. Формат інтегрованої безпекової моделі критичної інфраструктури

Джерело:узагальнено на основі [14], [95], [99]

Структурно-логічна схема функціонування суб'єктів державної системи безпеки та стійкості критичної інфраструктури (Додаток В) ілюструє процес організації системи управління та координації, а також відображає суб'єктів та основні завдання якими вони опікуються. Формалізаційним інструментом у функціонуванні державної системи безпеки та стійкості критичної інфраструктури виступає Національний план захисту критичної

інфраструктури, який зафіксує завдання, послідовність дій та механізм координації всіх залучених суб'єктів у різних режимах її функціонування.

Органи державної влади та місцевого самоврядування в умовах надзвичайного і воєнного стану продовжують виконувати свої конституційні повноваження, опираючись на законодавство України. Зокрема, регламентовано механізми координації та міжвідомчої взаємодії на територіальних рівнях під час запровадження зазначених правових режимів. Реалізація заходів із впровадження дії надзвичайного стану покладається на органи виконавчої влади, органи місцевого самоврядування та відповідні військові командування. Також вони у співпраці з військовим командуванням організовують контроль за додержанням конституційних прав і свобод громадян, забезпеченням громадського порядку, громадської безпеки, захисту інтересів держави. Координація діяльності органів виконавчої влади та місцевого самоврядування, воєнного командування, підприємств, установ і організацій в умовах надзвичайного стану в частині, що не належить до повноважень РНБО України, покладається на КМУ. Для координації дії з питань підтримання правопорядку і забезпечення безпеки громадян на відповідній території на місцях можуть створюватися оперативні штаби, до складу яких можуть включатися представники СБУ, Національної поліції, Військової служби правопорядку у ЗСУ, центральних органів виконавчої влади, що реалізують державну політику у сфері цивільного захисту, місцевого самоврядування на чолі з комендантами територій та місцевих органів виконавчої влади.

Важливим кроком у розвитку державної політики стало рішення Президента України, який 17.10. 2023 р. своїм Указом ввів у дію рішення РНБО «Про організацію захисту та забезпечення безпеки функціонування об'єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій» [271], яке орієнтовано на посилення захисту об'єктів критичної інфраструктури в умовах воєнного стану. Основні положення даного рішення передбачають посилення інженерного та фізичного протидронового захисту об'єктів критичної інфраструктури;. у разі виникнення надзвичайних ситуацій підвищити якість захисту та евакуації працівників об'єктів критичної інфраструктури; створення резерву обладнання та запасних частин для оперативного відновлення пошкоджених об'єктів; створення страхового фонду документації та критичних баз даних на захищених ресурсах; забезпечення об'єктів критичної інфраструктури резервними джерелами електроживлення; відпрацювання систем оповіщення населення про виникнення надзвичайної ситуації; затвердження Плану заходів з відновлення об'єктів критичної інфраструктури, що були зруйновані та/або пошкоджені внаслідок збройної агресії рф проти України; розробку та затвердження Плану енергетичної стійкості України; доповнення секторальних переліків об'єктів критичної інфраструктури, розташованими на тимчасово окупованій території України, та включити їх до Реєстру; утворення структурних підрозділів з питань захисту критичної

інфраструктури; розробку та затвердження за категоріями об’єктів критичної інфраструктури; забезпечити запровадження системи взаємодії та інформаційного обміну між суб’єктами національної системи захисту критичної інфраструктури; вжити заходів із посилення бойової спроможності мобільних вогневих груп які здійснюють оборону об’єктів критичної інфраструктури; підготовку методичних рекомендацій для органів місцевого самоврядування та місцевих органів виконавчої влади стосовно розробки та затвердження місцевих програм забезпечення стійкості та безпеки критичної інфраструктури; унеможливлення поширення інформації про об’єкти критичної інфраструктури; запровадження Міністерством оборони України навчальних програм та курсів підвищення кваліфікації з радіоелектронної боротьби та розвідки для військовослужбовців, залучених до забезпечення захисту і оборони об’єктів критичної інфраструктури [271].

Отже, варто відзначити, що сучасний етап реформування сектору безпеки і оборони України можна охарактеризувати як період активного формування мультиплікованої державної системи захисту критичної інфраструктури. Цьому сприяє наявність повноцінних систем захисту та кризового реагування. Практичної реалізації даного вектору державної політики можна досягнути за рахунок переходу до більш чіткого рівня координації дій та симбіозу, що передбачає узгодження основних параметрів функціонування зазначених систем реагування. До даної системи обов’язково має входити вектор превентивного та антикризового управління ризиками та загрозами за участю стейкхолдерів об’єктів критичної інфраструктури із розробкою спеціальних галузевих планів що застосовуватимуться у сфері їх захисту та не обмежуватиметься лише національним рівнем. Даний модуль сприятиме забезпеченню стійкості критичної інфраструктури та протидії стратегічним загрозам і ризикам на національному й міжнародному рівнях.

2.4. Сучасні концепції менеджменту в забезпеченні стійкості об’єктів критичної інфраструктури

У контексті національної безпеки визначальним є формування державної політики, орієнтованої на зміцнення та підтримку безпечної, функціонально ефективної і стійкої критичної інфраструктури в тих секторах, що мають ключове значення для безпеки держави, охорони здоров’я населення, економічної стабільності та якості життя в цілому. Стійкість у цьому аспекті розуміється як здатність передбачати змінні умови, адаптуватися до них, витримувати збої та оперативно відновлюватися після їх виникнення, включаючи навмисні атаки, техногенні інциденти або природні загрози [4]. Зміщення акценту з виключного захисту критичної інфраструктури на забезпечення її стійкості відображає потребу реагування на зміну ризикового ландшафту, що позначається дедалі більшою

невизначеністю.

Враховуючи зростаючу складність, взаємозалежність і взаємозв'язаність критичної інфраструктури, системний підхід до забезпечення її стійкості дає змогу сформувати нові перспективи у цій сфері [5]. Підвищення рівня стійкості критичної інфраструктури як на національному, так і на європейському рівні визначене одним із головних пріоритетів безпекової політики Європейського Союзу, що підтверджується рішеннями Ради ЄС щодо посилення відповідних заходів [36]. У цьому контексті забезпечення безпеки та стійкості критичних об'єктів в Україні, особливо в умовах збройної агресії з боку російської федерації, набуває виняткової актуальності.

Згідно з Концепцією безпеки та стійкості критичної інфраструктури, поняття «безпека» і «стійкість» розглядаються як взаємодоповнюючі складові загального підходу до захисту. Безпека трактується як зменшення ймовірності реалізації успішних атак або зниження впливу природних та техногенних загроз шляхом застосування фізичних засобів захисту та заходів кібербезпеки. Стійкість, своєю чергою, інтерпретується як спроможність інфраструктури протидіяти викликам, поглинати вплив негативних чинників, оперативно відновлюватися та адаптуватися до нових обставин. Відмовостійка інфраструктура характеризується надійністю, гнучкістю, адаптивністю та здатністю до швидкого функціонального відновлення після різних типів загроз – як навмисного, так і стихійного походження.

На тлі зростання природних і техногенних загроз, а також вразливостей, що виявляються у сучасному суспільстві, стає очевидною обмеженість традиційних моделей оцінювання ризиків і заходів щодо їх мінімізації. Відтак, концепція безпеки та стійкості критичної інфраструктури відіграє особливо важливу роль у розробці політик, спрямованих на пом'якшення наслідків надзвичайних подій, і акцентує необхідність для держав у впровадженні комплексних стратегій управління ризиками [7]. Основні складові цієї концепції – готовність до змін, здатність до адаптації, опірність і швидке відновлення – можуть бути репрезентовані через чотири структурні компоненти: готовність, заходи з пом'якшення наслідків, реагування та заходи з відновлення [8]. Сукупність цих елементів дозволяє спеціалістам перевести загальну ідею стійкості у практичну площину менеджменту підприємств критичної інфраструктури, забезпечивши можливість оцінювання динаміки покращення її рівня з часом. У таблиці 2.3 наведемо опис зазначених компонентів та відповідні приклади для практичного аналізу [260].

З даних, наведених у таблиці, випливає, що стійкість об'єктів критичної інфраструктури є інтегральним показником, що охоплює практично всі аспекти їх функціонування, що, у свою чергу, ускладнює можливість його прямої кількісної оцінки. Cantelmi R. та ін.. [288] акцентують увагу на складності та багатовимірності поняття стійкості критичної інфраструктури. У своїх дослідженнях він пропонує багаторівневий підхід, заснований на ризик-орієнтованій оцінці, яка враховує взаємозалежність інфраструктурних

систем. При цьому аналізуються можливі рішення, які можуть бути реалізовані на різних етапах життєвого циклу інфраструктур – від проєктування до будівництва та експлуатації.

Таблиця 2.3 – Складові стійкості об’єктів критичної інфраструктури

Складова	Характеристика	Приклад
Підготовленість	Діяльність, спрямована на передбачення відповідних загроз і можливих наслідків від їх виникнення, включно із превентивними заходами.	Утримання сил безпеки. Установлення / моніторинг фізичного контролю доступу. Розробка планів на випадок надзвичайних ситуацій і планів кібербезпеки. Проведення регулярних навчань для перевірки планів. Створення механізмів обміну інформацією
Пом’якшення наслідків	Діяльність, спрямована на протистояння та / або поглинання негативних наслідків події, зменшення тяжкості або наслідків загрози; свідчить про надійність інфраструктури.	Модернізація підприємств для пом’якшення наслідків різних природних загроз. Модернізація обладнання, яке буде протистояти передбачуваним небезпекам. Підвищення надійності систем підтримки інфраструктури. Створення альтернативного резервного майданчика, який може продовжити роботу після інциденту й сприяти відновленню. Розуміння міжгалузевих залежностей від ключових зовнішніх ресурсів. Завбачлива підготовка додаткових запасів.
Реагування	Заходи та програми, що здійснюються або розробляються для реагування та адаптації до негативних наслідків події; свідчить про винахідливість власників та операторів інфраструктури в управлінні кризовими ситуаціями	Підтримання можливостей реагування на місці на ключові небезпеки. Побудова відносин з місцевими службами швидкого реагування та міжсекторальними партнерами; Наявність можливостей для управління позаштатними ситуаціями на місці, включно з навченим персоналом, функціональним оперативним центром і розумінням міжгалузевих проблем.
Відновлення	Діяльність і програми, спрямовані на те, щоб допомогти організаціям повернути умови роботи до прийнятного рівня та відновитися після події; свідчить про здатність швидко відновити надання послуг.	Укладання угод про першочергове відновлення з ключовими постачальниками послуг. Оцінка часу й заходів, необхідних для відновлення повноцінної роботи організації після збою. Стратегії швидкої заміни/ремонту критично важливих компонентів. Підтримка запасів на випадок надзвичайних ситуацій.

Джерело [260]

Таким чином, реалізація функцій менеджменту у сфері забезпечення стійкості функціонування критичної інфраструктури з метою безперебійності надання життєво важливих функцій суспільству досягається шляхом реалізації узгодженого комплексу заходів, що охоплюють усі етапи циклу антикризового реагування:

1. Запобігання та уникнення загроз. На цьому етапі здійснюється управління формуванням інституційних і технічних спроможностей для виявлення, попередження та нейтралізації загроз. Впроваджуються профілактичні заходи, спрямовані на зменшення вразливостей, підвищення обізнаності серед усіх зацікавлених сторін щодо спектру потенційних загроз, а також розвиток оперативного потенціалу відповідальних суб'єктів.

2. Захист від впливу загроз. Метою цього етапу є управління у напрямку забезпечення цілісності критичної інфраструктури, збереження людських ресурсів і забезпечення безперебійного функціонування ключових послуг навіть в умовах надзвичайних ситуацій. Реалізується в межах загального підходу до ризиків будь-якого характеру (all-hazards approach) і має бути орієнтованим на підтримання національних інтересів, стабільності життєвих практик громадян, а також ефективності функціональних режимів об'єктів критичної інфраструктури [362].

3. Пом'якшення впливу загроз та мінімізація втрат. Даний етап передбачає реалізацію управлінських заходів, які дозволять знизити інтенсивність наслідків реалізації ризиків. Основний акцент робиться на зменшенні шкоди, тривалості негативного впливу, а також зниженні людських і матеріальних втрат. Залучення до процесу різних секторів суспільства – від індивідуальних громадян до організацій громадянського суспільства та суб'єктів критичної інфраструктури – є вкрай важливим. Ефективність заходів з пом'якшення тісно пов'язана з рівнем усвідомлення ризиків і здатністю до міжсекторального обміну інформацією та планування.

4. Реагування на загрози. Оперативне й скоординоване реагування дозволяє суттєво зменшити наслідки кризових ситуацій. Заходи включають управління рятувальними операціями, надання первинної допомоги, стабілізацію ситуації, забезпечення базових потреб населення та відновлення функціонування інфраструктурних об'єктів. Залучення громадян є ключовим ресурсом у перші години після інциденту, оскільки вони часто виступають джерелом додаткової робочої сили та підтримки для органів реагування.

5. Відновлення інфраструктури, функцій та життєдіяльності. Останній етап циклу охоплює заходи з відновлення фізичної, економічної, соціальної та організаційної інфраструктури. Йдеться про впровадження управлінських стратегій, що дозволяють поєднувати реконструкцію з підвищенням стійкості до майбутніх загроз. Особлива увага приділяється інклюзивному підходу до планування з урахуванням досвіду попередніх криз (принцип «відновлення з поліпшенням»), застосуванню найкращих практик і технологій, а також недопущенню повторення аналогічних подій. Здійснення якісної оцінки рівня стійкості критичних інфраструктур на основі запропонованого підходу

дійсно сприяє деталізації концепції стійкості у вигляді конкретних практичних дій. Проте, відсутність кількісного виміру цього показника обмежує можливість проведення порівняльного аналізу між різними об'єктами, зокрема в умовах їхньої належності до різних секторів критичної інфраструктури [357].

Сучасні концепції менеджменту в забезпеченні реалізації вище приведених заходів із забезпечення стійкості підприємств критичної інфраструктури можемо розподілити за наступними напрямками:

1 Управління ризиками (ризик-менеджмент). Ця концепція є фундаментальним підходом до підвищення безпеки систем критичної інфраструктури проти руйнівних подій. Вона включає систематичний процес виявлення, оцінки та управління бізнес-ризиками, забезпечуючи, щоб основні загрози не були пропущені. Цей процес, як правило, включає ідентифікацію критичних ризиків, розуміння потенційних загроз (подій або суб'єктів, що використовують вразливості), оцінку вразливостей, аналіз ймовірності та наслідків від перетворення ризиків у реальні надзвичайні ситуації, а також оцінку їх значущості. Сучасні підходи наголошують на проактивній, ризик-орієнтованій та багатоетапній стратегії захисту. Це передбачає зосередження ресурсів на найбільш слабких місцях та вжиття практичних кроків для мінімізації або усунення суттєвих ризиків, які можуть мати значний вплив на об'єкти критичної інфраструктури. Стратегії пом'якшення ризиків, як правило, поділяються на такі категорії, як уникнення ризиків (повне уникнення факторів, що створюють високі ризики), передача ризиків (передача відповідальності третій стороні, наприклад, через страхування) та зменшення ризиків (зменшення потенційного впливу ризику) [306].

2. Менеджмент операційної стійкості (операційний менеджмент). Операційний менеджмент полягає в ефективному і раціональному управлінні будь-якими операціями на підприємстві [81]. Передбачає планування безперебійності бізнесу, що є критично важливим компонентом стратегії управління ризиками будь-якої організації, що дозволяє компаніям готуватися та реагувати на руйнівні події своєчасно та ефективно, тим самим мінімізуючи вплив на їхні операції та репутацію. Ефективність у процесі практичної реалізації операційного менеджменту на підприємствах критичної інфраструктури досягається під час управління наступними складниками:

– управлінням процесами створення та проектування операційної системи;

– управлінням функціонуванням операційної системи;

– управлінням якістю та продуктивністю операційної системи;

– управлінням забезпеченням стабільності функціонування операційної системи;

– управлінням перетвореннями, змінами та розвитком операційної системи [81].

Закордонні вчені у напрямку удосконалення операційного менеджменту

на підприємствах із посиленими ризиками (у т.ч. об'єкти критичної інфраструктри) пропонують створення плану операційної безперервності, який повинен включати ключові компоненти, що охоплюють усі аспекти діяльності (від персоналу до ІТ-інфраструктури, від ланцюгів поставок до відносин з клієнтами), серед них варто визначити наступні [307]:

– Оцінка ризиків та аналіз впливу на операційну діяльність – це початковий крок виявляє потенційні небезпеки та загрози, які можуть порушити основні операції, та оцінює потенційний вплив цих загроз на критичні функції та процеси, дозволяючи розставляти пріоритети.

– План реагування на надзвичайні ситуації – окреслює негайні кроки, які необхідно вжити під час та відразу після руйнівної події, включаючи процедури евакуації, зв'язку з аварійними службами та початкової комунікації з працівниками та зацікавленими сторонами (це слугує критично важливою першою лінією захисту).

– План відновлення операційної діяльності – деталізує процедури відновлення операцій, які можуть включати переїзд на резервний майданчик, відновлення даних та систем, а також отримання необхідних ресурсів та поставок. Ефективне відновлення зосереджується не лише на поверненні до бізнесу, але й на тому, щоб це відбувалося з збереженням довіри клієнтів та відповідності регуляторним вимогам.

– Резервне копіювання та відновлення даних – включає регулярне резервне копіювання даних у віддалені місця, використання хмарного сховища або впровадження комплексних рішень для аварійного відновлення. Регулярне тестування є вирішальним для забезпечення надійності та ефективного відновлення даних, мінімізуючи час простою.

– План комунікацій – визначає, як компанія буде спілкуватися з працівниками, клієнтами, постачальниками та іншими стейкхолдерами під час та після катастрофи. Це включає використання різних каналів зв'язку (електронна пошта, телефон, соціальні мережі, спеціальна гаряча лінія екстреної допомоги) та стратегію кризової комунікації для управління репутацією компанії.

– Навчання та тестування – регулярні навчання та симуляції є життєво важливими для забезпечення того, щоб працівники були ознайомлені з планом операційної безперебійності та знали, що робити в надзвичайній ситуації. Комплексне, захоплююче та адаптоване навчання допомагає виявити слабкі місця в планах реагування та покращує загальну стійкість.

Досвід України в умовах військового конфлікту підкреслює глибоке значення надійного управління операційною безперебійністю для забезпечення операцій та підтримки основних послуг, навіть під надзвичайним тиском. Іншими словами менеджмент операційної стійкості – це не лише відновлення після катастрофи, а це управління підтримкою мінімальних операційних рівнів під час збоїв та забезпечення своєчасного та ефективного відновлення до функціонального стану операційної системи. Директиви ЄС прямо зазначають, що стійкість включає «планування на

випадок непередбачених обставин у відповідь на загрози для забезпечення мінімального рівня операцій під час перебоїв та своєчасного відновлення» [301]. Це підкреслює, що менеджмент операційної стійкості є проактивною стратегією, яка забезпечує безперервність основних послуг, тим самим безпосередньо сприяючи стійкості шляхом зменшення часу простою та пом'якшення каскадних ефектів. Це виходить за межі простого «повернення до норми» до «підтримки функціональності під тиском» та повернення до стану стійкої роботи. Хоча дана концепція часто зосереджується на технічних системах та задокументованих процедурах, кінцева ефективність плану безперебійності бізнесу значною мірою залежить від людського розуміння, навчання та чітких ролей та обов'язків.

3. Антикризовий менеджмент. Антикризовий менеджмент включає ефективні стратегії реагування та відновлення, а також негайні та скоординовані дії, що вживаються під час, або відразу після руйнівної події, з основними цілями порятунку життів, обмеження шкоди та швидкого відновлення основних послуг. Неадекватна підготовка може призвести до серйозних наслідків, включаючи людські жертви, значні матеріальні збитки та вигорання рятувальників [282]. Ключові елементи ефективного антикризового менеджменту підприємств критичної інфраструктри які виділяють учені [2] можуть містити:

– Чіткі протоколи комунікації – встановлення чітких методів як внутрішньої, так і зовнішньої комунікації є першочерговим для зменшення плутанини, забезпечення розуміння всіма членами команди своїх ролей та сприяння ефективній співпраці під час інцидентів. Це включає наявність готових загальних заяв, виважену публічну відповідь та забезпечення прозорості та чесності в поширенні інформації.

– Визначена ієрархія та ролі – чітко визначена ієрархія та призначені ролі та обов'язки для конкретних осіб дозволяють швидко та ефективно приймати рішення, забезпечуючи безперебійні операції, коли час є критичним.

– Розподіл ресурсів – заздалегідь спланований розподіл ресурсів на основі серйозності та характеру ситуації гарантує, що найневідкладніші потреби будуть задоволені в першу чергу. Це включає пріоритетне відновлення критично важливих об'єктів, таких як лікарні та аварійні служби.

– Взаємодія та співпраця – ефективний кризовий менеджмент вимагає співпраці з іншими організаціями та установами для забезпечення безперешкодного обміну інформацією та скоординованих дій. Взаємодіючі системи дозволяють установам ефективно працювати разом під час надзвичайних ситуацій. CISA, наприклад, працює над зміцненням можливостей екстреного зв'язку та реагування у федеральних, державних, місцевих, племінних та територіальних урядів через довірчі відносини та розробку програм [149].

– Методи навчання та симуляції – регулярні навчання та тренування,

включаючи сценарії, настільні навчання та передові методи, такі як навчання у віртуальній та доповненій реальності, є вирішальними для підготовки команд до реальних інцидентів, відточування тактичної майстерності та виявлення прогалин у планах.

– Післяінцидентний аналіз – характерна риса високоефективних організацій, включають збір зворотного зв'язку від усіх учасників, аналіз того, що спрацювало, а що ні, та оновлення планів реагування на основі отриманих уроків. Ця прихильність до самооцінки та постійного вдосконалення є життєво важливою для майбутньої готовності.

– Лідерство в кризовій ситуації – є життєво важливим, вимагаючи ситуаційної обізнаності, здатності передбачати потенційні збої та встановлювати надійні непередбачені обставини, а також сильного зосередження на підтримці добробуту колективу і реагування на кризи.

Хоча антикризовий менеджмент за своєю суттю полягає в реагуванні на подію, сучасні концепції наголошують на широкому докризовому плануванні, відпрацюваннях та безперервному навчанні для значного підвищення оперативності та зменшення впливу. Це демонструє, що ефективний кризовий менеджмент полягає не лише в реагуванні на подію в міру її розвитку, а й у широкій підготовці, яка передбачає потенційні сценарії, формує практичні компетенції за допомогою реалістичних навчань та встановлює чіткі протоколи до настання кризи. Ця проактивна позиція значно зменшує хаос, покращує прийняття рішень під тиском та, зрештою, призводить до кращих результатів у ситуаціях високого стресу.

Інші провідні концепції менеджменту для підвищення стійкості об'єктів критичної інфраструктури можемо узагальнити у таблиці 2.4.

Подальший розвиток інструментарію менеджменту у сфері безпеки об'єктів критичної інфраструктури включає прогнозовані методи, що фіксують характеристики системи в режимі реального часу в нормальних умовах. Осмислення ролі людського чинника у виникненні кризових ситуацій трансформувалося в концепцію організаційного чинника. Згідно з нею, якщо у відповідній ситуації людина припускається критичної помилки, відповідальність лежить не лише на працівнику, а й на системі, яка допустила таку помилку, не створивши необхідних запобіжних механізмів. Комплексне застосування подібних методів дозволило значно знизити частоту катастрофічних подій, що свідчить про беззаперечний прогрес у сфері забезпечення надійного функціонування об'єктів критичної інфраструктури [2]. Усвідомлюючи таку тенденцію, міжнародні організації наголосили на необхідності зміни глобального підходу до питань безпеки. Зокрема, було розроблено нові нормативні документи, які об'єднують стандарти та рекомендовані практики з метою [256]: посилення координації між усіма ресурсами й зацікавленими сторонами; створення єдиної юридичної основи; розвитку універсальних стандартів; ефективного реагування на майбутні виклики; залучення спеціалізованих експертних груп до міжрегіональної співпраці; реалізації нових стратегій безпеки.

Таблиця 2.4 – Концепції безпекового менеджменту для підвищення стійкості об'єктів критичної інфраструктури

Концепція та її суть	Можливості застосування
Альтернативні концепції	
Концепція життєздатної системи (Viable System Model – VSM). Підприємство розглядається як контрольована система	Є доцільною для узгодження інтересів внутрішніх стейкхолдерів та формування адаптивної системи управління безпекою підприємства критичної інфраструктури. Це сприяє підвищенню стійкості організації до загроз і забезпечує ефективне досягнення цілей економічної безпеки.
Управління за цілями (Management by Objectives – MBO). Цілісна система управління, орієнтована на кінцеві результати і заснована на використанні творчого потенціалу трудового колективу, нових методів і технологій управління	Систематичне та організоване застосування концепції створює основу для ухвалення управлінських рішень, спрямованих на досягнення цілей економічної безпеки підприємства та максимізацію результатів з використанням наявних ресурсів.
Концепція загального управління якістю (TQM). Постійне вдосконалення якості продукції, організації процесів та підвищення рівня кваліфікації персоналу, що дозволяє досягти швидкого і результативного розвитку бізнесу	Концепція може бути ефективно застосована для узгодження інтересів внутрішніх і зовнішніх стейкхолдерів як однієї з ключових цілей управління економічною безпекою підприємства.
Взаємодоповнюючі концепції	
Концепції сталого розвитку (Sustainable Development Conception). Сталий розвиток розглядається як керований процес	Концепція може слугувати імперативною настановою в управлінні економічною безпекою підприємства, орієнтованого на розвиток і стійкість**.**
Концепції управління вартістю (Value-Based Management). Концепція спрямована на вдосконалення стратегічних й оперативних рішень на всіх рівнях підприємства за рахунок концентрації зусиль тих, хто приймає рішення, на ключових факторах вартості	Застосування цієї концепції може стати основою для стратегічних і оперативних рішень, спрямованих на формування ресурсного забезпечення**,** адекватного потребам управління економічною безпекою підприємства.
Концепції стратегічного управління (SMC). Стосуються безперервних процесів оцінювання зовнішнього середовища, формулювання організаційних цілей, прийняття рішень щодо створення й утримання конкурентних переваг.	Концепція є підґрунтям управління економічною безпекою підприємства на засадах «жорстких змін» та настановою такого управління, орієнтованого на досягнення стратегічних цілей підприємства

Джерело: узагальнено на основі [31;298]

Варто також відзначити концепцію адаптивного менеджменту, що передбачає прийняття змін та сприяння безперервному навчанню. Адаптивний менеджмент характеризується як ітеративний та гнучкий підхід до управління складними системами, що включає безперервний цикл планування, впровадження, моніторингу та оцінки. Його основним принципом є зосередження на навчанні та адаптації, сприйняття невизначеності як невід'ємної можливості для інновацій, а не перешкоди.

Ключові принципи адаптивного менеджменту:

– Ітеративність – включає безперервний цикл, де кожна ітерація ґрунтується на уроках, отриманих з попередніх фаз планування, впровадження та оцінки.

– Гнучкість – підхід за своєю суттю є гнучким та чутливим, дозволяючи коригувати його на основі змінних умов та появи нової інформації.

– Співпраця – підкреслює активну участь різноманітних зацікавлених сторін, включаючи громадян, бізнес та державні установи, для залучення різноманітних перспектив та досвіду до процесу прийняття рішень [235].

Експериментування та навчання є критично важливими компонентами, що дозволяють організаціям глибше розуміти складні системи, якими вони керують, та знаходити більш ефективні рішення проблем. У контексті критичної інфраструктури адаптивний менеджмент чітко враховує вплив динамічних загроз, таких як зміна клімату (наприклад, екстремальні погодні явища, зміна температур, підвищення рівня моря) та прагне до класифікації як матеріальних (фізичних), так і нематеріальних (інституційних, культурних, екологічних) систем на основі результатів. Воно також надає значного значення розвитку та пріоритетності відносин, будь то між фізичними активами або між людьми та їхнім середовищем, оскільки ці відносини безпосередньо впливають на адаптивність критичної інфраструктури.

Перехід до адаптивного управління є прямим визнанням того, що традиційні, жорсткі моделі планування, які часто припускають передбачувані середовища, є недостатніми для динамічного, невизначеного та непередбачуваного характеру сучасних загроз критичній інфраструктурі. Адаптивний менеджмент визначається як «ітеративний та гнучкий» підхід, який прямо заявляє, що він полягає в «сприйнятті невизначеності як можливості для навчання та інновацій» [283]. Незважаючи на консенсус щодо необхідності адаптації, залишається незрозумілим, «що визначає адаптивність критичної інфраструктури, як вона стає адаптивною, та які наслідки цього» [283], що підкреслює внутрішню складність. Це означає, що зростаюча складність критичної інфраструктури, у поєднанні зі швидкою еволюцією загроз (наприклад, вплив зміни клімату, нові вектори кібератак), вимагає підходу до управління, який постійно вчиться з досвіду, моніторить результати та коригує стратегії в реальному часі, а не покладається на фіксовані, довгострокові плани.

Адаптивне управління підкреслює, що стійкість критичної інфраструктури полягає не лише в надійності фізичних чи технічних активів, а й у базових людських, організаційних та реляційних мережах. Учені чітко зазначають, що «розвиток та пріоритетність відносин (наприклад, між фізичними активами або між людьми та їхнім середовищем) можуть впливати на адаптивність критичної інфраструктури» [13]. Також підкреслюється спільна участь різноманітних зацікавлених сторін. Це означає, що формування міцних міжорганізаційних відносин, створення ефективних мереж обміну інформацією та виховання культури колективного

вирішення проблем та спільного розуміння є настільки ж важливими, як і технологічні інвестиції для побудови адаптивної спроможності.

Важливою складовою ефективного менеджменту об'єктів критичної інфраструктури, особливо в умовах підвищених ризиків безпекового середовища є стратегічне прогнозування – передбачення майбутніх загроз та можливостей їх профілактики. Стратегічне прогнозування є структурованим підходом, що дозволяє організаціям передбачати зміни, виявляти можливості та зменшувати ризики. Замість того, щоб реагувати на збої, передбачення дозволяє виявляти сигнали змін на ранній стадії, надаючи можливість для інновацій та зростання. Без передбачення майбутнього організації ризикують відставати у розвитку [221].

Методологія стратегічного прогнозування включає визначення областей розвідки, належний робочий процес та структуру управління для полегшення сканування навколишнього середовища, горизонтного сканування, аналізу тенденцій або сценарного планування. Це допомагає організаціям зрозуміти нові технології, суспільні зміни та інші фактори, які можуть суттєво вплинути на їх розвиток. CISA (Агентство з кібербезпеки та безпеки інфраструктури) використовує свою серію «Безпечне завтра» як стратегічну можливість передбачення для вивчення нових та розвиваючихся ризиків, які можуть суттєво вплинути на критичну інфраструктуру нації протягом наступних 5-20 років. Ця серія прагне побудувати більш стійке та безпечне майбутнє, об'єднуючи групи експертів, лідерів думок та інших зацікавлених сторін з різним досвідом для проактивного мислення про майбутні ризики. Виявлення цих ризиків є важливим для їх пом'якшення до того, як вони вплинуть на системи критичної інфраструктури [329].

Необхідність вийти за межі реактивних підходів є очевидною в контексті стратегічного прогнозування. Традиційні підходи до управління ризиками часто зосереджуються на відомих загрозах та минулих інцидентах. Однак ландшафт загроз критичній інфраструктурі є динамічним і постійно еволюціонує, включаючи нові технології, такі як інтерфейси штучного інтелекту, можуть створювати як можливості, так і значні ризики. Покладаючись лише на реактивні заходи, організації ризикують бути заскоченими несподіваними подіями, що призводить до значних збоїв та втрат. Стратегічне передбачення, навпаки, дозволяє завчасно виявляти «слабкі сигнали» – ранні індикатори потенційних змін у галузі чи на ринку. Це дає підприємствам критичної інфраструктури можливість діяти до того, як конкуренти, отримуючи перевагу першопрохідця, що є особливо важливим при адаптації до нових технологій, які можуть трансформувати галузь. Таким чином, це дозволяє організаціям розробляти гнучкі ініціативи, які відповідають кільком майбутнім сценаріям, забезпечуючи довгостроковий успіх, який не залишається на волю випадку.

Варто також відзначити, що людський фактор також відіграє значну роль у стійкості підприємств критичної інфраструктури. Хоча технічні рішення відіграють життєво важливі функції у безпеці, покладатися лише на них недостатньо. Підхід, що враховує людський фактор, є важливим для

ефективного зменшення ризиків. Цей підхід визнає, що людська поведінка та пізнання є критично важливими факторами, які необхідно враховувати при розробці безпечних систем [332]. Людська помилка залишається поширеною та значною проблемою в безпеці, причому дослідження показують, що приблизно 90% збоїв можна пояснити людською помилкою, навіть серед добре навчених та мотивованих осіб [339]. Фактори, такі як часовий тиск, організаційна невизначеність, неадекватне навчання та відсутність обізнаності про ризики, сприяють людським помилкам та створюють значні виклики для зусиль з безпеки. У безпеко-критичних середовищах, де рішення є чутливими до часу, а робоче навантаження високе, ризик людської помилки зростає, особливо в деградованих або аварійних режимах, де несправності обладнання можуть посилити ризики, що може призвести до серйозних операційних або організаційних наслідків [352].

Відповідно, одним із пріоритетних завдань сучасного менеджменту на підприємствах критичної інфраструктури є формування таких управлінських підходів, що враховують людський фактор, охоплюючи різні аспекти, зокрема операційний інтерфейс «людина-машина», аналіз людських помилок, організаційні процеси та політики, адекватність навчання та чіткість щодо обов'язків та комунікації. Методології людського фактора, такі як когнітивний аналіз завдань та аналіз робочого навантаження, допомагають виявити джерела людських помилок та потенційні ризики безпеки. Проєкти, що стосуються ролі людського фактора, спрямовані на підвищення стійкості критичної інфраструктури до природних небезпек, навмисних та випадкових шкідливих дій людини, включаючи кібератаки, диверсії, теракти, колабораціонізм та ін. Акцент робиться на здатності критичної інфраструктури, що залежить від людини, справлятися з несприятливою подією, включаючи її здатність готуватися до кризи, поглинати вплив, скорочувати час відновлення та адаптуватися шляхом зменшення майбутнього впливу та вразливостей [282].

Отже, у сфері менеджменту підприємств критичної інфраструктури виникає необхідність ефективного внеску соціально-гуманітарних дисциплін та залучення експертів, установ, а також включення відповідного соціально-гуманітарного досвіду є важливою для досягнення значущих та суттєвих ефектів, що підвищують суспільний вплив пов'язаних досліджень та інноваційної діяльності. Це означає, що співпраця між фахівцями з людського фактора, інженерами з безпеки та експертами з безпеки є все більш необхідною для розробки більш надійних та стійких систем, які захищають критичну інфраструктуру від загроз, що постійно розвиваються. Визнання внутрішньої схильності людини до помилок та важливості людської поведінки та пізнання в кібербезпеці, а також врахування потреб та обмежень операторів, є фундаментальним кроком до забезпечення цілісності, конфіденційності та доступності критичних систем. На сучасному етапі забезпечення стійкості об'єктів критичної інфраструктури потребує впровадження інноваційних концепцій менеджменту, які враховують

зростаючу складність, взаємозалежність систем та динамічний характер загроз. Серед провідних підходів, що формують нову парадигму менеджменту стійкості критичної інфраструктури, виділяють наступні:

1. Концепція управління ризиками та стійкістю. Цей підхід передбачає поєднання управління ризиками з заходами, спрямованими на підвищення стійкості критично важливих підприємств. Він включає ідентифікацію потенційних загроз, оцінку вразливостей та розробку стратегій реагування, що дозволяє забезпечити безперервність функціонування критичних систем навіть у разі виникнення надзвичайних ситуацій. Застосування цього підходу сприяє формуванню культури проактивного управління та адаптації до змінних умов середовища.

2. Концепція «антикрихкості» – запропонована Насімом Талебом і передбачає, що системи можуть не лише витримувати стресові впливи, але й покращувати свої характеристики внаслідок них [42]. У контексті критичної інфраструктури це означає створення таких структур, які здатні навчатися на кризах, адаптуватися та еволюціонувати, стаючи більш ефективними та надійними .

3. Конвергенція безпеки – цей підхід полягає в інтеграції фізичної та інформаційної безпеки в єдину систему управління. З огляду на зростаючу кіберзагрозу для критичної інфраструктури, конвергенція безпеки дозволяє забезпечити комплексний захист інфраструктурних об’єктів, враховуючи як фізичні, так і цифрові аспекти безпеки .

4. Модель багаторівневого управління (Multi-Level Governance Model) – ця модель передбачає координацію дій між різними рівнями управління (від національного до місцевого). Вона сприяє ефективному обміну інформацією, узгодженню стратегій та спільному реагуванню на загрози, що є ключовим для забезпечення стійкості критичної інфраструктури в умовах складних та взаємозалежних систем .

Застосування зазначених концепцій менеджменту в комплексі дозволяє створити ефективну систему управління стійкістю критичної інфраструктури, здатну адаптуватися до сучасних викликів та забезпечувати безперервність життєво важливих функцій суспільства. У довгостроковій перспективі вибір конкретних управлінських заходів має базуватися на стратегічних цілях розвитку країни та її соціально-економічних планах, при цьому необхідно враховувати результати техніко-економічного аналізу в межах конкретного об’єкту. Такий аналіз дозволяє оцінити доцільність реалізації заходів, спрямованих на підвищення стійкості критичної інфраструктури, з урахуванням доступних ресурсів та спроможності об’єкта критичної інфраструктури в майбутньому ефективно експлуатувати нові безпекові рішення. У процесі вибору та реалізації концепції менеджменту для забезпечення безпеки критичної інфраструктури необхідно брати до уваги низку ключових чинників:

1. Ресурсне забезпечення. Безперервне функціонування критичних об’єктів до, під час та після кризи вимагає системного управління ресурсами,

що охоплюють фінансові, людські, технічні, інформаційні та інші матеріально-технічні компоненти. Забезпечення належного рівня готовності вимагає заздалегідь сформованої бази підтримки потреб усіх етапів реагування та відновлення.

2. Спроможність до реагування. Наявність інституційного, організаційного й професійного потенціалу для реагування на кризові ситуації є критично важливою умовою ефективного менеджменту безпеки. Це стосується як органів місцевого самоврядування, так і операторів інфраструктури, сил безпеки та оборони, а також громадського сектору. Усі стейкхолдери повинні мати змогу виконувати свої функції в умовах підвищеного ризику.

3. Технології та інновації. Вибір концепції менеджменту повинен передбачати активне використання сучасних технологій у процесах прогнозування, моніторингу, захисту та відновлення. Інноваційні рішення мають інтегруватися в інфраструктурні системи з урахуванням можливостей їхньої експлуатації у кризових умовах. Важливим аспектом є також навчання персоналу, організація фінансування та доступ до спеціалізованих ресурсів.

Отже, формування управлінської моделі, орієнтованої на довгострокову стійкість, повинно ґрунтуватися на концепції випереджувальної адаптації. Такий підхід забезпечує готовність інфраструктури до функціонування в умовах майбутніх викликів і дає змогу не лише зберігати стабільність, але й досягати більш високого рівня ефективності після криз.

РОЗДІЛ 3
УДОСКОНАЛЕННЯ ОРГАНІЗАЦІЙНО-УПРАВЛІНСКОГО ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

3.1. Міжнародний досвід управлінського забезпечення стійкості об'єктів критичної інфраструктури

Сучасна воєнно-політична ситуація у світі формує нові багатовимірні ризики у сфері державної безпеки, зокрема щодо охорони критично важливих об'єктів. У цьому контексті управління системними ризиками вимагає поглибленої взаємодії між державними інституціями та міжнародними структурами, що функціонують у сфері забезпечення безпеки. Такий виклик актуалізує пошук нових управлінських підходів, інструментів виявлення, ідентифікації, стримування й нейтралізації потенційних загроз або, як мінімум, пом'якшення їхніх наслідків.

У зв'язку з цим заслуговує на увагу позиція С. С. Теленика, який розглядає критичну інфраструктуру як об'єкт адміністративно-правового регулювання [258, с. 185]. Учений наголошує на необхідності формування відповідної моделі діяльності, що повинна ґрунтуватися на чинній нормативній базі, стратегічно-програмних документах, кращих практиках правового забезпечення, а також запозиченому досвіді іноземних держав у цій сфері [258, с. 185].

Зважаючи на це, важливим є вивчення та порівняльний аналіз сучасних моделей державної політики провідних країн світу у сфері управління ризиками та забезпечення безпеки об'єктів критичної інфраструктури. Особливої уваги заслуговує досвід застосування превентивних механізмів, а також розбудови ефективних моделей взаємодії суб'єктів безпекової політики. При цьому ключовими характеристиками цих моделей є високий рівень координації захисних систем, забезпечення ситуаційної обізнаності стейкхолдерів, розвиток механізмів оперативного реагування, а також інституційна структурованість засобів безпеки.

Аналізуючи зарубіжний досвід, слід зазначити, що кожна держава формує власну модель захисту критичної інфраструктури, виокремлюючи критичні сектори, складаючи відповідні реєстри об'єктів та розраховуючи необхідні ресурси. Кількість таких секторів різниться, зважаючи на державні можливості, наявність інституційної підтримки, у тому числі з боку приватного сектору, який часто залучається до реалізації політики у цій сфері. Управління кожним сектором закріплюється за відповідними органами державної влади або агентствами, відповідальними також за підготовку фахівців і населення до ефективного реагування на характерні для певного сектора ризики [141, с. 145].

У США прикладом ефективної інституційної реалізації політики у сфері захисту критичної інфраструктури є діяльність Офісу захисту

інфраструктури (Office of Infrastructure Protection), що забезпечує загальне управління та координацію національних заходів у цій сфері, з акцентом на управління ризиками та підвищення рівня стійкості критичних об'єктів [83, с. 215].

Додатково важливу роль виконує Агентство з кібербезпеки та стійкості критичної інфраструктури (CISA) [155]. У його структурі діє Міжвідомчий комітет безпеки, який забезпечує ефективну комунікацію з державними органами, приватними компаніями та територіальними громадами на всіх рівнях. CISA виступає ключовим провідником міжсекторального партнерства у сфері безпеки, забезпечуючи стейкхолдерів інформаційними ресурсами, аналітичними інструментами та навчальними програмами, спрямованими на підвищення рівня обізнаності та готовності до загроз.

Серед функцій агентства – координація інформаційного обміну між державним і приватним секторами, що є критично важливим чинником у забезпеченні національної безпеки. Взаємодія з партнерами реалізується через галузеві координаційні ради, що спільно відповідають за мінімізацію ризиків, які загрожують стабільному функціонуванню критичних секторів. Експерти CISA проводять тренінги та навчальні заходи з безпеки критичної інфраструктури за допомогою різноманітних форматів – від дистанційного до очного навчання, включаючи самостійні курси й практичні семінари [155]. Тобто, агенція CISA відповідальна і за кіберзахист, і за захист критичної інфраструктури. Можемо зробити висновок, що Україна, запозичила досвід американської моделі, опираючись на досвід ЄС. Українська система захисту критичної інфраструктури відповідає новій Директиві ЄС 2557 щодо стійкості. Унікальність української системи кібербезпеки та захисту критичної інфраструктури варто відзначити у її адаптивності та еластичності, що дозволило під час повномасштабного вторгнення рф в Україну продемонструвати можливості до оперативного вдосконалення відповідно до новітніх загроз та кооперуватися для посилення національної безпеки.

Важливу роль у системі захисту критичної інфраструктури США виконує стратегічний документ – Національний план захисту інфраструктури 2013 (NIPP 2013) [329], розроблений Департаментом внутрішньої безпеки США. Він визначає підходи до захисту критичної інфраструктури країни від актів тероризму та інших небезпек. Цей план включає в себе координацію дій між федеральними, місцевими та приватними суб'єктами, а також визначає пріоритети та стратегії для ефективного захисту інфраструктури. Основний тезис, який прослідковується у NIPP 2013 проголошує, що «національне благополуччя залежить від безпечної та стійкої критичної інфраструктури» [329]. Основною метою Національного плану захисту критичної інфраструктури США 2013 року (NIPP 2013) є розвиток державно-приватного партнерства як ключового інструмента забезпечення безпеки та стійкості об'єктів критичної інфраструктури. Для досягнення цього завдання передбачено колективну участь усіх учасників процесу, включаючи державні органи, приватні компанії та громадські структури, з метою визначення

національних пріоритетів, формулювання стратегічних цілей, зменшення ризиків, оцінювання прогресу та адаптації до змінного середовища на основі зворотного зв'язку.

Серед ключових положень NIPP 2013 [329] виділяють:

1. Ідентифікацію та класифікацію секторів критичної інфраструктури;
2. Оцінювання ризиків і управління ними задля зниження потенційних загроз;
3. Розвиток інституційної взаємодії між органами державної влади, приватним сектором та місцевими органами управління;
4. Забезпечення обміну інформацією, особливо в контексті кібербезпеки;
5. Розробку стратегій реагування на інциденти та швидкого відновлення;
6. Визнання ролі та досвіду власників і операторів критичної інфраструктури;
7. Формування інтегрованого підходу, що охоплює всі рівні управління та забезпечує широке залучення суб'єктів різних секторів до системи національної безпеки.

У сучасних умовах національна безпекова політика США зазнає еволюції у напрямку формалізації статусу об'єктів критичної інфраструктури в нормативно-правовому полі, зокрема у федеральному законодавстві, указах Президента та відповідних директивах. Національна стратегія внутрішньої безпеки [332] окреслює перелік критичних секторів, серед яких: телекомунікації, енергетика, фінансово-банківська система, транспорт, водопостачання, служби реагування, державне управління, охорона здоров'я, хімічна промисловість, поштова служба, оборонно-промисловий комплекс, аграрний сектор та продовольче забезпечення [164]. У цьому документі також визначаються основні напрями координації зусиль федеральної та місцевої влади із залученням бізнес-структур до управління безпекою критичних об'єктів.

Важливим нормативним актом є Президентська політична директива з безпеки та стійкості критичної інфраструктури [338]. Документ визначає архітектуру інституційної взаємодії державних структур, приватного сектора й інших стейкхолдерів з метою формування пріоритетів захисту, оцінки вразливостей, розробки стратегій управління ризиками та програм підвищення стійкості. У директиві акцентується важливість інформаційної взаємодії, державно-приватного партнерства та скоординованого реагування на загрози як фізичного, так і кіберхарактеру.

Тріада стратегічних імперативів, яка визначає логіку дій у сфері безпеки критичної інфраструктури у США, включає:

1. гармонізацію діяльності федеральних органів влади для формування єдиного національного підходу до забезпечення безпеки;
2. створення ефективної системи обміну базовими даними та технічними стандартами;
3. інтеграцію аналітичної функції для забезпечення якісного планування і прийняття управлінських рішень [315].

Не менш значущим є документ «Національна стратегія фізичного захисту критичної інфраструктури та найважливіших об'єктів» [333], в якому закріплено концептуальний підхід до безпеки на засадах «спільної відповідальності». Ця модель передбачає участь усіх уповноважених суб'єктів – як на міжурядовому рівні (федерація, штати, місцеві органи влади), так і в межах міжсекторальної взаємодії між регуляторами та суб'єктами господарювання, що володіють або управляють об'єктами критичної інфраструктури. Така система дозволяє сформувати стійку та гнучку модель управління, яка відповідає викликам сучасного середовища. В межах даного інституційного конструкту визначено основні групи загроз:

– прямої інфраструктурної дії, що мають наростаючий (cascading) ефект та ведуть до руйнування об'єктів критичної інфраструктури внаслідок прямої атаки чи іншого впливу на ключові системи;

– непрямої інфраструктурної дії, здатна викликати збій, дезорганізацію роботи, в тому числі і за допомогою створення негативних соціальних ефектів;

– загрози використання конкретних об'єктів або їх елементів як засіб для ураження інших цілей.

Актуальним для аналізу та імплементації в українському контексті є підхід США до організації системи безпеки критичної інфраструктури, зокрема регламентований відповідними нормативно-правовими актами розподіл повноважень федерального уряду. Цей підхід передбачає чітке закріплення за кожним критичним сектором відповідного органу виконавчої влади, ідентифікованого як «провідне агентство» (lead agency), яке здійснює координацію, регулювання та надає інституційну підтримку в межах секторальної моделі управління. Національна стратегія фізичного захисту критичної інфраструктури та ключових об'єктів визначає параметри комплексного регулювання, включно з ідентифікацією об'єктів у кожному секторі, їх класифікацією, визначенням потенційних загроз, стандартизацією захисних вимог, систематизацією геопросторових даних, організацією механізмів обміну інформацією (включаючи дані з обмеженим доступом), а також регламентацією засобів захисту персоналу, який обслуговує об'єкти критичної інфраструктури [314].

Додатково вказаним документом визначено стратегічні напрямки наукових досліджень та технічних розробок, спрямованих на вдосконалення моделей безпеки та підвищення ефективності системи управління критичною інфраструктурою.

Сучасна парадигма національної та внутрішньої безпеки США також включає механізми обмеження участі іноземних інвесторів у сферах, пов'язаних із критично важливими об'єктами. Це створює передумови для законодавчих ініціатив, спрямованих на модернізацію процедури оцінювання ризиків, пов'язаних з іноземним капіталом у стратегічних секторах [163, с. 134; 307]. У відповідь на ці виклики розвідувальні структури США спільно з Міністерством оборони ініціювали низку регуляторних рішень щодо

посилення контролю за іноземними інвестиціями. Їхній зміст зосереджений на вимогах проходження обов'язкового аналізу відповідності інвестпроєктів інтересам національної безпеки. У межах цього процесу здійснюється перевірка щодо цілей, мотивів та потенційного впливу країни-інвестора, зокрема з урахуванням чинників належності до категорії «країн, що викликають особливе занепокоєння» (countries of special concern). У разі встановлення загроз, пов'язаних із спробами придбання критичних технологій або об'єктів, таким суб'єктам може бути відмовлено в укладенні відповідного правочину.

Законодавчі органи, у свою чергу, наполягають на обов'язковому розслідуванні потенційних наслідків таких угод для національної безпеки, особливо у випадках, коли йдеться про встановлення «кумулятивного контролю» (cumulative control) внаслідок попередніх правочинів із критичними об'єктами, енергетичними потужностями або стратегічно важливими матеріалами. Така політика є прикладом застосування стратегічного комплексу превентивних заходів, спрямованих на мінімізацію ризиків внутрішньої дестабілізації інфраструктурної безпеки.

Окрему увагу варто приділити діяльності Офісу захисту інфраструктури США, який надає пріоритет підготовці фахівців, задіяних у забезпеченні безпеки об'єктів критичної інфраструктури у таких секторах, як енергетика, хімічна промисловість, комерційна інфраструктура, гідротехнічні об'єкти тощо. У межах освітніх програм регулярно проводяться спеціалізовані семінари, під час яких персонал інформується про новітні тенденції, актуальні загрози та практики підвищення стійкості критичної інфраструктури. Таким чином, формуються секторальні системи професійної підготовки, що сприяють розвитку компетенцій серед персоналу та громад щодо ефективного забезпечення безпеки критичної інфраструктури.

Відзначимо, що суттєвим інституційним проривом у сфері захисту критичної інфраструктури стало прийняття 15 листопада 2021 року Закону про інвестиції в інфраструктуру та робочі місця [316], який долучив до даного процесу також Управління науково-технічної політики (OSTP). Основна місія даного інституту передбачає співпрацю з федеральними департаментами, агентствами та Конгресом для створення спільної візії та єдиних стратегій, чітких планів, зваженої державної політики та ефективних рішень на основі наукового обґрунтування. OSTP також посилює взаємодію із зовнішніми партнерами, включаючи промисловість, благодійні організації та громадянське суспільство, державні, місцеві та територіальні органи влади. Діяльність OSTP орієнтована також на покращення розуміння впливу надзвичайних подій на критичну інфраструктуру та стимулювання дослідницької діяльності для надання практичної, керованої даними, конкретної та дієвої інформації, концепцій, методів, технологій, а також інструменти для власників і операторів критичної інфраструктури щодо потенційного пом'якшення впливу та відновлення після подій [178]. Зазначеним вище законом регламентовано спільні дії OSTP та Міністерства

внутрішньої безпеки (Department of Homeland Security – DHS) у напрямку проведення досліджень, розробки, тестування та оцінки критичної інфраструктури на її стійкість. На підтримку Закону OSTP розробила стратегічну структуру та план витрат на підтримку безпеки та стійкості критичної інфраструктури, а також створила Програму дослідження безпеки та стійкості критичної інфраструктури (CISRR) для керування широким спектром пов'язаних заходів, що проводяться OSTP для вирішення проблем критичної інфраструктури. Окрім цього Законом «Про інвестиції в інфраструктуру та робочі місця» передбачено до 2026 року фінансування у розмірі 550 млрд дол. США на нові інфраструктурні ініціативи, серед яких: ремонт і реконструкція доріг і мостів (110 млрд дол.), модернізація та обслуговування пасажирських і вантажних залізничних систем (66 млрд дол.), оновлення ліній електропередач, запобігання виходу з ладу елементів електромереж та забезпечення збільшення частки відновних джерел енергії (65 млрд дол.), розширення широкосмугового зв'язку в сільській місцевості та малозабезпечених громадах (65 млрд дол.), забезпечення населення чистою питною водою, включаючи заміну свинцевих труб і боротьбу із забрудненням вод свинцем та іншими хімікатами (55 млрд дол.), захист інфраструктури від фізичних атак, кібертероризму та погодних катаклізмів (55 млрд дол.), оновлення громадського транспорту, створення нових автобусних маршрутів і підвищення доступності для людей похилого віку та інвалідів (39 млрд дол.), модернізація та розширення американських аеропортів, диспетчерських веж і систем контролю (25 млрд дол.), прибирання територій Суперфонду та забудованих територій, покинутих шахт і старих нафтових і газових свердловин (21 млрд дол.), портову інфраструктуру та викиди вантажівок у портах (17 млрд дол.), забезпечення безпечних зон на дорогах, пішоходах, трубопроводах та інших (11 млрд дол.), інфраструктуру водопостачання Заходу країни, включаючи розвиток зрошення та протидії посухам (8 млрд дол.), розвиток загальнонаціональної мережі зарядних станцій для електромобілів (7,5 млрд дол.), електричні шкільні автобуси, переважно для малозабезпечених, сільських та племінних громад (5 млрд дол.) [303]. Отже, зазначений інвестиційний пакет покликаний модернізувати застарілі елементи критичної інфраструктури та посилити її стійкість.

Аналіз практики реагування на надзвичайні ситуації у сфері критичної інфраструктури США свідчить про наявність чітко налагодженого механізму координації між Департаментом внутрішньої безпеки (Department of Homeland Security – DHS) та власниками й операторами об'єктів критичної інфраструктури. Цей процес координується Національним координаційним центром інфраструктури (National Infrastructure Coordinating Center – NICC), що виконує функції центрального органу забезпечення фізичної безпеки та стійкості активів критичної інфраструктури. NICC забезпечує постійний зв'язок з федеральними структурами, відомствами та суб'єктами приватного сектора, моніторингом потенціалу реагування, ситуаційною обізнаністю та

підтримкою безпеки на регіональному та національному рівнях [142].

Відповідно до Президентської політичної директиви 21 (Presidential Policy Directive 21) [338], центральне місце у структурі забезпечення стійкості займають як фізичні, так і кіберкоординаційні центри. У сфері кібербезпеки провідну роль виконує Національний центр інтеграції кібербезпеки та комунікацій (National Cybersecurity and Communications Integration Center – NCCIC). У межах DHS він функціонує як головна організація з координації заходів кіберзахисту критичної інфраструктури. NCCIC здійснює управління процесами реагування, пом'якшення наслідків та відновлення після значущих кіберінцидентів у тісній взаємодії з правоохоронними структурами, розвідувальними агентствами, міжнародними групами реагування, національними центрами аналізу інформації та суб'єктами критичної інфраструктури [142]. Основна мета діяльності NCCIC полягає у зборі, захисті та обробці даних, що дозволяє оперативно реагувати на кіберзагрози в межах усього спектра безпекових завдань.

NICC і NCCIC, доповнені функцією комплексного аналізу, забезпечують ефективну систему обміну інформацією, формуючи розгалужену систему ситуаційної обізнаності в секторах критичної інфраструктури. Комунікація забезпечується як безпосередньо з центрами, так і через відповідні галузеві агентства (Sector-Specific Agencies – SSA), регіональні кластери, центри обміну та аналізу інформації (Information Sharing and Analysis Centers – ISAC), синтетичні аналітичні центри тощо. Така багаторівнева архітектура інформаційного обміну сприяє підвищенню ефективності реагування на інциденти, узгодженості дій між стейкхолдерами та уніфікації аналітичних підходів до оцінювання загроз.

Особливе значення у системі комунікацій посідає Інформаційна мережа внутрішньої безпеки – Критична інфраструктура (Homeland Security Information Network – Critical Infrastructure – HSIN-CI). Дана платформа забезпечує захищений мережевий канал обміну інформацією між усіма учасниками системи захисту КІ. Стейкхолдери мають доступ до матеріалів, що охоплюють повний спектр безпекових інтересів, зокрема: звітів про інциденти, аналітики загроз, моделювання потенційних впливів, оцінок вразливості, рекомендацій щодо захисних заходів. Контент HSIN-CI адмініструється NICC, що гарантує його актуальність та оперативну наповнюваність. Окремі критично важливі сектори (та підсектори) управляють власними портальними ресурсами в межах HSIN-CI [149]. Завдяки такій структурі забезпечується цілісна та ефективна система взаємодії у сфері захисту критичної інфраструктури, що базується на партнерстві, інформаційній відкритості та технологічній інтеграції.

Щоб забезпечити широкий обмін важливою інформацією, NICC також отримує та надає інформацію через інші портали. Наприклад, створено Портал команди комп'ютерної готовності до надзвичайних ситуацій Сполучених Штатів (United States Computer Emergency Readiness Team –

US-CERT) і Команди реагування на надзвичайні ситуації промислових систем керування (ICS-CERT). NCCIC надає безпечну веб-платформу для спільної роботи системи з обміну конфіденційною інформацією щодо забезпечення кібербезпеки, фізичного захисту, депферності, превентивного реагування та регенерації із залученням приватного сектору, уряду і міжнародних партнерів. Він надає партнерам доступ до двох компонентів захищеного порталу, які містять інформацію про кіберіндикатори, інциденти та перелік відомого зловмисного програмного забезпечення, що може використовуватись проти систем критичної інфраструктури:

– Cobalt Compartment – інформаційний центр безпеки корпоративних систем.

– Відділ систем керування (The Control System Compartment) – містить матеріали про промислові системи керування, обмежені власниками та операторами активів систем керування [156].

Секторальні та міжгалузеві структури включають:

– Галузеві координаційні ради (Sector Coordinating Councils – SCCs) – самоорганізовані, самокеровані та самоврядні ради стейкхолдерів, що складаються з власників, операторів та їхніх представників, які взаємодіють у широкому діапазоні галузевих стратегій, політики, діяльності та безпекових питань. SCCs служать основними точками співпраці між урядом і власниками (операторами) об'єктів критичної інфраструктури та приватного сектору для координації та планування політики безпеки та стійкості критичної інфраструктури.

– Міжгалузева рада критичної інфраструктури – рада стейкхолдерів, що складається з голів і заступників голів SCCs, координує міжсекторальні питання, ініціативи та взаємозалежності для підтримки безпеки та стійкості критичної інфраструктури.

– Урядові координаційні ради (GCC) – складаються з представників різних рівнів влади (включно з федеральним), відповідно до робочого ландшафту кожного окремого сектору, ці ради забезпечують міжвідомчу, міжурядову та міжюрисдикційну координацію всередині та між секторах і співпрацювати з SCCs на основі державно-приватного партнерства.

– Федеральна рада вищого керівництва (FSLC) – складається з вищих посадових осіб з SSA та інших федеральних департаментів та агентств, які відіграють роль у забезпеченні безпеки та стійкості критичної інфраструктури, FSLC сприяє комунікації та координації у сфері безпеки та стійкості критичної інфраструктури на федеральному рівні.

– Координаційна рада державного, місцевого та територіального уряду (SLTTGCC) – складається з представників серед державних установ. SLTTGCC сприяє залученню партнерів з безпеки та стійкості до національної критичної інфраструктури та забезпечує організаційну структуру для координації між державними та місцевими рівнями юрисдикції в розробці та реалізації урядових стратегій та програм.

– Координаційна рада регіонального кластеру (RC3) – включає

регіональні групи та коаліції по всій країні у різноманітних ініціативах з підвищення безпеки та стійкості критичної інфраструктури в державному та приватному секторах [149].

Аналізуючи основні інституційно-правові засади державної політики США у сфері захисту критичної інфраструктури, можна узагальнити низку кращих практик, релевантних до вивчення та потенційного впровадження в Україні. Зокрема, актуальним видається визначення послідовності основних кроків формування національної концепції безпеки та стійкості критичної інфраструктури:

1. Встановлення стратегічних цілей та завдань концепції.
2. Аналіз міжнародного досвіду, виявлення прикладів ефективних програм і планів безпеки та стійкості критичної інфраструктури, які можуть бути адаптовані до національного контексту.
3. Визначення перспектив імплементації зазначених практик у розрізі окремих секторів критичної інфраструктури.
4. Ідентифікація основних стейкхолдерів у кожному секторі.
5. Закріплення інституційних ролей та обов'язків відповідальних суб'єктів.
6. Формування механізмів міжвідомчої координації та комунікації між державними інституціями, операторами критичної інфраструктури та іншими заінтересованими сторонами.
7. Розбудова системи управління ризиками, встановлення алгоритмів реагування, створення переліку індикаторів ефективності та проведення їхньої оцінки.
8. Розробка сценаріїв міжсекторальних навчань та тренувань.
9. Визначення часових параметрів реалізації заходів і контроль за їх дотриманням.
10. Пропагування необхідності широкого залучення стейкхолдерів та популяризація засад концепції.

Зазначені кроки формують підґрунтя для побудови ефективної системи реагування, в якій кожен суб'єкт чітко усвідомлює свої функції в умовах загроз.

Доцільно також звернути увагу на досвід Європейського Союзу у сфері реалізації державної політики захисту критичної інфраструктури. У межах Європейської програми захисту критичної інфраструктури (European Programme for Critical Infrastructure Protection – EPCIP) Європейська комісія ініціювала пакет заходів, спрямованих на підвищення захищеності об'єктів критичної інфраструктури держав-членів ЄС. Значним елементом цієї програми є ініціатива з захисту критичної інформаційної інфраструктури (Critical Information Infrastructure Protection – CIP), яка покликана зміцнити безпеку ІКТ-компонентів життєво важливої інфраструктури [293].

У межах реалізації EPCIP було створено Комісію інформаційного попередження про критичну інфраструктуру (CIWIN – Commission of a Critical Infrastructure Warning Information Network), що виконує функції

захищеної інформаційно-комунікаційної платформи для обміну даними про спільні загрози, вразливості, заходи реагування та превентивні стратегії серед членів спільноти CIP ЄС. Портал CIWIN функціонує з січня 2013 року, забезпечуючи міждержавну координацію й обмін передовими практиками [149].

Вивчення зарубіжного досвіду дає підстави стверджувати, що спільною характеристикою державної політики у сфері критичної інфраструктури є її орієнтація на досягнення стійкості систем. R. Cantelmi запропонував розглядати стійкість у рамках часової послідовності фаз антикризового управління – «до, під час і після» кризи [289]. Такий підхід дозволяє трактувати стійкість як багатокомпонентну категорію, що охоплює повний цикл управління кризами.

T. W. Coombs, у свою чергу, виокремлює три основні стадії процесу забезпечення стійкості: докризову, кризову та посткризову. Докризова фаза включає оцінку ризиків, розробку планів, реалізацію профілактичних заходів; кризова – оперативне реагування та управління інцидентами; посткризова – аналіз наслідків, відновлення функціонування та реалізація заходів запобігання майбутнім інцидентам [294, с. 198].

Таким чином, поняття стійкості критичної інфраструктури передбачає не лише здатність протидіяти загрозам, але й адаптуватися до них та ефективно відновлюватися. Варто також визнати, що інциденти на об’єктах критичної інфраструктури неминучі, тому акцент слід робити на розвитку абсорбційної та адаптаційної спроможності систем.

Продовжуючи аналізувати змістовне наповнення теоретизування «стійкість», звернемось до словника Управління ООН зі зменшення ризику стихійних лих (UNDRR) у якому дана дефініція ідентифікується як «здатність системи, громади або суспільства, що піддаються впливу небезпеки, протистояти, поглинати, адаптуватися та відновлюватися від наслідків небезпеки своєчасно та ефективно, в тому числі шляхом збереження та відновлення своїх основних базових структур та функцій» [351]. Стійкість системи критичної інфраструктури іноземні учені трактують як здатність протидіяти, адаптуватися та швидко відновлюватися після потенційно деструктивної події [342. с. 25].

Актуалізація феномену стійкості критичної інфраструктури знаходить пояснення у проєкті Critical Entities Resilience Directive 2022 року (Директива CER) [301] це питання у зазначеному документі належним чином відзначене: «необхідно докорінно змінити нинішній підхід із захисту конкретних активів на посилення стійкості критично важливих об’єктів». У цьому контексті «стійкість» означає здатність запобігати, протистояти, пом’якшувати, абсорбувати, пристосовуватися та відновлюватися після інциденту, який порушує або може порушити роботу критично важливого об’єкта. Насправді це досить добре відповідає основному визначенню в літературі з питань стійкості критичної інфраструктури. Зміну вектору безпекової парадигми ЄС можна пояснити зростанням кількості держав-членів, які усе більше

усвідомлюють важливість ідеї стійкості, в якій захист не є основою стабільності роботи критичної інфраструктури, а однією зі складових поряд із запобіганням і пом'якшенням ризиків та відновленням. Виходячи з цього, Європейська Комісія у своїй пропозиції дійшла висновку, що необхідно забезпечити «більш комплексний підхід до забезпечення стійкості критично важливих об'єктів у низці секторів у всьому Європейському Союзі» [297].

Погоджуємось із думкою О.Суходолі [254, с. 2], який стверджує що основна ціль політики ЄС щодо забезпечення стійкості критичної інфраструктури полягає у підвищенні спроможності держав-членів гарантувати безперебійність надання основних життєво важливих послуг підтримки суспільних функцій, громадського здоров'я, економічної діяльності та безпеки навколишнього середовища на внутрішньому ринку ЄС. Директива CER відводить особливе місце розбудові спроможності ЄС та держав-членів бути підготовленими до виникнення кризових ситуацій.

Варто відмітити, що Директива CER стала основоположною інституцією на шляху стратегічного зміцнення безпеки критичної інфраструктури ЄС крізь призму її стійкості. Із цією метою документ передбачає імплементацію державами-членами ЄС наступних заходів:

– ухвалення стратегій підвищення стійкості критичних об'єктів;

– розробку на національному рівні у визначених Директивою CER секторах вимоги до проведення ризик-аналізу стійкості на об'єктах критичної інфраструктури;

– зобов'язання операторів критичних об'єктів до розробки та ратифікації планів стійкості технічних, безпекових та організаційних заходів відповідно до визначеного рівня загроз;

– організація груп стійкості операторів критичної інфраструктури у якості консультативно-координаційного механізму діяльності Єврокомісії;

– створення дорадчого інституту з метою допомогти операторам критичних об'єктів оцінити дієвість вжитих заходів забезпечення стійкості;

– призначення уповноважених координаційних органів для забезпечення взаємодії між державами-членами ЄС, Єврокомісією, інститутами та операторами критичних об'єктів ЄС з метою оцінювання стану імплементації положень Директиви CER;

– підготовка методичних та інструктивних матеріалів для проведення колективних навчань, консультування, запровадження програм підвищення кваліфікації персоналу операторів критичної інфраструктури [254, с. 3], [301].

Аналізуючи основні інституційно-правові засади державної політики США у сфері захисту критичної інфраструктури, можна узагальнити низку кращих практик, релевантних до вивчення та потенційного впровадження в Україні. Зокрема, актуальним видається визначення послідовності основних кроків формування національної концепції безпеки та стійкості критичної інфраструктури:

1. Встановлення стратегічних цілей та завдань концепції.

2. Аналіз міжнародного досвіду, виявлення прикладів ефективних програм і планів безпеки та стійкості КІ, які можуть бути адаптовані до національного контексту.

3. Визначення перспектив імплементації зазначених практик у розрізі окремих секторів критичної інфраструктури.

4. Ідентифікація основних стейкхолдерів у кожному секторі.

5. Закріплення інституційних ролей та обов'язків відповідальних суб'єктів.

6. Формування механізмів міжвідомчої координації та комунікації між державними інституціями, операторами критичної інфраструктури та іншими заінтересованими сторонами.

7. Розбудова системи управління ризиками, встановлення алгоритмів реагування, створення переліку індикаторів ефективності та проведення їхньої оцінки.

8. Розробка сценаріїв міжсекторальних навчань та тренувань.

9. Визначення часових параметрів реалізації заходів і контроль за їх дотриманням.

10. Пропагування необхідності широкого залучення стейкхолдерів та популяризація засад концепції.

Зазначені кроки формують підґрунтя для побудови ефективної системи реагування, в якій кожен суб'єкт чітко усвідомлює свої функції в умовах загроз.

Доцільно також звернути увагу на досвід Європейського Союзу у сфері реалізації державної політики захисту критичної інфраструктури. У межах Європейської програми захисту критичної інфраструктури (European Programme for Critical Infrastructure Protection – EPCIP) Європейська комісія ініціювала пакет заходів, спрямованих на підвищення захищеності об'єктів критичної інфраструктури держав-членів ЄС. Значним елементом цієї програми є ініціатива з захисту критичної інформаційної інфраструктури (Critical Information Infrastructure Protection – CIP), яка покликана зміцнити безпеку ІКТ-компонентів життєво важливої інфраструктури [293].

У межах реалізації EPCIP було створено Комісію інформаційного попередження про критичну інфраструктуру (CIWIN – Commission of a Critical Infrastructure Warning Information Network), що виконує функції захищеної інформаційно-комунікаційної платформи для обміну даними про спільні загрози, вразливості, заходи реагування та превентивні стратегії серед членів спільноти CIP ЄС. Портал CIWIN функціонує з січня 2013 року, забезпечуючи міждержавну координацію й обмін передовими практиками [149].

Вивчення зарубіжного досвіду дає підстави стверджувати, що спільною характеристикою державної політики у сфері критичної інфраструктури є її орієнтація на досягнення стійкості систем. R. Cantelmi запропонував розглядати стійкість у рамках часової послідовності фаз антикризового управління – «до, під час і після» кризи [289]. Такий підхід дозволяє

трактувати стійкість як багатокомпонентну категорію, що охоплює повний цикл управління кризами.

T. W. Coombs, у свою чергу, виокремлює три основні стадії процесу забезпечення стійкості: докризову, кризову та посткризову. Докризова фаза включає оцінку ризиків, розробку планів, реалізацію профілактичних заходів; кризова – оперативне реагування та управління інцидентами; посткризова – аналіз наслідків, відновлення функціонування та реалізація заходів запобігання майбутнім інцидентам [294, с. 198].

Таким чином, поняття стійкості критичної інфраструктури передбачає не лише здатність протидіяти загрозам, але й адаптуватися до них та ефективно відновлюватися. Варто також визнати, що інциденти на об'єктах критичної інфраструктури неминучі, тому акцент слід робити на розвитку абсорбційної та адаптаційної спроможності систем.

Ключовими інституціями у сфері захисту критичної інфраструктури Німеччини є:

1. Закон про підвищення безпеки систем інформаційних технологій (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme). Федеральний уряд робить внесок у те, щоб IT-системи та цифрові інфраструктури Німеччини стали одними з найбезпечніших, зокрема, у сфері критичної інфраструктури. Закон вимагає, щоб оператори критичних інфраструктур забезпечували належний захист їхніх інформаційних систем від кіберзагроз [358].

2. Закон про Федеральне відомство з інформаційної безпеки (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik – BSI). Закон регулює сферу інформаційної безпеки в Німеччині через Федеральне відомство BSI, що відповідає за захист інформаційних систем державних і некомерційних організацій від кібератак, зломів та інших загроз. BSI займається розробкою стандартів безпеки, проведенням досліджень та аналізу загроз, наданням консультацій та підтримки організацій у сфері інформаційної безпеки [305].

3. Національна стратегія захисту критичної інфраструктури (Nationale Strategie zum Schutz Kritischer Infrastrukturen – NSKR). NSKR стратегія була розроблена з метою забезпечення безпеки та стійкості важливих секторів, таких як енергетика, транспорт, телекомунікації, фінанси та інші, від різних загроз, включаючи кібератаки. Визначає основні принципи та завдання захисту критичних інфраструктур, включаючи електроенергетику, транспорт, телекомунікації та інші сектори. Вона також передбачає регулярну інвентаризацію та класифікацію критичних об'єктів, а також розробку заходів для їх захисту. Вона також встановлює роль та відповідальність різних органів і організацій, які займаються захистом критичних інфраструктур [334].

Важливим у державній політиці Німеччини є урахування міжгалузевого підходу, який стає необхідним там, де внаслідок просторової близькості різних інфраструктурних об'єктів зосередження уваги на окремих галузевих правилах безпеки є недостатньо або може перешкодити виробленню

ефективного управлінського рішення. Однією з інституцій міжгалузевого реагування на небезпеки, тісно пов'язані із захистом критичної інфраструктури, є Стратегія кібербезпеки [299] У ній основна увага приділяється загрозам, що походять від кіберпростору у різних секторах. Також варто відзначити «Стратегію Німеччини щодо адаптації до зміни клімату» [309] у якій велику роль відведено цілому ряду різних явищ зі спектру природних небезпек та заходів відповідної протидії. «Стратегія безпеки вантажних перевезень та логістики» [347] є прикладом галузевого стратегічного документа, який безпосередньо відноситься до захисту критичної інфраструктури та стратегії KRITIS. Вона визначає значимість захисту критично важливих інфраструктур для вантажних перевезень та логістики.

Відповідно до Польської практики, основну роль у розбудові системи захисту критичної інфраструктури відіграє Урядовий центр безпеки (Rządowe Centrum Bezpieczeństwa – RCB) [153]. Урядовий центр безпеки регулює процес запобігання кризовим ситуаціям, а в разі їх виникнення координує заходи з мінімізації їх наслідків. Центр оцінює ризик загроз національній безпеці, уніфікуючи сприйняття загроз окремими міністерствами. Тим самим він підвищує спроможність відповідних служб та органів державного управління справлятися зі складними ситуаціями у секторах критичної інфраструктури. У штат RCB входять цивільні експерти, офіцери та солдати Війська Польського. Основними завданнями RCB є:

– підтримка Урядової Групи Кризового Регулювання (Rządowego Zespołu Zarządzania Kryzysowego – RZZK), яка є міжміністерською консультативною групою, що формує думку та відповідає за ініціювання і координацію кризового управління;

– моніторинг та проведення аналізу загроз на основі даних, отриманих від усіх кризових центрів, що діють у державному управлінні;

– цілодобове чергування, що забезпечує обіг інформації в Національному центрі управління кризами, який у разі загрози запускає процедуру врегулювання, а також приймає та поширює сигнали, що передаються НАТО, ЄС та ООН;

– застереження від загроз та публікація інформації в соціальних мережах (Twitter, Facebook, Instagram) та у ЗМІ;

– нагляд за захистом національної та європейської критичної інфраструктури;

– створення планів, звітів, аналізів та рекомендацій щодо загроз національній безпеці та прогнозів кризових ситуацій;

– створення Національного плану врегулювання кризових ситуацій (Krajowego Planu Zarządzania Kryzysowego), що визначає напрямки цивільного планування на центральному та провінційному рівнях;

– створення звіту про загрози національній безпеці – національна стратегія оцінки ризиків та зменшення ризиків стихійних лих;

– постійне чергування з підвищення обороноздатності держави.

У системі формування державної політики Польщі у сфері захисту критичної інфраструктури ключову роль відіграє Урядовий центр безпеки, який відповідає за підготовку Національної програми захисту критичної інфраструктури (Narodowy Program Ochrony Infrastruktury Krytycznej – NPOIK). Центр здійснює взаємодію з операторами та адміністрацією критичних об'єктів. На основі конфіденційного додатку до NPOIK, який містить чіткі критерії визначення критичної інфраструктури, директор RCB спільно з профільними міністрами, відповідальними за окремі сектори критичної інфраструктури, формує уніфікований перелік об'єктів, установок, пристроїв і послуг, що належать до критичної інфраструктури, з подальшим розподілом за функціональними системами [328].

Важливим елементом механізму управління критичними ситуаціями є Урядова група кризового регулювання (Rządowy Zespół Zarządzania Kryzysowego – RZZK), діяльність якої регламентується ст. 8 Закону «Про управління кризовими ситуаціями» [354]. RZZK виконує функцію державного координатора у сфері кризового реагування, зокрема розробляє і реалізує плани з протидії надзвичайним подіям, у тому числі природного, техногенного та антропогенного характеру. Серед ключових функцій групи варто виокремити:

– координацію дій державних та недержавних організацій під час кризових подій;

– розробку стратегій і процедур превентивного характеру;

– взаємодію з міжнародними партнерами у сфері обміну інформацією та ресурсами;

– інформування громадськості щодо наявних ризиків та рекомендацій.

У контексті практичного застосування NPOIK, особливу увагу заслуговує роль воєвод, які виступають як ключові координатори між централізованими інституціями та територіальними структурами. Відповідно до чинних нормативних положень, на рівні воєводств реалізуються такі функції:

– організація виконання завдань із захисту критичної інфраструктури у межах стратегічного планування регіону;

– збір, обробка та передача інформації про об'єкти критичної інфраструктури до центральних органів влади;

– узгодження планів захисту, які розробляють оператори критичної інфраструктури;

– участь у формуванні регіонального безпекового форуму як інструменту підвищення стійкості критичних об'єктів.

Воєводи забезпечують перехідний рівень між системним і територіальним підходами у сфері забезпечення безпеки критичної інфраструктури. Підпорядковані їм служби, включаючи інспекції та підрозділи охорони, є ключовими суб'єктами підготовки до потенційних дестабілізацій функціонування об'єктів критичної інфраструктури у межах регіону.

Задля досягнення цілей NPOIK воєводи також:

– організовують регіональні форуми захисту критичної інфраструктури, беручи участь у реалізації державної політики відповідно до положень Програми;

– оцінюють регіональні ризики шляхом підготовки Часткового звіту про загрози національній безпеці (Częściowy raport o zagrożeniach bezpieczeństwa narodowego), який слугує аналітичним інструментом для Національного плану врегулювання кризових ситуацій (Krajowy Plan Zarządzania Kryzysowego) [320];

– співпрацюють з органами місцевого самоврядування для реалізації заходів цивільного планування та кризового реагування;

– взаємодіють із операторами критичної інфраструктури та компетентними органами, підтримуючи їхню діяльність і сприяючи реалізації положень NPOIK [328].

Таким чином, польська модель інтеграції між центральним урядом, регіональними інституціями та приватними суб'єктами у сфері критичної інфраструктури формує багаторівневу й адаптивну систему, орієнтовану на стійкість, превенцію та ефективне реагування на загрози.

Комплекс безпекових заходів в межах державної політики охарактеризованих країн корелює із загальноєвропейською інституцією – European Programme for Critical Infrastructure Protection (EPCIP). Даний документ є ініціативою Європейського Союзу, націленою на забезпечення протекції критичної інфраструктури в Європі. EPCIP була започаткована ще у 2006 році, маючи на меті максимізацію рівня безпеки та стійкості критичних інфраструктур. Основні принципи зазначеної Програми включають оцінку ризиків, розуміння загроз, застосування заходів безпеки, міжсекторальну співпрацю та рефлексію між країнами у напрямку модернізації заходів реагування на інциденти та регенерацію роботи після них на об'єктах критичної інфраструктури [293].

Магістральною віссю державної політики у сфері захисту критичної інфраструктури у ЄС є Директива від 8 грудня 2008 року Council directive 2008/114/EC «On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection» (Щодо ідентифікації та позначення європейських критичних інфраструктур та оцінки необхідності покращення їх захисту). Вона встановлює процедуру ідентифікації та маркування європейських об'єктів критичних інфраструктур (ECI) і загальний підхід до оцінки потреб у покращенні їх захисту. Документ передбачає створення Комісії щодо покращення захисту ECI. Директива також зобов'язує власників (операторів) ECI готувати плани безпеки і призначати офіцерів зв'язку з безпекою, що зв'язують власника/оператора з національним органом, відповідальним за захист критичної інфраструктури. Інституція також визначає пріоритетність участі приватного сектору в нагляді та управлінні ризиками, плануванні безпекових заходів та відновленні після надзвичайної ситуації [301].

У системі захисту критичної інфраструктури ЄС існує поняття «Critical Infrastructure Protection Point» (CIP Point), що передбачає точку зв'язку, визначену для обміну інформацією та координації з питань захисту критичної інфраструктури. У тому числі відбувається інформаційний реверс стосовно загроз, ризиків та інцидентів, а також координація спільних дій для запобігання та реагування на події, які можуть загрожувати критичній інфраструктурі. Ці CIP точки використовуються для налаштування партнерства між країнами-членами ЄС, Європейською Комісією та іншими стейкхолдерами у сфері захисту критичної інфраструктури. Органи та структури CIP Points може визначати кожна країна-член ЄС, враховуючи свої особливості та потреби [140, с. 153].

Спільні дії державної політики стійкості, що були описані вище, передбачають наявність стратегічних вказівок, які описують основну філософію дій та досвід вирішення усіх важливих питань щодо безпеки критичної інфраструктури з посиланням на всі відомі ризики. На цій основі можна спроєктувати відповідні підцілі, які, у свою чергу, будуть конкретизовані в концепціях, планах, програмах та віддзеркалюватимуться в них. Зусилля держави у цій сфері мають бути орієнтовані на забезпечення та посилення рівня захищеності критичної інфраструктури за допомогою відповідних заходів, архітектуру яких пропонуємо узагальнити у відповідному квадро-комплексі (рис 3.1).

Рис.3.1. Квадро-комплекс забезпечення стійкості критичної інфраструктури

Джерело:[242, с. 106]

Аналіз досвіду країн Європейського Союзу щодо забезпечення балансу компонентів «трикутника стійкості» критичної інфраструктури дозволяє виокремити ключові принципи, які доцільно враховувати при адаптації зазначеного підходу в державну політику України у сфері забезпечення стійкості об'єктів критичної інфраструктури. Серед основних позицій варто

виділити:

– Аналіз та оцінювання ризиків і загроз – як комплексний процес ідентифікації, класифікації та оцінювання загроз, що потенційно впливають на функціонування критично важливих об’єктів і систем. Це є передумовою для забезпечення надійності та стійкості функціонування інфраструктури в умовах зовнішнього та внутрішнього тиску.

– Превентивність – орієнтована на своєчасне реагування на виявлені ризики через впровадження профілактичних заходів, що дозволяють мінімізувати ймовірність виникнення критичних збоїв та підвищити рівень загальної захищеності систем.

– Імплементація – полягає у втіленні ефективних управлінських рішень у межах системи кризового реагування, спрямованих на мінімізацію наслідків надзвичайних ситуацій та оптимізацію управління під час кризових подій.

– Апроксимація досвіду – передбачає залучення найкращих практик на основі аналізу реальних інцидентів, які відбулися як у межах країни, так і за її межами, з метою стандартизації підходів до захисту та формування актуальних вимог до операторів об’єктів критичної інфраструктури у співпраці з міжнародними партнерами [242, с. 107].

Послідовна реалізація зазначеного чотирикомпонентного підходу формує ефективний цикл управління ризиками, який забезпечує сталу дієвість системи захисту та підвищує інституційну спроможність держави у сфері безпеки критичної інфраструктури (рис. 3.2).

Рис. 3.2. Модель забезпечення стійкості критичної інфраструктури
Джерело: узагальнено автором на основі [185],[343]

У межах даного підходу стійкість КІ набуває комплексного виміру, що включає такі ключові функціональні елементи:

1. Прогнозування потенційних порушень – необхідне для здійснення системного планування, превентивної підготовки та оцінки вразливостей.

2. Поглинання впливу – здатність системи витримувати тиск або адаптуватися до несподіваних викликів без втрати функціональності.

3. Адаптація – забезпечення безперервності функціонування або надання послуг в умовах зміненого середовища.

4. Відновлення – спроможність системи до швидкого повернення до нормального стану після виникнення серйозних порушень.

У контексті європейської практики стійкість критичної інфраструктури визначається через три головні характеристики:

– Надійність – здатність зберігати працездатність в умовах надзвичайних ситуацій за рахунок інженерної стійкості, резервних систем та інших технічних рішень.

– Винахідливість – включає ефективну підготовку до кризових ситуацій, зокрема через навчання, управління безперервністю діяльності, контроль ланцюгів постачання тощо.

– Оперативне відновлення – швидке реагування та повернення до нормальної роботи, що реалізується через реалізацію планів екстрених заходів, негайної мобілізації ресурсів і координації дій [242, с. 109].

Таким чином, формування державної політики у сфері забезпечення стійкості критичної інфраструктури має ґрунтуватися на цілісному циклі управління ризиками, який поєднує превенцію, адаптацію, інституційну винахідливість і оперативну реакцію на загрози [242, с. 109].

На підставі проведеного аналізу зарубіжного досвіду інституційно-правових підходів до реалізації державної політики у сфері захисту критичної інфраструктури в контексті забезпечення її стійкості, а також спираючись на наявні дослідження, можна виокремити такі характерні риси:

– У більшості держав-членів Європейського Союзу спостерігається недостатня концептуальна та термінологічна уніфікація у сфері визначення поняття «критична інфраструктура» в базових політичних і нормативних документах.

– Лише частина країн має чітко ратифіковані закони про критичну інфраструктуру; інші ж не здійснюють офіційної ідентифікації таких об’єктів, що обмежує формування національної політики у напрямі зміцнення стійкості та інклюзивності.

– У більшості випадків питання функціонування критичної інфраструктури інтегруються в чинні нормативно-правові та планово-управлінські документи на національному рівні.

– Національні органи управління з надзвичайних ситуацій відіграють провідну роль у забезпеченні безпеки критичної інфраструктури, координуючи діяльність інших суб’єктів управління – як на центральному,

так і на місцевому рівнях – під час комплексних кризових ситуацій міжсекторального характеру.

– Увага до критичних об'єктів значною мірою зумовлюється змінами в інвестиційній політиці окремих країн, де критична інфраструктура визнається стратегічно важливою для національної безпеки.

– Більшість держав ЄС впроваджують національні програми захисту критичної інфраструктури, розробляють механізми ідентифікації, прогнозують потенційні наслідки дестабілізації інфраструктури та здійснюють оцінку джерел ризиків.

– Впровадження державних стратегій управління ризиками щодо критичної інфраструктури базується на чотирьох фундаментальних етапах: запобігання, готовність, реагування та відновлення.

– Політика у сфері критичної інфраструктури дедалі більше орієнтується на активізацію інвестиційної діяльності, забезпечуючи баланс між державними структурами, приватними операторами та іноземними бізнес-інституціями для посилення загальної стійкості.

– Особливе значення надається чіткому визначенню стейкхолдерів у приватному секторі та побудові ефективної моделі державно-приватного партнерства, включаючи елементи кластеризації.

– Значна увага приділяється розвитку освітніх ініціатив та підготовці фахівців у сфері захисту критичної інфраструктури.

– Посилюється взаємодія між безпековими акторами шляхом налагодження механізмів обміну інформацією, формування банків знань, а також захисту інформаційних активів операторів інфраструктури, зокрема у сфері кібербезпеки.

– Розробка програм стійкості критичної інфраструктури передбачає чітке визначення цілей і завдань на всіх рівнях управління (національному, регіональному, місцевому, галузевому), орієнтуючись на культурно-політичні особливості та чинну нормативну базу [311].

У межах концептуального узагальнення результатів дослідження доцільно окреслити такі стратегічні напрями розвитку державної політики України у сфері підвищення стійкості критичної інфраструктури як на національному, так і на регіональному рівнях:

– Удосконалення інституційно-правової бази шляхом гармонізації із міжнародними стандартами та включення уніфікованих норм до національних стратегічних документів.

– Формування кадрового потенціалу, орієнтованого на розвиток професійних компетентностей у представників органів державної влади, операторів критичної інфраструктури, експертного середовища та громадськості.

– Актуалізація секторної структури критичної інфраструктури на основі порівняльного аналізу світового досвіду, наукових досліджень та стратегічних викликів національного рівня.

– Інтегроване управління ризиками, що включає моделювання сценаріїв

загроз, оперативне планування та визначення чітких алгоритмів реагування й відновлення у разі криз.

– Розбудова міжсекторальної взаємодії, включаючи розвиток державно-приватного партнерства між стейкхолдерами усіх рівнів.

– Посилення ресурсного забезпечення, що охоплює не лише фінансові інструменти, але й інституційну та технічну спроможність суб'єктів забезпечення безпеки критичної інфраструктури.

Отже, на основі узагальнення зарубіжного досвіду реалізації державної політики у сфері захисту критичної інфраструктури встановлено, що провідні країни світу застосовують системні підходи до забезпечення її стійкості. Основні акценти зроблено на інтегрованому управлінні ризиками, міжсекторальній взаємодії, державно-приватному партнерстві, розвитку організаційної, соціальної та технологічної стійкості. Визначено необхідність адаптації цих практик в Україні з урахуванням національного контексту, зокрема через удосконалення нормативно-правової бази, кадрове забезпечення, стратегічне планування, кіберзахист і комунікаційні механізми між стейкхолдерами. Запропонований підхід формує концептуальну основу для формування цілісної, адаптивної та прогнозованої системи управління критичною інфраструктурою в умовах сучасних безпекових викликів.

3.2. Інституційні перетворення у напрямку підвищення ефективності державної політики захисту критичної інфраструктури

Як зазначалося вище, провідною тенденцією у підходах розвинених країн до захисту об'єктів критичної інфраструктури є актуалізація категорії «стійкості» як ключового елементу державної політики у безпековій сфері. В умовах глобальних трансформацій у сфері безпеки та з огляду на євроінтеграційний вектор розвитку України, дифузія цієї концепції в національну політику слугує системоутворюючим тригером у процесі зміцнення захищеності критичної інфраструктури.

Етимологічно поняття «стійкість» походить від латинського resilio, resilire, що означає «відновлення» або «здатність повертатися до початкового стану» [318, с. 291]. Виходячи з цього, можна стверджувати, що пріоритетними об'єктами державної політики у сфері стійкості є саме пошкоджені або дестабілізовані елементи критичної інфраструктури. Її стійкість полягає у здатності операторів об'єктів адаптуватися до змін у безпековому середовищі, підтримувати функціональність у кризових умовах і швидко відновлюватися після інцидентів. Зростаючу увагу до цієї проблематики засвідчує факт, що кількість наукових досліджень, присвячених питанням стійкості, вже перевищує кількість робіт, орієнтованих виключно на захист об'єктів критичної інфраструктури [242, с. 105].

Іноземні дослідники також підтримують тезу про необхідність колективної відповідальності за формування національної стратегії безпеки як базової умови для підвищення загальної стійкості держави. У цьому контексті науковці закликають до ширшого залучення інституцій поза межами відповідних міністерств, визнаючи важливість їх участі у формуванні й реалізації стратегічних заходів із підвищення стійкості критичної інфраструктури [1, с. 112; 95, с. 25].

Відповідно, всі суб'єкти державного управління, що беруть участь у реалізації політики захисту критичної інфраструктури, мають взаємодіяти у сфері ризик-аналізу та загроз з розширеним колом інституцій, відповідальних за прогнозування, запобігання, реагування та відновлення в умовах надзвичайних ситуацій.

Кожен інституційний суб'єкт, який розробляє та реалізує політику у сфері безпеки критичної інфраструктури, повинен мати чітке уявлення про спектр можливих ризиків і загроз, які стосуються підвідомчих йому об'єктів, а також володіти відповідними ресурсами та інструментами для реалізації захисних заходів.

Погоджуючись із висновками Д. С. Бірюкова та С. І. Кондратова [9, с. 109], слід наголосити, що практична імплементація заходів у сфері безпеки повинна спиратися на глибоке наукове опрацювання проблеми. До числа ключових елементів інституційних перетворень дослідники пропонують включити:

– секторальну диференціацію об'єктів критичної інфраструктури на національному, регіональному та місцевому рівнях;

– комплексну ідентифікацію загроз та ризиків у межах кожного окремого сектора критичної інфраструктури;

– оцінку ступеня вразливості секторів до специфічних загроз із урахуванням контексту;

– виявлення потенційних наслідків дестабілізації або знищення окремих компонентів критичної інфраструктури;

– розробку превентивних заходів на основі моделі функціонування національної системи захисту критичної інфраструктури.

Таким чином, адаптація концепції стійкості як ключової парадигми у сфері національної безпеки передбачає не лише оновлення нормативно-правової бази, але й трансформацію інституційної архітектури, що забезпечує динамічну, адаптивну й інклюзивну модель управління ризиками та загрозами в інфраструктурному секторі.

Узагальнюючи, можна стверджувати, що в основі розглянутих підходів до захисту критичної інфраструктури лежить реалізація заходів стратегічного планування державними інституціями з метою мінімізації відомих ризиків та запобігання виникненню нових загроз. Результатом цього процесу мають стати управлінські рішення на національному, регіональному та місцевому рівнях, спрямовані на впровадження комплексу заходів з ідентифікації потенційних ризиків, удосконалення інституційно-правових механізмів

управління ризиками і загрозами, інвестування в підвищення ефективності оперативного реагування, а також забезпечення швидкого відновлення функціонування об'єктів критичної інфраструктури після надзвичайних ситуацій [282, с. 78].

Показовим у цьому контексті є досвід Сполучених Штатів Америки. Так, у Національному плані захисту інфраструктури (National Infrastructure Protection Plan, NIPP) 2013 року зазначено, що «національні зусилля щодо посилення безпеки та стійкості критичної інфраструктури залежать від здатності її власників і операторів у державному та приватному секторах приймати обґрунтовані рішення з урахуванням ризиків та обмежених ресурсів як у стабільних умовах, так і в умовах кризи». Аналізуючи інституційні трансформації державної політики США у сфері захисту критичної інфраструктури, варто підкреслити її поліінституціональний характер. Цей феномен пояснюється активною залученістю до формування та реалізації політики безпеки приватного сектору, власників і операторів об'єктів критичної інфраструктури, урядових органів, органів місцевого самоврядування, неурядових організацій, секторальних агентств, федеральних департаментів і наукових установ [329].

Основною метою такого підходу є стимулювання інновацій у сфері розробки безпечних і стійких технологій, а також підвищення ефективності та узгодженості реалізації програм на всіх рівнях управління. Це, у свою чергу, сприяє зниженню рівня ризиків і загроз, а також активізації залучення приватних інвестицій у сферу захисту критичної інфраструктури. Такий вектор інституційних змін є особливо актуальним з огляду на трансформацію глобального геополітичного та безпекового середовища, у якому загрози постійно ускладнюються, посилюються та масштабуються.

У країнах Європейського Союзу спостерігається перехід від парадигми захисту до парадигми резильєнтності, що чітко відображено у спеціалізованих публікаціях NIST [335], дослідженнях MITRE [325] та у стандартах ISO [317]. Ця тенденція також знайшла відображення в новітніх директивах Ради ЄС, що визначають сучасні пріоритети у сфері безпеки критичної інфраструктури. Згідно з аналізом С. І. Пирожкова та Н. В. Хамітова, поняття «резильєнтність» ототожнюється з життєстійкістю та здатністю до відновлення [186, с. 48]. Зважаючи на міжнародну практику, у контексті забезпечення безпеки об'єктів критичної інфраструктури доцільно застосовувати саме поняття «резильєнтність критичної інфраструктури», яке в науковій літературі розглядається як здатність суб'єктів міжнародних відносин протидіяти гібридним загрозам.

Таким чином, резильєнтність критичної інфраструктури доцільно визначити як здатність та готовність держави, суспільства й органів публічної влади реалізовувати ефективний комплекс заходів, спрямованих на забезпечення готовності до надзвичайних ситуацій, запобігання їх виникненню, протидію ризикам та загрозам, швидке відновлення нормального функціонування інфраструктурних об'єктів після кризових

подій, а також постійне підвищення компетентностей персоналу, засвоєння досвіду та залучення приватного капіталу. Такий підхід передбачає активну участь не лише урядових структур, а й усіх ключових стейкхолдерів сфери критичної інфраструктури.

Ще одним із напрямків інституційних перетворень для забезпечення резильєнтності критичної інфраструктури з метою розвитку можливостей ефективно протистояти ризикам, варто розглянути перспективи проведення комплексного їх аналізу. Відзначимо, що ризик-аналіз в окремих країнах став важливим складником системи забезпечення національної безпеки та публікується у формі окремого документа – «Національної оцінки ризиків» (National Risk Assessment – NRA). Починаючи з першого десятиліття 2000-х років, уряди окремих країн, що входять до Організації економічного співробітництва та розвитку (OECD), почали розробляти портфельний аналіз «всіх небезпек», з якими стикається їхня національна безпека, які, врешті-решт, можуть призвести до масштабних надзвичайних ситуацій, у тому числі і на об'єктах критичної інфраструктури [330]. Мотиви даної ініціативи можемо відзначити:

– у потребі систематизації та ідентифікації ризиків, за допомогою якого можна заповнити сліпі зони у захисті критичної інфраструктури;

– у необхідності комплексної готовності до різних типів ризиків відповідно до загального набору критеріїв;

– у необхідності досягнення консенсусу між секторальними органами захисту критичної інфраструктури та інвесторами щодо пріоритетів інвестування у заходах з управління ризиками;

– у необхідності краще зрозуміти зв'язки між різними типами ризиків, з метою розробки міжсекторальних планів протидії ризикам та ліквідації наслідків.

У контексті інституційної трансформації в Україні доцільним є забезпечення системного процесу визначення та аналізу спектру ризиків, з якими стикається держава у сфері функціонування критичної інфраструктури. Ефективним прикладом використання відповідного інструментарію є досвід Великої Британії, де уряд щорічно готує Національну оцінку ризиків (National Risk Assessment). Ця ініціатива включає реалізацію ключових елементів системи стійкості: прогнозування (готовність), формування реєстру ризиків (протистояння), а також оцінку ризиків (запобігання) [176].

Подібний підхід застосовується і в США, де ризики для критичної інфраструктури аналізуються з урахуванням вразливостей, загроз та можливих наслідків. При цьому використовуються експертні оцінки, що базуються на 5-бальній або, в окремих випадках, 3-бальній шкалі – від мінімального до катастрофічного рівня [305, с. 260].

Різнорідність об'єктів критичної інфраструктури, що належать до різних галузей, підкреслює складність та багатовимірність проблематики аналізу ризиків у сфері безпеки. Особливою рисою критичного ризик-аналізу є

орієнтація на оцінку потенційно шкодочинних наслідків, які можуть виникнути внаслідок технічних збоїв, дестабілізації технологічних систем або помилок персоналу об'єкта.

З огляду на це, особливу увагу слід приділити складовій управління критичними ризиками як одній із ключових компонент державної політики у сфері забезпечення безпеки та резильєнтності критичної інфраструктури. Варто також розглядати цю проблему в контексті адміністрування як сфери компетенції органів державної влади.

У цьому аспекті доцільно звернутися до фундаментального дослідження О. Я. Лазора та О. Д. Лазор [109, с. 116], які визначають процес адміністрування як консультативно-дорадчу та організаційно-розпорядчу діяльність органів державної влади. Таким чином, адміністрування в межах державного управління слід трактувати з урахуванням підпорядкованості законам, узгодженості інтересів усіх учасників процесу та відповідальності за стан керованих систем. Розширене тлумачення цієї категорії пропонує В. В. Овчарук [138, с. 116], розглядаючи адміністрування як управлінську діяльність, функцію менеджменту, вид менеджменту або стиль управління.

Отже, дійдемо висновку, що процес управління критичними ризиками слід проводити із позиції синхронізації публічного адміністрування та менеджменту. Доречним у даному випадку вважаємо розширення структури державної політики у сфері захисту та резильєнтності критичної інфраструктури предикатом «критичний ризик-менеджмент». Це дозволить посилити складову захисту як державних критичних об'єктів, так і приватних. Слушним у даному розумінні вважаємо позицію вчених В. О. Мусієнка та М. Е. Зінченка, які тлумачать поняття ризик-менеджмент як «процес прийняття та виконання управлінських рішень, спрямованих на зменшення ступеня ймовірності виникнення результату несприятливого характеру та мінімізацію можливих втрат, які викликані його реалізацією» [118, с. 103]. Доцільно трактувати систему критичного ризик-менеджменту в межах забезпечення резильєнтності критичної інфраструктури як частину системного підходу до прийняття управлінських рішень [88, с. 55]. Отже, вважаємо доцільним сприймати критичний ризик-менеджмент як спектр процедур і практичних заходів, націлених на вирішенні завдань з профілактики і зниження рівня потенційних ризиків та загроз виникнення критичних ситуацій, що загрожують стійкості функціонування об'єктів критичної інфраструктури, зниження потенційних втрат та інших негативних наслідків. По суті, мова йде про застосування превентивних заходів для унеможливлення виникнення надзвичайних ситуацій на життєво-важливих об'єктах та планові заходи щодо мінімізації та ліквідації негативних наслідків за умов їх виникнення. Оскільки, як зазначалося вище, управління ризиками у структурі державно політики захисту критичної інфраструктури відбувається в умовах неясності, в основі варто розглядати методи

прогнозування і соціальний та технічний аналіз під час оцінки ризику (рис 3.3.). Відповідно до схеми, зазначимо, що захист критичної інфраструктури має базуватися на механізмах державного управління та оцінці критичних ризиків. Аналіз ризику та вразливості є основними методами та важливими інструментами для проведення проактивного та ефективного управління безпекою [327, с. 455].

Середовище державного управління, спрямоване на створення ефективної системи захисту критичної інфраструктури, повинно містити структурований модуль ризик-менеджменту. Цей модуль має базуватися на розробці та аналізі альтернатив управлінських рішень із використанням результатів оцінки ризиків, їх аналізу та прогнозування можливих наслідків з метою їхньої мінімізації.

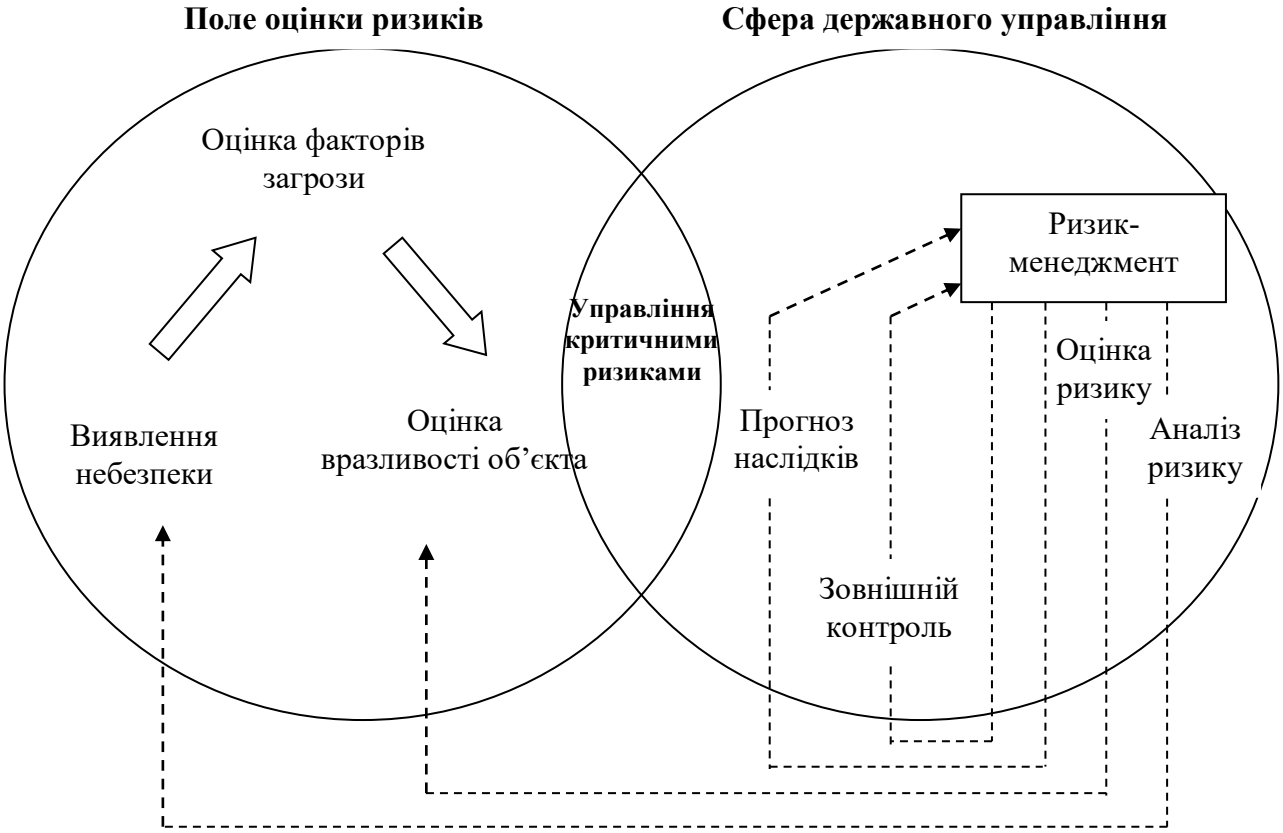


Рис. 3.3. Алгоритм забезпечення критичного ризик-менеджменту як складової державної політики резильєнтності критичної інфраструктури

Джерело: розроблено автором [282, с. 79]

Зазначений процес передбачає реалізацію багатокритеріальних задач, що передують ухваленню рішень в умовах невизначеності. Оцінка ризиків виступає ключовим етапом у розробці заходів ризик-менеджменту і здійснюється згідно з алгоритмом, який охоплює виявлення небезпек, аналіз загроз та оцінку вразливості критичних об'єктів. Це, своєю чергою, вимагає

створення допоміжного алгоритму, який би дозволяв моделювати можливі сценарії надзвичайних ситуацій і забезпечував здатність керівництва та персоналу об'єктів критичної інфраструктури своєчасно адаптуватися до таких обставин у реальному середовищі. Отже, інтеграція ризик-менеджменту в архітектуру державної політики сприятиме формуванню дієвого механізму управління загрозами, їх ідентифікації та прогнозування на об'єктах критичної інфраструктури.

Для просторово-часової характеристики алгоритму виникнення ризикової ситуації на критично важливому об'єкті доцільно використати наукові напрацювання В. В. Вітлінського та Г. І. Великоіваненка [225, с. 345], які пропонують спиратися на такі ключові критерії:

– чітке визначення загроз, які можуть зумовити ризикову ситуацію;
– ймовірність виникнення такої ситуації;
– рівень зменшення деструктивних наслідків після її настання.

Зазначений підхід узгоджується з логікою наукового дослідження проблеми захисту критичної інфраструктури через призму адміністративно-правового регулювання в умовах невизначеності.

Доречно також врахувати позицію учених О. Є. Кузьміна, М. Є. Адаміва та О. Г. Мельника [103, с. 75], які підкреслюють, що в умовах зростання дефіциту інформаційно-часових ресурсів, що супроводжує ухвалення управлінських рішень, зростає ймовірність їх неадекватного тлумачення. Це, у свою чергу, призводить до латентності рішень, які приймаються в системі управління критичною інфраструктурою.

Виходом з такої ситуації науковці вважають впровадження антисипативного управління, орієнтованого на прогнозування потенційних ризиків як внутрішнього, так і зовнішнього середовища. Невизначеність, притаманна результатам управлінських рішень, зумовлює необхідність прогнозування їхніх наслідків, що може реалізовуватись через імовірнісні моделі на основі методів теорії розпливчастих множин, які не підлягають суворій формалізації та мають логіко-аналітичний характер.

У цьому контексті критичний ризик-менеджмент може розглядатися як сфера застосування інструментарію нечіткої логіки. Спираючись на дослідження С. В. Козловського [92, с. 350], С. А. Олизаренка, А. В. Перепелиці та В. А. Капранова [139, с. 42], можна стверджувати, що саме для розв'язання подібних управлінських задач доцільно застосовувати методи структурування знань, моделювання управлінських рішень та когнітивного аналізу із використанням засобів інженерії наукових знань і штучного інтелекту.

Загальна методика моделювання на основі нечіткої логіки, акомодована під умови забезпечення безпеки критичної інфраструктури, має передбачати поетапне розв'язання таких задач: препарація основних детермінант впливу на критичну інфраструктуру та інтеракції між ними; визначення і

формалізацію лінгвістичних оцінок факторів; побудову нечіткої бази знань про взаємозв'язки між факторами [115, с. 201]. Прислухаємось до І. Г. Фадєєвої та ін.. [273, с. 215], котрі пропонують декілька алгоритмів систем нечіткого умовиводу, опис яких заснований на поділі вихідного процесу на ряд послідовних етапів:

1. Формування бази даних правил нечіткого висновку системи.
2. Фазифікація вхідних змінних.
3. Агрегація підумов у нечітких умовах правил дії.
4. Активізація або композиція підвисновків в правила нечіткі умови-дія.
5. Накопичення висновків нечіткої умови правила дії.
6. Дефазифікація вихідних змінних.

Отже, при формуванні алгоритму, оператор критичного об'єкту буде аналізувати поточну ситуацію, порівнюючи її з раніше розробленими шаблонами критеріальних факторів, які є ознаками надзвичайної ситуації. Відповідно, описану алгоритмізацію нечітких висновків у межах кризового ризик-менеджменту можна застосовувати у ситуаціях, відносно стабільних та у вузький проміжок часу при мінімальному об'ємі ситуаційної інформації, а формалізовані алгоритмічні узагальнення підходять для прийняття екстрених управлінських рішень на об'єктах критичної інфраструктури, що робить даний процес актуальним в умовах війни [282, с. 75].

У контексті інституційних трансформацій ключовим напрямом вважаємо розробку узагальнених критеріїв та алгоритмів для оцінки резильєнтності. Цей напрям є актуальним кроком до трансформації феномену резильєнтності в прикладні інструменти управління у сфері захисту критичної інфраструктури.

Іноземні дослідники Yang Z. та Barroca B. [356] оцінюють потенціал резильєнтності критичної інфраструктури на основі здатності чотирьох взаємопов'язаних підсистем країни (так званого квадро-комплексу):

– соціально-економічної системи;
– державних інституцій;
– науково-освітньої складової;
– техніко-інфраструктурної системи.

Зазначені компоненти є потенційно важливими для ефективної реалізації державної політики у сфері захисту об'єктів критичної інфраструктури. У цьому контексті поняття резильєнтності розкривається через взаємозв'язок двох базових категорій: «наслідків» та «дії», які, в залежності від конкретної ситуації, можуть інтерпретуватися як витрати, вигоди, збитки або побічні ефекти. Їх обов'язково слід враховувати у процесі прийняття рішень при управлінні інцидентами або кризовими ситуаціями на об'єктах критичної інфраструктури.

Концептуальний сценарій резильєнтності об'єкта критичної інфраструктури доцільно представити у вигляді діаграми (рис. 3.4), яка

відображає дуальність резильєнтності – «наслідок» ↔ «дія».

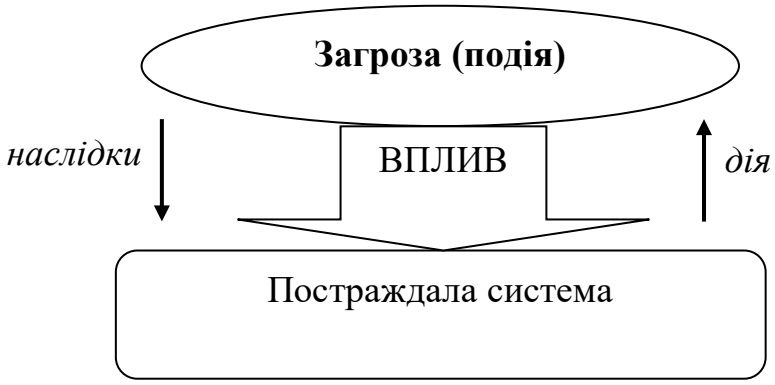


Рис. 3.4. Концептуальний сценарій резильєнтності об’єктів критичної інфраструктури

Джерело: розроблено авторами

Цей сценарій ілюструє алгоритм «як загроза впливає на систему» та акцентує увагу на двох ключових умовах:

1. Подія (загроза) призводить до виникнення деструктивних наслідків у системі або її окремих компонентах.

2. Система відповідає на загрозу шляхом реалізації комплексу заходів: протидії, сприйняття, адаптації, трансформації, відновлення та навчання.

Слушною у продовжені даного вектору дослідження вважаємо також теорію норвезьких вчених K.Øien та L.Bodsberg [346, с. 17] у якій вони виділяють чотири ключові атрибути «дії» у напрямку досягнення резильєнтності об’єктів критичних інфраструктур – «аналіз ризиків/загроз», «передбачення/підготовка», «проходження/витримка», «реагування/ відновлення» та «адаптація/навчання». Учені також підтверджують запропоновану вище тезу, щодо інтеграції до концептуального сценарію резильєнтності ризик-менеджменту, заснованого на наслідках дій, метою виконання яких є мінімізація їх деструктивного впливу. Відповідно, оцінка наслідків може бути використана для обґрунтування дій. Наслідки певного сценарію досягнення резильєнтності можуть бути використані як досвід для покращення потенційних дій. Крім того, ефективність окремих дій можна оцінити за рівнем зменшення наслідків майбутніх сценаріїв резильєнтності. Отже, оцінка наслідків дій є ірраціональним і безперервним процесом.

Виходячи із описаних вище ключових атрибутів резильєнтності об’єктів критичних інфраструктур, трансформування інституційних систем їх захисту варто розглядати крізь призму ресурсних системних детермінант, серед яких можемо виділити фізичний захист і оборону, кіберзахист і оборону, превентивні заходи захисту й оборони та освітньо-науковий підхід (рис. 3.5).

Структурно-логічна схема забезпечення резильєнтності критичної інфраструктури в межах реалізації державної політики передбачає деталізацію поетапної реалізації дій, спрямованих на забезпечення

безперервності функціонування об’єктів критичної інфраструктури та їх здатності до адаптації в умовах загроз.

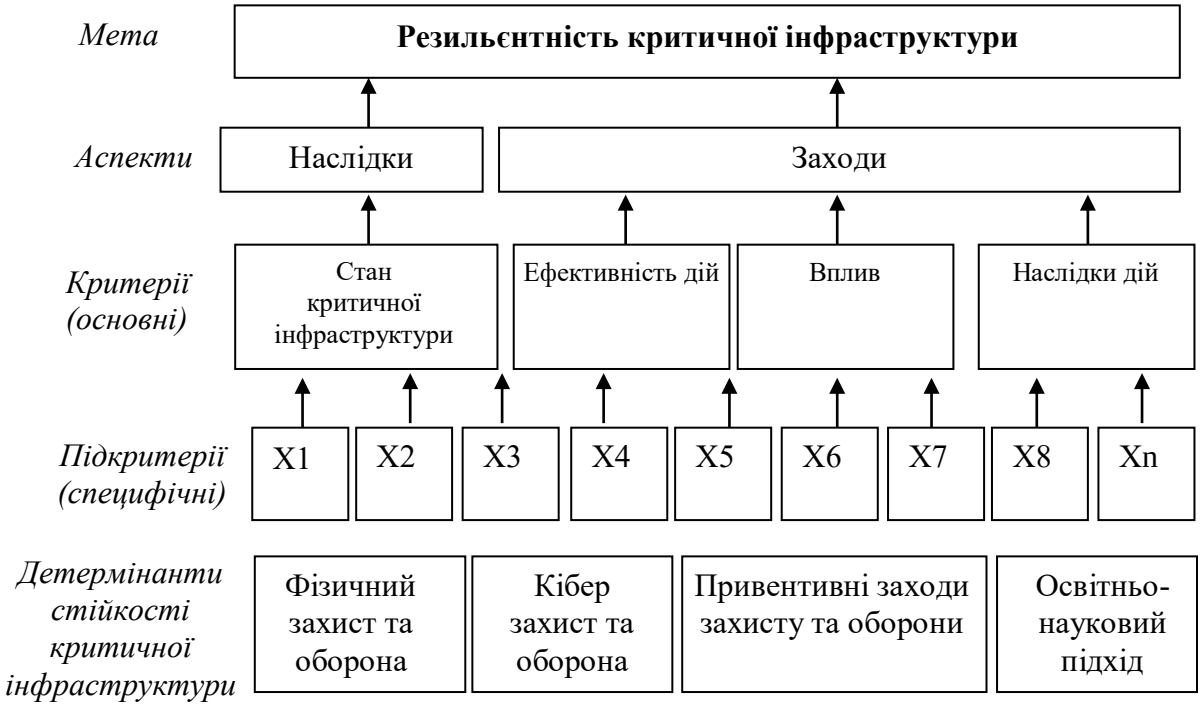


Рис. 3.5. Структурно-логічна схема забезпечення стійкості критичної інфраструктури в межах реалізації державої політики

Джерело: розроблено авторами

Цей процес умовно можна поділити на п’ять етапів:

1. Етап оцінки можливих подій – передбачає системний аналіз ризиків і загроз, з якими може зіткнутися об’єкт критичної інфраструктури. На цьому етапі акцент робиться на діях, що посилюють готовність системи до потенційних небезпек.

2. Етап перед подією – охоплює часовий проміжок від моменту появи ознак загрози до початку надзвичайної ситуації або деструкції. Основними діями на цьому етапі є передбачення, підготовка та запобігання.

3. Етап протягом події – триває з моменту початку деструкції до досягнення нею максимального впливу. На цьому етапі реалізуються заходи з подолання, витримки та протистояння негативному впливу на систему.

4. Етап після події – розпочинається після досягнення піку деструктивного впливу та триває до моменту повного або часткового відновлення функціональності об’єкта. Здійснюються дії реагування на кризу та відновлення роботи системи.

5. Етап підготовки до наступної події – охоплює період після відновлення функціональності до появи нової потенційної загрози. На цьому етапі система має продемонструвати здатність до адаптації, навчання та вдосконалення, що ґрунтується на попередньому досвіді.

У контексті надзвичайних ситуацій, терористичних загроз та збройних

конфліктів ефективне забезпечення резильєнтності критичної інфраструктури є неможливим без чіткої взаємодії та розподілу функцій між суб'єктами державної політики. Ці функції повинні бути інституційно закріплені й реалізовані управлінськими структурами публічної влади.

Як було показано в попередніх розділах, погоджуємось із позицією вчених С. І. Кондратова та О. М. Суходолі [95, с. 26], які вказують на недостатню координацію між відомствами, відповідальними за захист критичних об'єктів. Відповідальність за їх безпеку покладається на різні міністерства та служби, кожне з яких функціонує у власному галузевому контексті, із притаманними йому наборами ризиків, планами реагування, термінологією та процедурами.

Водночас, слабкість міжвідомчої комунікації й низька ефективність існуючих процедур взаємодії між національними системами безпеки та кризового реагування в умовах масштабних інцидентів пояснюється, зокрема, недостатньо розвиненою практикою міжвідомчих навчань та відсутністю єдиної методичної бази [244, с. 115]. Отже, дана проблема потребує адекватної відповіді у вигляді управлінського рішення по створенню певних міжсекторальних осередків захисту, які б опікувалися безпекою конкретних об'єктів критичної інфраструктури. Для цього важливо регламентувати градацію розподілу відповідальності за типами проєктних загроз (рис.3.6).

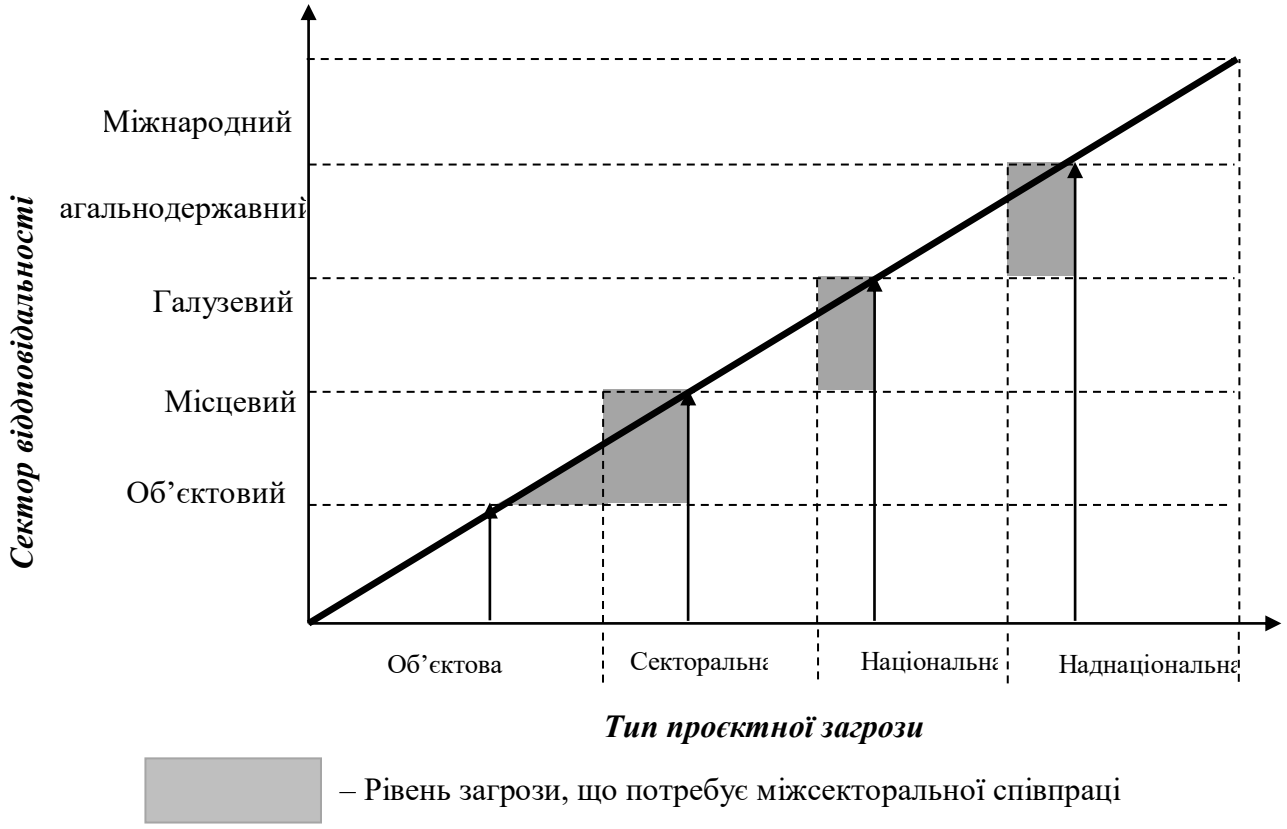


Рис. 3.6. Розподіл відповідальності за типами проєктної загрози
Джерело: узагальнено автором на основі [60], [289]

Варто розмежувати рівень загроз на об'єктові, секторальні, національні та наднаціональні. Відповідно до проєктних загроз потребує розмежування сфери їх відповідальності за наступними секторами:

I. Міжнародний рівень – посилювати координацію з НАТО, діалогу та співпраці між Єврокомісією, Центром координації реагування на надзвичайні ситуації (ERCC), Агентства Європейського Союзу зі співробітництва правоохоронних органів (EUROPOL), Європейського центру компетенції з кібербезпеки (ECCC) застосування механізму «раннього попередження» (UCPM) та ін.

II. Загальнодержавний рівень – реалізується Кабінетом Міністрів України, Національним банком України, органами державної влади згідно розподілу повноважень уповноваженим органом у сфері захисту критичної інфраструктури та іншими державними та центральними органами виконавчої влади.

III. Регіональний та галузевий рівні – здійснюється центральними та місцевими органами виконавчої влади, яких призначено відповідальними за формування й реалізацію державної політики у сфері захисту об'єктів критичної інфраструктури.

IV. Місцевий рівень – координується органами місцевого самоврядування, місцевими органами виконавчої влади, а в умовах воєнного стану – військово-цивільними адміністраціями в межах повноважень.

V. Об'єктовий рівень – здійснюється безпосередньо операторами критичної інфраструктури.

В межах інституційних перетворень у напрямку посилення резильєнтності критичної інфраструктури на основі розмежування відповідальності за проєктні загрози, вважаємо за доцільне, посилити на державному рівні активність у забезпеченні проведення регулярних міжсекторальних тренувань і навчань з оперативного реагування на кризові ситуації на критичних об'єктах з метою посилення рівня міжвідомчої комунікації для превенції загроз. Доцільно проводити дані заходи із обов'язковим залученням представників Національної гвардії, СБУ, Державної прикордонної служби, Національної поліції, ЗСУ, Держслужби з надзвичайних ситуацій, а також представників органів виконавчої влади та місцевого самоврядування, Департаментів цивільного захисту і операторів об'єктів критичної інфраструктури. Дану пропозицію можна віднести до категорії антикризових превентивних заходів державного управління у сфері захисту життєво-важливих об'єктів критичної інфраструктури.

Зобразимо основні положення зазначених міжсекторальних навчань у формі імітаційної моделі навчального сценарію превентивного захисту об'єктів критичної інфраструктури (рис. 3.7).

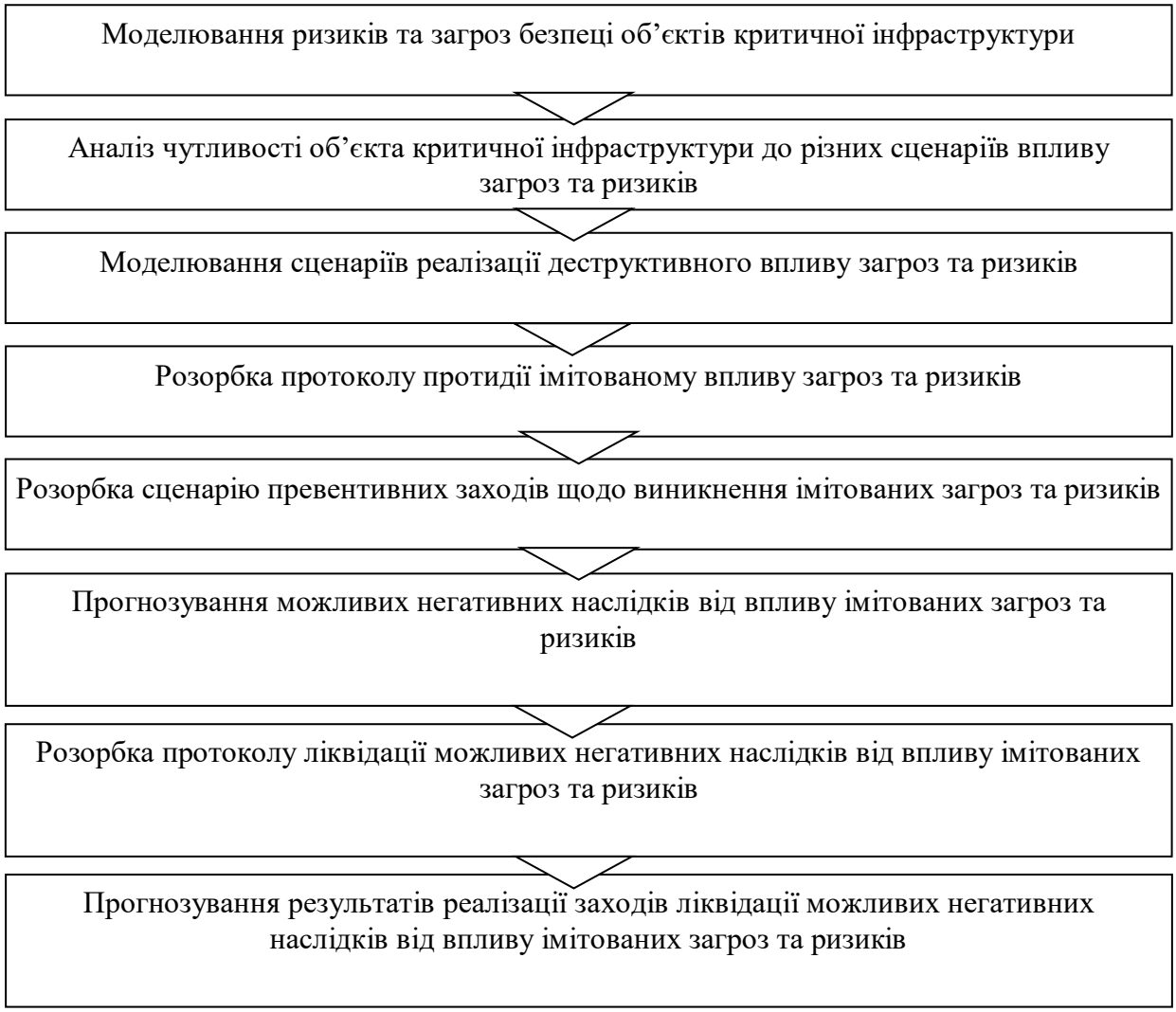


Рис. 3.7. Імітаційна модель навчального сценарію міжсекторальних навчань із превентивного захисту об’єктів критичної інфраструктури
Джерело: узагальнено авторами

Дану пропозицію підтримує Г. І. Зубко [83], пропонуючи деталізацію описаного навчального сценарію та включити до нього:

– диференціація навчальних заходів, інструментів та інформації за основними модулями: універсальним (базові знання для усіх секторів критичної інфраструктури), спеціальним (профільне навчання для кожного сектора або об’єкта) та цифровізованого;

– загальний модуль необхідно наповнити курсами націленими на навчання громадськості, суспільства та відповідних стейкхолдерів з метою підвищення рівня їх компетентностей із основних питань цивільного захисту та превентивних дій стосовно загроз та ризиків критичній інфраструктурі загального характеру;

– спеціальний модуль для кожного сегменту критичної інфраструктури направлено на структурування навчальних заходів із підвищення кваліфікації основних суб’єктів процесу захисту критичної інфраструктури, відповідних

державних службовців, секторальних та функціональних органів, власників та операторів критичної інфраструктури;

– модуль цифровізованого навчання, передбачає формування компетенцій у суб'єктів захисту критичної інфраструктури у кіберпросторі на основі посилення ролі IT-технологій та штучного інтелекту для забезпечення резильєнтності критичної інфраструктури.

У сучасних умовах одним із найбільш небезпечних та поширених видів дистанційного ураження об'єктів критичної інфраструктури є кіберзброя. Відповідно до визначення [270], це «кіберзасіб ведення війни, який за конструкцією, поточним або передбачуваним використанням становить загрозу для життя і здоров'я людей, здатен до виведення з ладу або порушення функціонування, пошкодження чи знищення критично важливих об'єктів інфраструктури та призводить до наслідків, які кваліфікуються як кібератака».

З огляду на зростаючу цифровізацію суспільства, особливої актуальності набуває модуль цифрового навчання, що має включати системні заходи з посилення кібербезпеки в межах критичної інфраструктури. В умовах воєнного стану в Україні посилення резильєнтності критичних об'єктів передбачає не лише вдосконалення технічного забезпечення, а й завершення інституційних ініціатив, зокрема створення кібервійська, ініційованого РНБО України та Президентом.

У відповідності до Стратегії кібербезпеки України від 27.01.2016 р. [269], формування національної системи кібербезпеки повинно забезпечити ефективну взаємодію між:

– органами державної влади й місцевого самоврядування;

– військовими формуваннями та правоохоронними органами;

– науковими установами, навчальними закладами, громадськими організаціями;

– підприємствами та організаціями, зокрема тими, що є власниками або розпорядниками об'єктів критичної інформаційної інфраструктури.

Продовжуючи дослідження перспектив інституційних перетворень у сфері захисту критичної інфраструктури, доцільно звернути увагу на наукові положення М. Б. Домарацького. Дослідник наголошує на тому, що у розвинених державах розробляються спеціальні галузеві плани превентивного захисту критичної інфраструктури, які базуються на комплексному аналітичному підході, що включає:

– атрибуцію секторів критичної інфраструктури з урахуванням їх стратифікації за місцевим, регіональним та національним рівнями;

– ідентифікацію критичних ризиків і потенційних загроз;

– аналіз вразливості окремих секторів;

– моніторинг ризиків дестабілізації, пов'язаних із виведенням з ладу окремих об'єктів;

– розробку превентивних сценаріїв захисту на етапі стратегічного планування [40].

Окремої уваги потребує сфера управління у кризових і надзвичайних ситуаціях. Складність таких управлінських завдань суттєво зростає через:

– високий рівень невизначеності подій;

– дефіцит достовірної інформації;

– поширення недостовірних повідомлень через засоби масової інформації та інформаційно-психологічні операції.

За таких умов особливої ваги набуває впровадження сучасних методик, програмного забезпечення та технічних засобів для побудови гнучких систем управління. Основними цілями є:

– підвищення оперативності прийняття рішень;

– забезпечення їх ефективності;

– створення інструментів контролю виконання управлінських рішень.

Ці завдання вимагають координації та інтеграції діяльності широкого спектра організацій і служб. Така координація має стати невід'ємним елементом єдиної державної системи аналітичного забезпечення, що забезпечує ефективну підтримку рішень органів державної влади в умовах кризових ситуацій.

Одним із ключових векторів державної політики із підвищення резильєнтності об'єктів критичної інфраструктури учені [355], [306] виділяють формування монолітної державної системи, націленої на гарантування безпеки населення та критичних об'єктів, виконуючи наступні завдання:

– удосконалювати нормативно-правову базу щодо посилення відповідальності суб'єктів за порушення встановлених правил, норм, вимог, невиконання необхідних робіт, які призвели до збитків;

– розподіляти повноваження, відповідальність і сфери взаємодії органів державної влади з власниками і операторами критичної інфраструктури;

– координувати науково-технічну політику в сфері створення інновацій у секторі технологій безпеки критичної інфраструктури;

– створити об'єднану систему моніторингу стану захищеності та безпеки об'єктів критичної інфраструктури;

– сформувати постійно діючу систему попередження та знешкодження загроз для об'єктів критичної інфраструктури;

– створити систему дозвільного характеру діяльності об'єктів критичної інфраструктури незалежно від форм власності;

– реалізовувати заходи із наповнення загальноукраїнського Реєстру об'єктів критичної інфраструктури диференціюючи критерії за ступенем потенційної терористичної уразливості об'єктів;

– розробка засобів і методів захисту і контролю доступу сторонніх осіб до об'єктів критичної інфраструктури;

– удосконалення системи відбору, допуску, підготовки та атестації керівників і фахівців на об'єктах критичної інфраструктури;

– розробка методики оцінки мір безпеки на об’єктах критичної інфраструктури.

Опираючись на теорії сучасних публікацій з державного управління, щодо складних соціально-економічних систем, можна стверджувати, що напрям посилення резильєнтності критичної інфраструктури варто розглядати з двох базових позицій:

– як стан захищеності макросистеми від внутрішніх та зовнішніх загроз або ризиків;

– як сукупність елементів (адміністративних, технічних, інформаційних і т.д.), які задіяні для подальшого підтримання стану захищеності макросистеми [355], [306].

Ґрунтуючись на результатах проведених досліджень, слід акцентувати увагу на застарілості чинної безпекової парадигми, яка переважно зосереджена на внутрішніх детермінантах порушення безпеки критичної інфраструктури. Водночас у сучасній науковій та прикладній площині недостатньо розкритим залишається інституційний аспект, зокрема – комплексність системного підходу до забезпечення стійкості та формування макросистеми захисту критичної інфраструктури.

Ключовим фактором, що зумовлює необхідність інституційної трансформації державної політики захисту критичної інфраструктури, є зовнішні загрози, передусім – повномасштабне вторгнення військ РФ. Саме цей чинник нині має найбільший деструктивний вплив на систему національної безпеки в цілому та її критичні елементи зокрема.

У зв’язку з цим доцільно сформулювати Превентивну концепцію резильєнтності об’єктів критичної інфраструктури, що ґрунтується на оцінці ризиків, комплексному управлінні загрозами, а також на системному підході до інтеграції інституцій, процедур та нормативної бази. Цю пропозицію підтримує також О. М. Суходоля, який наголошує на необхідності орієнтації чинної системи кризового управління на реагування на випередження, а не лише на ліквідацію наслідків. Учений підкреслює важливість формування системи спроможностей держави до адаптації, а також методологічного поєднання зусиль усіх органів, залучених до захисту критичної інфраструктури [253; 254].

Крім того, важливо врахувати і позицію О. О. Резнікової [223], яка у своїх працях розробляє Концепцію забезпечення національної стійкості, що є основою для формування стратегічного бачення державної політики у сфері захисту критичних об’єктів.

Основні положення Превентивної концепції резильєнтності об’єктів критичної інфраструктури:

1. Встановлення адміністративно-правової відповідальності за порушення, що призводять до погіршення безпеки критичної інфраструктури. Запровадження чітких механізмів притягнення до відповідальності має стати важелем управлінського контролю.

2. Законодавче врегулювання комплексної національної оцінки ризиків і

загроз у сфері безпеки критичної інфраструктури, що забезпечить цілісне бачення загроз у міжгалузевому та просторовому вимірах.

3. Формування Національного реєстру загроз критичній інфраструктурі, а також визначення центрального органу виконавчої влади, відповідального за його ведення та оновлення.

4. Уніфікація нормативно-правової бази у сфері кризового реагування. Це необхідно для скоординованих дій органів державної влади у разі виникнення загроз, надзвичайних або воєнних ситуацій.

5. Створення постійно діючих механізмів двосторонньої комунікації між органами державної та місцевої влади і населенням, а також формалізація взаємодії з приватним сектором, неурядовими організаціями та міжнародними партнерами.

6. Розробка чіткої схеми розподілу відповідальності та повноважень між органами державної влади за напрямами забезпечення національної стійкості та захисту критичних об'єктів.

7. Формування національної мережі науково-аналітичних центрів, що займатимуться стратегічним аналізом загроз, прогнозуванням ризиків та підготовкою рішень для органів державної влади в умовах високої невизначеності.

8. Розробка діючих механізмів комунікації державних органів влади та місцевого самоврядування, приватного бізнесу, неурядових організацій, та міжнародних партнерів з питань забезпечення резильєнтності критичної інфраструктури.

9. Обов'язковість здійснення систематичних міжвідомчих та міжсекторальних тренувань і навчань за участю цивільного населення з метою посилення рівня готовності до реагування на широкий спектр загроз, посилення стійкості громад, а також економічної та суспільної стійкості [223].

В межах зазначеної ініціативи, особливої уваги вимагає блок науково-освітнього забезпечення резильєнтності критичної інфраструктури. Відповідно до Стратегічного оборонного бюлетеня України, значення освіти є одним із ключових напрямів реалізації безпекової політики. У документі визначено основні вимоги і даному напрямку:

– набуття центральними органами виконавчої влади, іншими державними органами необхідних компетентностей щодо задоволення потреб оборони держави і захисту її території від можливої агресії та ефективного управління оборонними ресурсами;

– розвиток компетентностей сил оборони в контексті підготовки до всебічного забезпечення всеохоплюючої оборони України [270].

Актуальність даного вектору підтверджено у Концепції створення державної системи захисту критичної інфраструктури, схваленій Розпорядженням КМУ № 1009-р від 06.12.2017 р. [230], де одним зі шляхів розв'язання проблеми забезпечення захисту критичної інфраструктури визначено «створення системи підготовки та перепідготовки кадрів у сфері

захисту критичної інфраструктури та встановлення вимог до планування проведення навчань (тренувань) та заходів щодо захисту критичної інфраструктури» [230]. На цьому також наголошено у Законі України «Про критичну інфраструктуру» [60], п.4, п.5 ст. 25 визначено необхідність: «створення системи підготовки кадрів для сфери захисту критичної інфраструктури» [60] (п.4), «підвищення комплексних знань, навичок і умінь персоналу та керівного складу операторів критичної інфраструктури, персоналу суб'єктів господарювання, які провадять діяльність, пов'язану із забезпеченням безпеки об'єктів критичної інфраструктури, з питань реагування на кризові ситуації на таких об'єктах» [60] (п.5). Значимість наукової складової підкреслено у п.6 ст. 25 , що передбачає «залучення експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки галузевих проектів та нормативно-правових актів у сфері захисту критичної інфраструктури» [60]. Однак, аналізуючи Стандарт вищої освіти України за спеціальністю 281 Публічне управління та адміністрування (відповідно до переліку галузей знань і спеціальностей затвердженого постановою Кабінету Міністрів України від 30 серпня 2024 р. № 1021 – D4 «Публічне управління та адміністрування») за СВО бакалавра, серед компетенцій фахівця немає жодної, яка б передбачала підготовку до управління безпекою критичної інфраструктури. А у Стандарті цієї спеціальності СВО магістра міститься лише одна – СК 06. «Здатність здійснювати професійну діяльність з урахуванням потреб забезпечення національної безпеки України», однак вона носить досить загальний характер [129], [130]. Те ж саме можемо сказати за результатами аналізу стандартів вищої освіти України за спеціальністю 073 Менеджмент (відповідно до переліку галузей знань і спеціальностей затвердженого постановою Кабінету Міністрів України від 30 серпня 2024 р. № 1021 – D3 «Менеджмент») СВО бакалавра та магістра, де немає жодної компетентності, яка б враховувала специфіку управління підприємствами критичної інфраструктури.

У перспективах вирішення виявленої проблеми слушною вважаємо пропозицію Г. Ю. Зубка [83], який пропонує внести зміни до чинного Класифікатора професій та Стандарту вищої освіти України за вказаними спеціальностями в частині доповнення компетентностей орієнтованих на управлінське забезпечення критично-важливими підприємствами в рамках національної системи безпеки об'єктів критичної інфраструктури. Це, у свою чергу, дозволить посилити інституційну спроможність у цій сфері і формування ефективної системи підготовки публічних службовців і працівників державних установ, підприємств і відомств та приватного сектора. Стратегією в питанні державної служби та управління людськими ресурсами передбачено необхідність впровадження сучасної цілісної, мобільної та гнучкої системи професійного навчання державних службовців з розвиненою інфраструктурою та належним ресурсним забезпеченням, що орієнтована на розвиток компетентностей і потреби в професійному розвитку

державних службовців [77]. Також варто зазначити, що відповідно до (ст. 49) Закону України «Про Державну службу» [57] передбачено наявність індивідуальних програм підвищення рівня професійної компетентності державного службовця, які складають службовець разом із відомчою службою управління персоналом. Центральним органом виконавчої влади з формування та реалізації державної політики у сфері державної служби є Національне агентство України з питань державної служби [168], яке відповідно до покладених на нього завдань сприяє розвитку системи закладів освіти надає освітні послуги з підготовки, спеціалізації та підвищення кваліфікації державних службовців. До даних програм також доречно включити блок із підвищення кваліфікації у напрямку забезпечення захисту критичної інфраструктури. Також в Україні існує низка наукових та науково-дослідних організацій, що потенційно спроможні зробити належний внесок у створення та функціонування відповідної системи надання необхідних компетенцій у сфері захисту критичної інфраструктури: провідні класичні університети, заклади освіти системи правоохоронних і силових структур, навчальні заклади та науково-дослідні установи.

Отже, внесення змін до чинного Класифікатора є першим кроком до розбудови як самої національної системи безпеки стратегічної інфраструктури, так і інституційної спроможності у цій сфері. Також до системи підготовки кадрів і населення, окрім перелічених, необхідно буде залучити інші галузеві установи, що мають профільну компетенцію у відповідному секторі, а також залучати експертні спільноти.

У сучасному суспільстві система інфраструктури та її компоненти не існують ізольовано, а функціональні або фізичні зв’язки між ними є динамічними та складними. Через взаємозалежність всередині інфраструктури або між інфраструктурами збій у будь-якій частині системи вплине на інші частини або навіть пошириться та спричинить порушення в інших інфраструктурах через функціональне чи фізичне підключення [350]. Таким чином, небезпека або збій можуть призвести до непередбачуваних каскадних наслідків. Це також стосується і наднаціональних загроз та ризиків, до детермінує посилення міжнародного співробітництва. Співробітництво України з ЄС у напрямку посилення захисту об’єктів критичної інфраструктури повинно сфокусуватись на наступних напрямках:

– розвиток воєнно-політичного діалогу між Україною та ЄС з широкого спектру питань спільної глобальної політики забезпечення стійкості критичної інфраструктури;

– підготовка українських фахівців у сфері забезпечення стійкості критичної інфраструктури;

– досягнення взаємосумісності визначених силових підрозділів для участі у спільних навчаннях та операціях

– посилення технологічної інтеграції об’єктів критичної інфраструктури.

Отже, на сучасному етапі удосконалення державної політики у сфері

захисту критичної інфраструктури варто сфокусувати інституційні перетворення у точці забезпечення її резильєнтності на основі чинних національних систем безпеки, захисту та кризового реагування за умов еволюції рівня координації дій до якісно нового рівня та взаємодії між ними [183]. Вкрай важливим питанням є врегулювання публічно-приватної взаємодії у формі кластерного підходу до забезпечення захисту об'єктів критичної інфраструктури диференційовано за відповідними сферами. При чому має бути визначено не тільки сфери застосування, принципи, правові засади, форми здійснення та об'єкти критичної інфраструктури, які можуть бути передані у власність приватному партнеру, а також особливості співуправління окремими об'єктами та специфіка партнерської взаємодії тими об'єктами, які належать до сфер національної безпеки з державною монополією.

3.3. Кластерний підхід до забезпечення захисту критичної інфраструктури в умовах воєнного стану в Україні

Проведені дослідження у сфері державної політики безпеки дають підстави дійти висновку, що Україні вдалося створити унікальну систему захисту об'єктів критичної інфраструктури, комбінуючи різноманітні тактичні прийоми із використанням радянських засобів протиповітряної оборони та сучасних видів озброєння передових країн світу. Створено із використанням цифрових технологій та мобільних додатків унікальну систему сповіщення населення в режимі реального часу а також моніторингу, фіксації та передачі оперативної інформації. Ефективність продемонструвала також використання проти ворожих повітряних цілей зенітно-ракетних комплексів, винищувачів, розміщення мобільних ударних груп та візуальних постів спостереження. Однак, підтримуємо позицію учених, котрі вважають сучасну модель державного управління в сфері захисту об'єктів критичної інфраструктури реактивною, тобто орієнтованою на вирішення проблем, а не на їх попередження. При цьому, як показують результати аналізу світового досвіду, неможливо досягнути прийнятного рівня безпеки та резильєнтності за відсутності дієвої системи превентивного захисту від проєктних ризиків та загроз [83]. Це ставить перед нашою державою дилему зміни загальної парадигми державної політики у цій сфері в умовах зростання військово-терористичної загрози у нашій державі. Як фідбек на вимоги сьогодення, цей вектор передбачатиме розробку стратегії протидії техногенному та інфраструктурному тероризму, інтегруючи нову функцію, пов'язану з необхідністю синхронізації в екстремальних ситуаціях державних служб, приватного сектору та операторів (власників критичних об'єктів), що набуває превентивного значення в умовах постійної ескалації складності сучасних загроз (гібридна війна, техногенний тероризм та ін.). Крім того, в умовах активних бойових дій, у геометричній прогресії зростають ризики

випадкового нанесення ударів по об'єктах критичної інфраструктури (у т.ч. ядерним та хімічним). Водночас, враховуючи значну кількість потенційних об'єктів терористичних атак, цілком можливим є свідомі атаки ворога на ядерні об'єкти, з метою дестабілізації суспільства.

Нагальною потребою державної політики резильєнтності критичної інфраструктури є інституційне закріплення питань взаємодії систем захисту. У даному напрямку корисним є досвід захисту критичної інфраструктури у США, що інтегрує процес визначення заходів і реального досвіду захисту від загроз і небезпек в сталому режимі. Відповідальність за захист у сталому режимі покладається на спільноту окремих осіб, домогосподарства, органи влади всіх рівнів, приватний некомерційний сектор, власників і операторів критичної інфраструктури та бізнес. Рекомендується використовувати сталий режим координації для визначення основних сил і засобів, необхідних для виконання місії із забезпечення захисту (рис.3.8).

Рис. 3.8. Сталий режим захисту критичної інфраструктури
Джерело: [158]

Сталий режим захисту вимагає децентралізованого управління ризиками для ефективного виконання завдань. Як національна модель координації між різними партнерами, організаціями та зацікавленими сторонами у сфері захисту, стабільна координація діяльності у сфері захисту спирається на існуючі координаційні структури для обміну інформацією та підтримки обґрунтованої та адаптивної діяльності місії у сфері захисту. Захист є безперервним процесом і вимагає адаптивної моделі організаційного навчання та міжвідомчої координації.

На основі проаналізованого вище досвіду США та країн ЄС, варто обґрунтувати пропозицію щодо законодавчого закріплення механізму спільного захисту критичної інфраструктури. Пропонуємо розглянути інноваційну ідею концепції кластерного підходу до забезпечення резильєнтності критичної інфраструктури в умовах правового режиму воєнного стану в Україні на основі створення Кластерів резильєнтності

критичної інфраструктури (КРКІ). Головна ідея даного концепту полягає у створенні навколо важливих інфраструктурних об'єктів кластерних інтеграційних об'єднань, які будуть спроможні забезпечити синергію безпекових заходів реалізованих в межах співпраці державних інститутів влади, систем захисту та реагування, самих інфраструктурних об'єктів та їх стейкхолдерів [75] (рис. 3.9).

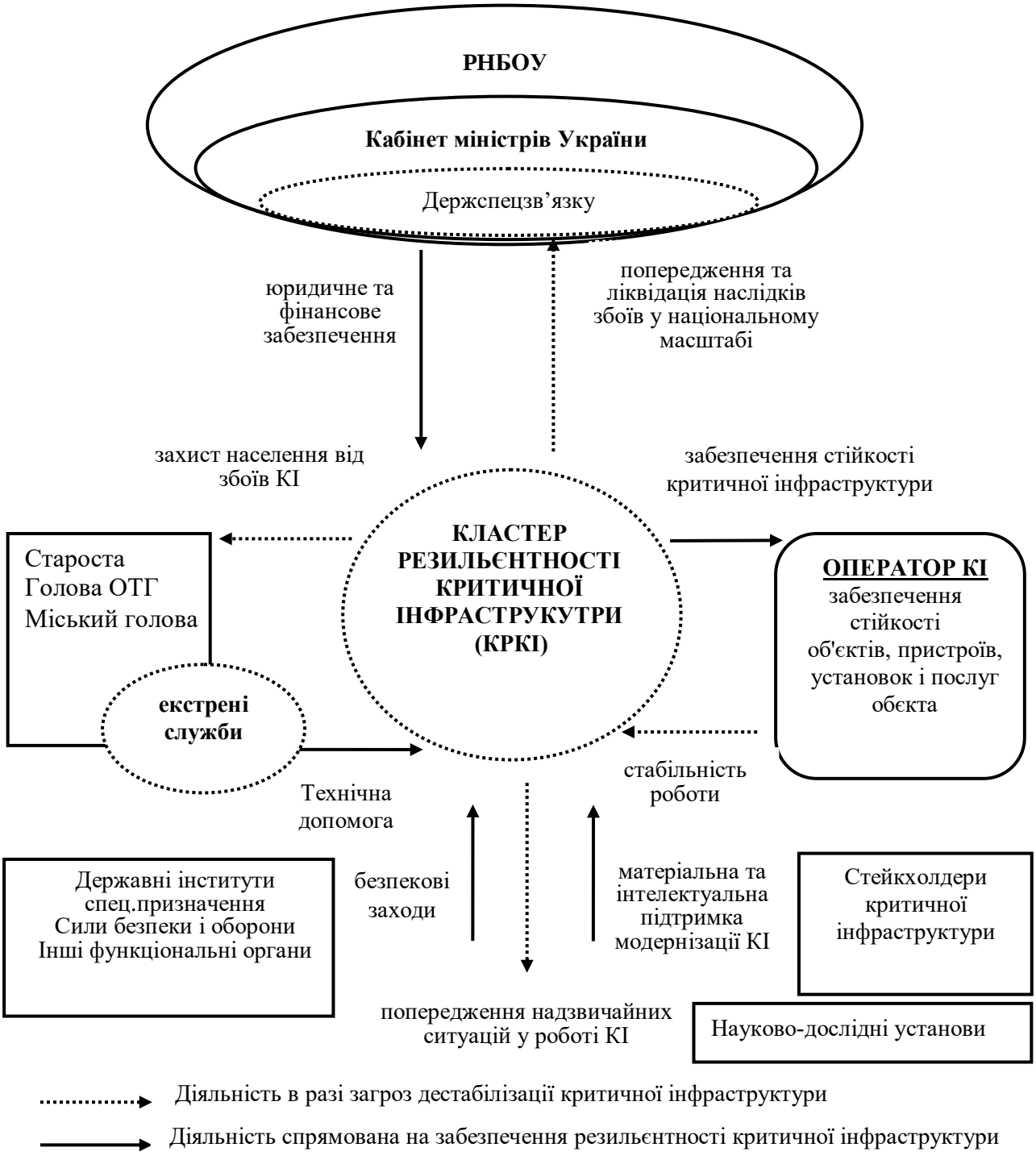


Рис. 3.9. Модель кластерного підходу до забезпечення резильєнтності критичної інфраструктури в Україні

Джерело: розробка автора

Більшість вітчизняних науковців у діагностуванні феномену «кластер» дійшли висновку, що його основними індикаторами є інноваційність, географічна близькість, незалежність учасників та їх спільний інтерес. У нашому випадку, спільним інтересом слід вважати безперебійність функціонування об'єктів критичної інфраструктури. Важливо зазначити, що кластер впливає не лише на функціональність самих об'єктів, але і на регіон у якому він функціонує. Відповідно, ефекти від створення кластера резильєнтності критичної інфраструктури проявляється у синергії дій його учасників за рахунок: анти тригерних ефектів, ефектів охоплення, масштабу, зниження безпекових витрат, накопичення знань та інновацій, ефекту інвестиційних переваг протидії ризикам, ефект колективного використання інфраструктурних об'єктів, превентивний ефект [248].

Інфраструктурні об'єкти в даному проєкті варто розглядати як тригери на основі яких зароджуються конкурентні переваги членів кластера, що присвоює їм статус «стейкхолдера». Цю дефініцію вперше обґрунтував у 1984 р. Е. Фріман у своїй праці «Стратегічне управління: роль зацікавлених сторін» [308]. Інтерпретуючи крізь призму пропонованого кластерного підходу трактування Е. Фріманом сутності інтенції «стейкхолдер», можемо дійти висновку, що його зміст передбачає окремих суб'єктів зацікавлених результатами роботи критичної інфраструктури, що є складовими її внутрішнього або зовнішнього середовища та здійснюють певний внесок у поліпшення роботи та захист об'єктів критичної інфраструктури. Колективне використання стейкхолдерами результатів роботи об'єктів критичної інфраструктури дасть змогу зменшити витрати та підвищити економічну вигоду за рахунок мінімізації ризиків дестабілізації роботи. При цьому, кластер, що успішно розвивається стає привабливим для залучення нових учасників.

Європейська практика кластерного підходу засвідчила, що це складні та динамічні структури, які здатні посилити економічне зростання за рахунок використання інноваційного потенціалу регіону. До того ж, в нинішніх умовах правового режиму воєнного стану такі потужні та стабільні об'єднання змогли б швидко рефлексувати на зміну безпекового середовища та переорієнтуватися на виробництво необхідної продукції для потреб ЗСУ та посилення систем захисту. Відзначимо, що кластери в світі стають потужним інструментом для втілення передових інновацій, діджиталізації, нових сучасних бізнес-моделей, ресурсоефективних технологій, формування засад інклюзивної соціальної креативної економіки та ін. [3].

Підтвердити дієвість та релевантність подібної кластерної ініціативи можемо на прикладі досвіду ЄС, де Директива CER [301] передбачає «розвиток скоординованої міжгалузевої та багатонаціональної оперативної співпраці у сфері захисту критичної інфраструктури від гібридних загроз, не порушуючи при цьому головних принципів ринкового лібералізму» [18].

Отже, сучасний європейський механізм державного управління у сфері захисту критичної інфраструктури закладає у основу доктрину лібералізму, що прагне забезпечити індивідуальну свободу та рівність перед законом. Лібералізм підтримує ринкову економіку, демократію та індивідуалізм [18]. Це природно призводить до розвитку державно-приватного партнерства чи інших багаторівневих моделей управління, що уникають механізму примусу. Зокрема це також представлено у Директиві CER (ст. 9-19), де передбачено, що «регулювання з боку держави передбачає підтримку приватних компаній, які опікуються посиленням стійкості критичної інфраструктури шляхом передачі матеріалів, методологій та навчання персоналу» [301]. Тобто, можемо дійти висновку, що вектор посилення колективності в державній політиці захисту життєво важливих об'єктів у країнах ЄС базується на заходах мотивації, а не примусу. Реальний приклад можемо розглянути в Нідерландах, де існує формат «округів безпеки», який уособлює механізм комунікації органів державної й місцевої влади із неурядовими організаціями та бізнесом щодо питань забезпечення національної стійкості. Перш за все він орієнтований на посилення стійкості місцевих громад до надзвичайних та кризових ситуацій. Округ безпеки передбачає об'єднання спроможностей кількох територіальних громад зі створенням спільного органу управління та з метою забезпечення ефективної взаємодії. Відповідна співпраця територіальних громад здійснюється на основі меморандумів про співробітництво. Місцеві муніципалітети територіально консолідовані в округи безпеки з урахуванням специфіки їх категорії ризиків і загроз та особливостей безпекового середовища на окремій території держав, зокрема на її кордонах із сусідніми країнами – Бельгією та Німеччиною. Головною функцією округів безпеки є ефективне реагування об'єднаних територіальних громад на кризові ситуації мікро-рівня. Цього досягають через інтеграцію єдиної системи забезпечення безпеки та стійкості, інтеграції ресурсів, посилення спроможностей та їх раціональної експлуатації, підтримання максимального рівня готовності. Важливе значення має налагодження належної взаємодії муніципалітетів та місцевих громад, сил і засобів служб оперативного реагування (протипожежних, протиповеневих, рятувальних, епідеміологічних, невідкладної допомоги, медичних, екологічних, поліцейських та ін.), інститутів антикризового управління, інформаційного, логістичного, консалтингового забезпечення округів, волонтерських організацій і приватних підприємств, територіальних підрозділів державних органів – перш за все сил реагування у вигляді берегової охорони, органів управління та безпеки у галузі водного господарства, армії і флоту та спеціальних служб. Науково-методичний супровід діяльності округів безпеки Нідерландів здійснює Нідерландський інститут громадської безпеки (Nederlands Instituut Publieke Veiligheid – NIPV) [43] Він являє собою інститут громадських знань, який об'єднує та

посилює стійкість регіонів безпеки, центрального уряду і партнерів у кризових ситуаціях за допомогою проведення досліджень, освіти, консультування та інформаційної підтримки. NIPV діє як експертний центр, коли мова йде про високоякісні знання щодо управління кризовими ситуаціями. Інститут проводить прикладні дослідження в цій галузі, систематизує науковий і практичний досвід, надає експертну допомогу щодо придбання та експлуатації оперативно-технічних засобів, створює курси професійної підготовки спеціалістів відповідного рівня, створює методичні рекомендації щодо планування у сфері антикризового управління, а також методики, довідники, керівні документи щодо дій округів безпеки в умовах звичайної діяльності та кризових явищ, і розвитку стійкості громад включно [151].

Варто також відзначити факт функціонування Європейського кластеру безпеки критичних інфраструктур (ECSCI). Основною метою даної організації є дослідницька діяльність орієнтована на створення синергії та сприяння генерації проривних рішень для розв'язання проблем безпеки та захисту критичної інфраструктури за допомогою міжпроєктної співпраці та інновацій. Діяльність відбувається із висвітленням різних підходів до кластерних проєктів організовуючи національні й міжнародні семінари, міжнародні конференції за участю представників промисловості, політиків, науковців та представників Європейської Комісії [145]. Ще однією ініціативою ЄС, яка варта уваги у забезпеченні резильєнтності критичної інфраструктури, є служба науки та знань Європейської комісії, Об'єднаний дослідницький центр (European Commission's Joint Research Centre – JRC) [146] – спільний науково-дослідницький центр Європейської комісії, який забезпечує незалежні наукові та технічні підтримку для розроблення, виконання та моніторингу політики ЄС. У сфері критичної інфраструктури дана платформа передбачає функціонування Європейської довідкової мережі захисту критичної інфраструктури (ERNCIP, n.d.), робота якої організована в тематичних групах критичної інфраструктури (наприклад, авіація, промисловість, продовольча безпека та ін.), які об'єднують сотні дослідників та експертів різних країн, які працюють у відповідних наукових колах або компетентних державних органах [145].

Нестор О. Ю. наголошує , що політика держави має зосереджуватись на збереженні ролі приватного сектору у фінансуванні критичної інфраструктури [135]. Відповідно, основна мета ініціювання таких проєктів створення кластерів резильєнтності критичної інфраструктури – вирішення життєво важливих для населення країни (територіальної громади) проблем із залучення ресурсів приватного бізнесу (фінансових, матеріально-технічних, технологічних, організаційних, кадрових) а також посилення ролі науково-інтелектуального потенціалу країни.

Особливої уваги вимагає науково-інформаційне забезпечення в межах

функціонування КРКІ. Приклад ефективної комунікації можемо знайти в ЄС, де функціонують Центри обміну інформацією та аналізу (Information Sharing and Analysis Centers – ISACs). Це некомерційні організації, які створюють централізований ресурс для збору інформації про основні загрози, їх причини та інциденти, що стосуються безпеки критичної інфраструктури. Дані центри діють на умовах публічно-приватного партнерства, забезпечуючи реверсний обмін аналітичними даними, знаннями та досвідом між приватним і державним секторами. ISAC або подібні ініціативи існують у більшості країн-членів ЄС. ISAC глибоко інтегруються в інформаційний простір свого сектору, транспортуючи важливу інформацію до відповідних суб'єктів захисту [147].

У більш розширеному форматі дана структура існує також у США, де функціонує Real Estate Information Sharing and Analysis Center (RE-ISAC). Орган створено у лютому 2003 року організацією The Real Estate Roundtable (некомерційна громадсько-політична установа). RE-ISAC є яскравим прикладом публічно-приватного партнерства між сектором комерційних об'єктів США та федеральними чиновниками внутрішньої безпеки. Організація служить основним інформаційним каналом попередження про терористичні, природні та кібернетичні загрози та інформування про можливості спільного між урядом і приватним комерційним сектором реагування на них. Роль Real Estate ISAC полягає в підтримці місії захисту критичної інфраструктури власників і операторів шляхом надання інформації про потенційні антропогенні інциденти та стихійні лиха, щоб вони могли визначити потенційні ризики, пом'якшити їх, наскільки це можливо та ефективно реагувати. В результаті RE-ISAC та його члени можуть досягти цілей, які жодна галузева організація не може досягти поодинці [152].

Модель кластерного підходу до забезпечення резильєнтності критичної інфраструктури в Україні також здатна забезпечити значні перспективи до організації міжсекторального навчання та підвищення кваліфікації на основі обміну інформацією, досвідом та залученням науково-дослідницьких установ. Підтвердження перспективності даного напрямку та його практичну реалізацію можемо знайти у досвіді США [164], де дана модель проведення комплексу навчальних (тренінгових) заходів реалізуються у вигляді:

– семінарів (Seminars) та воркшопів (Workshops) – передбачають активну форму залучення кола зацікавлених сторін до вивчення окремих проблем у сфері захисту критичної інфраструктури, їх обговорення, роз'яснення інноваційних підходів, новітніх правил та процедур реагування;

– «настільних вправ» (Tabletop Exercises, TTX) – забезпечують активне аудиторне обговорення, теоретичне відпрацювання способів реагування на певні абстрактні події, дискусії стосовно дієвості стандартних регламентів, планів та протоколів дій відповідальних суб'єктів на проєктні загрози та ризики на об'єктах критичної інфраструктури. Фактично даний вид навчання

передбачає оцінку ефективності інституційно-правовго забезпечення захисту критичної інфраструктури а не дій операторів чи безпекових служб;

– фокусне навчання (Drills) – проводиться в реальному часі із залученням безпосередніх учасників, сил та засобів сфери захисту критичної інфраструктури в мінімальному обсязі, який регламентується функціональною спрямованістю заходу. Даний вид навчання націлений на аудит спроможності кадрового складу відповідних служб у стандартних надзвичайних ситуаціях на об'єктах критичної інфраструктури (наприклад пожежна евакуація);

– повномасштабні тренування (Full-Scale Exercises) – проводяться в реальному часі та в умовах детальної імітації нестандартної надзвичайної ситуації до яких залучаються усі сили та засоби реагування у повному складі.

Аналізуючи досвід США та інших країн НАТО у сфері розширення компетентностей кадрового складу сфери захисту критичної інфраструктури можна препарувати наступні підходи до сфери між секторальних навчань і тренувань:

1) залежно від масштабу охоплення секторів критичної інфраструктури, процес тренувань та навчання можна поділити на міжнаціональне, загальнодержавне, регіональне та територіальне, секторальне, кластерне та об'єктове;

2) залежно від залучених до процесу тренувань на навчання сил, ресурсів та суб'єктів захисту, а також складеності та масштабності завдань, що відпрацьовуються, їх можна поділити на командно-штабні та тактико-спеціальні;

3) процедури навчань і тренувань дозволяють отримати комплексну оцінку спроможності державної політики у сфері безпеки критичної інфраструктури та стану готовності сил реагування на кризові ситуації.

У свою чергу, комплексність оцінки досягається в наслідок моніторингу:

– комплексності нормативно-правової бази у сфері БСКІ, відсутності у ній прогалин, суперечностей та неузгодженостей;

– наявності та прорахованості відповідних превентивних антикризових планів, а також планів реагування та відновлення;

– наявності підготовлених кваліфікованих працівників, достатності матеріальних та фінансових ресурсів та оснащеності;

– синхронізованості дій залучених сил реагування.

Перекладаючи досвід США з питань формування та розвитку системи підготовки персоналу з питань забезпечення безпеки та стійкості стратегічної інфраструктури на українські реалії, варто зосередити увагу на таких аспектах, як нормативно-правове та організаційне забезпечення такої системи особливо в умовах здійснення реформи державного управління, ініційованої Стратегією реформування державного управління України на 2022-2025 роки [227].

Отже, відповідно до проведеного вище аналізу, у сфері захисту критичної інфраструктури потребують уточнення питання, що стосуються підготовки кадрів, підвищення компетентностей та залучення експертного потенціалу з питань її захисту та забезпечення резильєнтності. Варто препарувати та чітко урегулювати положення із підготовки кадрів і населення у сфері безпеки критичної інфраструктури, адже така підготовка має відбуватися на принципах системності та систематичності відповідно до кадрових потреб цільових інститутів профільними закладами освіти та експертними організаціями і науково-дослідними установами.

Варто наголосити, що Державна служба України з надзвичайних ситуацій має у своєму розпорядженні найбільш широкий спектр можливостей щодо комплексного вирішення представлених вище проблем із забезпечення превентивного захисту критичної інфраструктури [244].

Основними механізмами моделі кластерного підходу до забезпечення резильєнтності критичної інфраструктури в Україні варто передбачити:

– розробку й реалізацію загальнодержавних, регіональних та місцевих програм підтримки та мотивування створення кластерів резильєнтності критичної інфраструктури з інтегрованими захисними механізмами;

– ініціювання організації галузевих та міжгалузевих асоціацій, об’єднань та громадських організацій, спеціалізованих фондів з дифузії об’єктів критичної інфраструктури до бізнес-середовища;

– формування спроможних кластерів резильєнтності критичної інфраструктури.

Отже, можемо зробити висновок, що кластери резильєнтності критичної інфраструктури – це інноваційний формат публічного управління в сфері забезпечення безпеки, стійкості й економічного розвитку регіонів, який передбачає об’єднання спроможностей територіальних громад, інститутів публічного управління, наукових установ, об’єктів критичної інфраструктури та їх стейкхолдерів шляхом створення спільного об’єднання з метою координації і розширення взаємодії. Як свідчить міжнародна практика, сутністю цього явища є встановлення довгострокових стратегічних відносин у реалізації суспільно значущих проєктів між приватним сектором, публічною владою та об’єктами критичної інфраструктури. В умовах України, зазначена ініціатива стає можливою до практичного втілення в межах реалізації проєктів «державно-приватного партнерства», яке передбачено у відповідному Законі України [55]. У зазначеному нормативному акті явище державно-приватного партнерства трактується як «співробітництво між державою Україна, Автономною Республікою Крим, територіальними громадами в особі відповідних державних органів, що згідно із Законом України «Про управління об’єктами державної власності» здійснюють управління об’єктами державної власності, органів місцевого самоврядування, Національною академією наук України, національних

галузевих академій наук (державних партнерів) та юридичними особами, крім державних та комунальних підприємств, установ, організацій (приватних партнерів), що здійснюється на основі договору в порядку, встановленому цим Законом та іншими законодавчими актами, та відповідає ознакам державно-приватного партнерства» [55]. Серед таких ознак:

1) створення та/або будівництво (нове будівництво, реконструкція, реставрація, капітальний ремонт та технічне переоснащення) об'єкта державно-приватного партнерства та/або управління (користування, експлуатація, технічне обслуговування) таким об'єктом;

2) довготривалість відносин (від 5 до 50 років);

3) передача приватному партнеру частини ризиків у процесі здійснення державно-приватного партнерства;

4) внесення приватним партнером інвестицій в об'єкт державно-приватного партнерства [55].

Потребує уваги уніфікація спільної термінології у сфері перспектив розвитку кластерної моделі. Звернемо увагу на певні термінологічні відмінності у визначеннях, наприклад, ст. 10 Закону України «Про основні засади забезпечення кібербезпеки України» [68] регламентує застосування процедури «державно-приватної взаємодії», у якості «широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері» [68]. У ст. 25 Закону України «Про критичну інфраструктуру» [60] у сфері захисту критичної інфраструктури уже передбачено застосування процедури «державно-приватного партнерства». Отже, можемо дійти висновку що термін «державно-приватна взаємодія» використовується лише по відношенню до сфери кібербезпеки а «державно-приватне партнерство» носить більш широкий спектр сфер застосування, серед яких можна виокремити наступні сфери дотичні до критичної інфраструктури:

– генерація, транспортування і постачання теплової енергії та перерозподіл і постачання природного газу;

– будівництво та експлуатація доріг, автострад, залізниць, мостів, шляхових естакад, злітно-посадкових смуг на аеродромах, морських і річкових портів та їх інфраструктури, тунелів і метрополітенів;

– збір, очищення та розподіл води;

– забезпечення функціонування меліоративних систем;

– виробництво, розподілення та постачання електричної енергії.

Зауважимо, що зазначений список не охоплює усі сектори критичної інфраструктури, що обмежує можливості застосування його норм до формування кластерів резильєнтності в усіх сферах критичної інфраструктури, а також залучати інші недержавні організації сфери

публічного управління. Відповідно вирішення даної дилеми потребує ухвалення окремого закону чи внесення відповідних змін до чинних законів у сфері захисту та резильєнтності критичної інфраструктури. Реалізація цього завдання в умовах воєнного стану та військового вторгнення рф передбачає налагодження тісної співпраці і створення дієвих організаційних механізмів на загальнодержавному, а також локальному місцевому та регіональному рівнях. Зокрема на низових рівнях слід забезпечити первинне реагування на ризики, загрози і кризові ситуації. Таким чином оперативність, ефективність та превентивність заходів реагування на подібні явища дозволить попередити деструктивний вплив на критичну інфраструктуру. Створення стабільних форматів взаємодії органів державної і місцевої влади, підприємств та організацій, інститутів самоорганізації населення, науково-дослідних установ із об'єктами критичної інфраструктури на регіональному і локальному рівнях є умовою ефективності провадження державної політики у сфері забезпечення безпеки та резильєнтності критичної інфраструктури. Головною умовою має стати посилення превентивних заходів, що дозволить трансформувати модель державного управління у сфері захисту критичної інфраструктури із реактивної у активну фазу.

Враховуючи виявлену розрізненість термінології та інституційні бар'єри міжсекторальної взаємодії, більш відповідним умовам реалізації моделі кластерного підходу вважаємо інтеграцію у сферу державної політики терміну «публічно-приватне партнерство». Учені Н. Е. Дєєва та В. В. Хмурова пропонують тлумачити дану дефініцію як «модель співробітництва бізнесу та держави, що дозволяє реалізовувати важливі проєкти за допомогою інновацій, капіталу та ресурсів приватного бізнесу, без перевантаження державного бюджету» [24]. Нашу позицію підтверджує І. М. Кульчій, стверджуючи, що використання категорії «публічно-приватне партнерство» є більш доцільним ніж «державно-приватне партнерство». Учений пояснює цю позицію по-перше – усталеністю в міжнародному правозастосуванні саме публічно-приватного партнерства; по-друге – публічно-приватне партнерство передбачає розширення суб'єктного складу інститутами публічного управління на центральному та місцевому рівнях [108]. Також, відповідно до міжнародної практики, сутністю явища публічно-приватного партнерства є встановлення довгострокових стратегічних відносин із реалізації суспільно-важливих проєктів між приватними інвесторами та органами публічного управління, що об'єднує центральні органи виконавчої влади, органи місцевого самоврядування та інститути самоорганізації суспільства, що найбільш відповідає заявленій ініціативі створення кластерів резильєнтності критичної інфраструктури.

У довіднику з публічно-приватного партнерства, виданому Міжнародним банком реконструкції та розвитку у 2017 р. [340], наведено визначення дефініції «публічно-приватне партнерство» як «довгострокового

контракту між приватною стороною та державною організацією на надання державного активу або послуги, в якому приватна сторона несе значний ризик і відповідальність за управління, а винагорода пов'язана з результатами роботи» [340]. Довідник також визначає сектори, в яких застосовується публічно приватне партнерство у світі: виробництво та розподіл електроенергії, водопостачання та каналізація, утилізація сміття, трубопроводи, медицина, освіта, транспорт, правоохоронна служба, залізниця, дороги, системи інформаційних технологій, житлово-комунальний сектор та ін. Слушним у якості розширення запропонованої ініціативи вважаємо також визначення публічно-приватного партнерства, яке пропонують П. І. Надолішній і Н. В.Пироженко, як «систему законодавчо врегульованих і юридично оформлених відносин між органами державної влади, органами місцевого самоврядування, приватним бізнесом (юридичними та фізичними особами), громадськими організаціями для вирішення суспільно значущих проблем на довготривалий період часу, заснованих на узгодженні інтересів і взаємній зацікавленості в досягненні намічених цілей, на довірі і таких, що передбачають добровільне об'єднання ресурсів, спільне ухвалення рішень, раціональний розподіл ризиків і спільну відповідальність за результати» [121]. Погоджуємося також із думкою О. Ю. Нестор , яка вважає публічно-приватне партнерство сучасним способом сприяння приватному забезпеченню задоволення підвищеного попиту на послуги критичної інфраструктури [135]. Актуальність запропонованої моделі кластерного підходу можемо підкріпити також позицією вченого Г. Ю. Зубка, котрий, вивчаючи перспективи публічно-приватного партнерства у сфері захисту критичної інфраструктури, відзначає, що «у даному векторі державної політики бракує системного підходу до управління комплексом секторних підсистем, об'єктів, ресурсів та залучення до цих процесів приватних партнерів» [83]. Вважаємо, що саме кластер резильєнтності допоможе у вирішенні описаної квестії.

Юридично базові відносини в межах функціонування кластеру резильєнтності критичної інфраструктури на основі публічно-приватного партнерства пропонуємо врегулювати відповідно до ст. 1130. ЦКУ, яка передбачає заключення договору «Про спільну діяльність» [276], згідно якого сторони зобов'язані «спільно діяти без створення юридичної особи для досягнення певної мети, що не суперечить законодавству» [276]. Договір про спільну діяльність можуть оформляти підприємства, спеціалізовані як на окремих товарах (послугах), так і окремих технологічних процесах. За договором простого товариства учасники беруть зобов'язання об'єднати свої вклади для досягнення спільної мети, наприклад, спільного будівництва об'єкту критичної інфраструктури, необхідного усім учасникам. У зазначених договорах можуть брати участь як приватні, так і державні суб'єкти, а також некомерційні організації. Тобто, дана організація

передбачає колективне інвестування у необхідне обладнання для функціонування критичної інфраструктури та її резильєнтності.

З метою розвитку нормативно-правового поля адаптації моделі кластерного підходу до забезпечення резильєнтності критичної інфраструктури в Україні, прислухаємось до пропозицій учених О.Ю. Носова та Т. В.Черничко, які наголошують, що з цією метою слід сформувати методичні рекомендації щодо реалізації кластерної політики та створення кластерів резильєнтності критичної інфраструктури [137]. За основу можна взяти Закон України «Про стимулювання розвитку регіонів» [74], який визначає правові, економічні та організаційні засади реалізації державної регіональної політики щодо стимулювання розвитку регіонів та подолання депресивності територій із внесенням відповідних змін. У даному контексті стимулювання розвитку регіонів могло би також здійснюватись на засадах моделі кластерного підходу до забезпечення резильєнтності критичної інфраструктури в Україні. Зазначена модель відповідає напрямкам державної регіональної політики, зазначеної у Законі України № 2389-IX від 09.07.2022 р. «Про внесення змін до деяких законодавчих актів України щодо засад державної регіональної політики та політики відновлення регіонів і територій» [54] зокрема відповідає наступним положенням:

– включає вектори відновлення регіонів і територій, що постраждали внаслідок збройної агресії проти України, в соціальному, гуманітарному, економічному, екологічному, безпековому та просторовому вимірах;

– передбачає адаптацію регіональної економіки та суспільства для посилення стійкості територіальних громад до безпекових викликів;

– створює ефективний механізм представництва інтересів мікросередовища на загальнонаціональному рівні.

Важливим є розробка алгоритму створення територіального кластеру резильєнтності критичної інфраструктури, який можемо зобразити на основі інтерпретації проаналізованого закордонного досвіду та інституційно-правового поля України (рис.3.10).

Ініціювати створення територіального кластеру резильєнтності критичної інфраструктури на основі пропозиції про здійснення державно-приватного партнерства можуть центральні, місцеві органи виконавчої влади, органи місцевого самоврядування чи органи АРК, Національна академія наук України, галузеві академії наук, державні, комунальні підприємства, установи, організації, господарські товариства (100 відсотків статутного капіталу яких належить державі), територіальні громади а також суб’єкти, які можуть бути стейкхолдерами відповідних об’єктів критичної інфраструктури. Зазначені суб’єкти подають до Уповноваженого органу у сфері захисту критичної інфраструктури відповідне подання та підготовлену концептуальну записку необхідності створення КРКІ. Останній здійснює оцінку відповідності пропозиції вимогам законодавства та ініціює створення відповідної Комісії для оцінки ефективності, територіальних та

функціональних можливостей КРКІ, до складу якої входять члени комітетів Верховної Ради України, до предмета відання яких належать об'єкти критичної інфраструктури та питання регіональної політики.

Рис.3.10. Алгоритм створення територіального кластеру резильєнтності критичної інфраструктури

Джерело: сформовано автором на основі [60], [200], [222].

Подання складається з концептуальної записки де обґрунтовано концептуальні аспекти формування відповідного кластеру. Комісія здійснює оцінку та визначає склад функціональних типів територій України на яких планується створення кластеру та аналізує техніко-економічні особливості на основі чого формує висновок за результатами аналізу ефективності. Висновок містить інформацію щодо проєкту, інформацію про очікувані соціально-економічні, екологічні та безпекові результати створення КРКІ, обґрунтування факторів, що обумовлюють підвищення ефективності реалізації проекту саме у формі кластерної моделі, обґрунтування інформації

про ризики здійснення проєкту, інформацію про потребу в державній підтримці та її форму (матеріальна, фінансова, інформаційна та ін.), інформацію про організаційну форму здійснення діяльності та висновок стосовно доцільності (недоцільності) створення КРКІ. Якщо Комісія встановлює, що пропозиція створення кластеру є недоцільною, вона видає негативний висновок, який має бути обов'язково достатньо аргументованим та повідомляє про це Уповноважений орган у сфері захисту критичної інфраструктури. Уповноважений орган повідомляє про відмову в розгляді пропозиції суб'єкту, який подав пропозицію, із зазначенням підстави відмови. У разі хвального висновку Комісія повідомляє про це Уповноважений орган у сфері захисту критичної інфраструктури та розробляє техніко-економічне обґрунтування, останній видає відповідне розпорядження про створення КРКІ та повідомляє про це суб'єкт, який подав пропозицію [200], [222].

Для планування відновлення та стимулювання розвитку регіонів та територій, а також з метою запровадження кластерів резильєнтності критичної інфраструктури Законом України № 2389-IX від 09.07.2022 р. «Про внесення змін до деяких законодавчих актів України щодо засад державної регіональної політики та політики відновлення регіонів і територій» [54]. визначаються такі функціональні типи територій: території відновлення, регіональні полюси зростання, території з особливими умовами для розвитку, території сталого розвитку. Перелік функціональних типів територій, а також вимоги щодо показників для віднесення територій до різних функціональних типів визначаються Кабінетом Міністрів України.

Розпочати апробацію зазначеної ініціативи пропонуємо саме із територій відновлення. Дана категорія Законом ідентифікується як «мікрорегіони, територіальні громади, на території яких відбувалися бойові дії та/або які були тимчасово окуповані, та/або території яких зазнали руйнувань об'єктів критичної інфраструктури, соціальної інфраструктури, об'єктів житлового фонду внаслідок ведення бойових дій, а також які характеризуються різким погіршенням рівня соціально-економічного розвитку та значним переміщенням населення до інших регіонів та/або інших держав».

Регіональними полюсами подальшого розвитку моделі кластерного підходу до забезпечення резильєнтності критичної інфраструктури в Україні є мікрорегіони та територіальні громади, що віднесені до територій сталого розвитку. Вони є самодостатніми, з наявним соціально-економічним потенціалом територій та спроможні до збалансованого розвитку в економічній, соціальній та екологічній сферах.

У напрямі інституційно-правового врегулювання запропонованих ініціатив підтримуємо пропозицію Г. Ю. Зубка [83]. щодо внесення відповідних змін до законів України «Про державно-приватне партнерство»,

«Про управління об’єктами державної власності», «Про концесію», які регулюють переважно партнерство і взаємодію в галузі економіки та реалізації інвестиційних й інфраструктурних проєктів а також Закону «Про критичну інфраструктуру». Серед основних завдань кластерів варто визначити:

– підтримка публічно-приватного партнерства у розбудові системи захисту критичної інфраструктури, заснованої на спільній відповідальності, співпраці та довірі, а також інших принципах лібералізму державної політики, доступних для них інформаційних каналах, зовнішня підтримка, суттєва допомога або допомога у пошуку компетентних експертів, здатних вирішити конкретні проблеми, що виникають у функціонуванні критичної інфраструктури;

– співпраця з науковими установами в ідентифікації ризиків та загроз критичній інфраструктурі та допомога в пошуку компетентних експертів у побудові комплексу превентивних заходів та методів їх застосування, методів прогнозування результатів, які можуть бути використані при удосконаленні моделі кластерного підходу до забезпечення резильєнтності критичної інфраструктури в Україні;

– звітність про проблеми, виявлені під час впровадження моделі кластерного підходу, подання пропозицій щодо вирішення проблем та пропозицій щодо вдосконалення системи захисту органам державної влади;

– розробка пропозицій внесення змін до нормативно-правових актів з метою сприяння та підтримки виконання завдань у сфері забезпечення резильєнтності критичної інфраструктури;

– оцінка ризиків порушення роботи систем критичної інфраструктури, спричиненого руйнуванням або дисфункцію об’єктів (збір інформації, необхідної для виявлення загроз, прогнозування наслідків та визначення вразливостей критичних об’єктів);

– співпраця з органами, до компетенції яких входять регулювання питань критичної інфраструктури;

– співпраця з іншими координаторами функціонування критичної інфраструктури (ідентифікація взаємозалежностей між системами критичної інфраструктури, робота з експертами з інших систем, моделюванням вразливостей та превентивних заходів, інформування про загрози);

– співпраця з операторами критичної інфраструктури у сфері її захисту, активізація співпраці із науковими установами та її підтримка (ініціювання та підтримка контактів, запрошення на конференції, симпозіуми, тренінги, на яких розглядаються питання, пов’язані із резильєнтністю критичної інфраструктури, оцінкою ризиків, методами управління у надзвичайних ситуаціях, підготовка консультативних зустрічей з операторами критичної інфраструктури, тощо);

– задоволення потреб операторів та стейкхолдерів щодо обміну актуальною інформацією;

– підтримка організації системних міжсекторальних навчань з підвищення ефективності захисту критичної інфраструктури (допомога в розробці програми навчань, допомога у приєднанні до програми, виконання ролі арбітра, спостерігача навчань, допомога в оцінці результатів навчань, допомога в наданні необхідної інформації);

– діяльність, спрямована на відновлення функціональності пошкоджених об'єктів критичної інфраструктури (підтримка контактів з операторами щодо їхніх потреб, надання інформації іншим координаторам системи, органам державної влади, допомога в пошуку компетентних експертів та інвесторів) ;

– проведення періодичного аналізу та оцінки ефективності захисту критичної інфраструктури у відповідній системі (на основі співпраці з операторами, робочих візитів, опитувань, інтерв'ю);

– стимулювання впровадження сучасних методів захисту критичної інфраструктури (збір інформації про сучасні методи захисту, обмін цією інформацією з операторами критичної інфраструктури);

– організація тренінгів, конференцій та науково-дослідницьких симпозіумів, удосконалення організаційно-технічних та формально-правових заходів щодо протидії збоям у функціонуванні критичної інфраструктури;

– стимулювання активності суб'єктів, залучених до процесу захисту критичної інфраструктури (листування, опитування та інтерв'ю щодо виявлення прогалин у системі захисту та потреб операторів, візити, збір тем для обговорення та ін.);

– підтримка системних ініціатив, спрямованих на підвищення безпеки критичної інфраструктури (збір інформації про ініціативи операторів щодо підвищення її безпеки, матеріально-технічна підтримка, допомога в контактах зі стейкхолдерами, які можуть посилити ці ініціативи та ін.).

Незважаючи на позитивні сторони розвитку кластерних ініціатив, в Україні варто відзначити певні проблеми у цьому напрямку:

– низький рівень довіри на всіх рівнях (місто, область, країна) державного управління, а також у суспільства до колективних форм діяльності;

– обмеженість належного правового забезпечення публічно-приватного партнерства для потенційних учасників кластеру у сфері критичної інфраструктури. Незважаючи на те, що в Україні у 2010 році було прийнято Закон «Про державно-приватно-партнерство», який міг би дати можливість державним органам брати участь у партнерстві, існує потреба розширити діапазон можливих форм і стратегій для взаємодії;

– диспропорції між інтересами місцевої влади та бізнес-партнерів,

зокрема щодо модернізації інфраструктури для започаткування кластеру;

– відсутність національної та регіональної політики, спрямованої на фінансово-матеріальну мотивацію кластерних ініціатив.

Як показують результати досліджень, найперспективнішими джерелами фінансування ініціатив розвитку кластерів резильєнтності критичної інфраструктури в умовах воєнного стану в Україні можуть стати наступні міжнародні проєкти, що доступні в межах програм, що реалізуються міжнародними фондами:

– програми підтримки розвитку інноваційного підприємництва на локальному та міжнародному рівнях (наприклад Accelerate-2030, Climate-KIC Accelerator, European Institute of Innovation and Technology та ін.);

– міжнародна система освіти, міжнародні форуми, конференції та семінари у напрямку розвитку необхідних компетентностей (наприклад USAIDE, PAUCI, Open Society Institute, Soros Foundation та ін.);

– проекти розвитку та підтримки транскордонного співробітництва (Світовий банк, фонди ЄС, ОЕСР та ін.).

Європейський досвід засвідчує, що кластери є складними та динамічними структурами, які в умовах коронакризи змогли швидко відреагувати на зміну середовища та переорієнтуватися на виробництво необхідної продукції та стали потужним стратегічним інструментом для втілення ресурсоефективних рішень і формування засад інклюзивної соціальної креативної економіки [147]. Це природно призводить до розвитку описаного вище публічно-приватного партнерства чи інших багаторівневих моделей управління, що детерміновано інституційними умовами монополізму у сфері державної політики захисту критичної інфраструктури Урядом. При цьому, як демонструють результати досліджень, державній владі не вистачає їх монополізованих повноважень, а також необхідних сучасних знань і ресурсів для оптимального виконання обов’язків щодо забезпечення резильєнтності таких об’єктів, оскільки більшість об’єктів критичної інфраструктури належить та управляється приватним сектором. Спільні державно-приватні безпекові проекти у ЄС дозволяють вирішити дану проблему, генеруючи практичні рекомендації, що перевіряються в реальних ситуаціях та дозволяють досягти високого рівня технологічної готовності. Учасниками таких проектів є науково-дослідницькі установи, оператори та власники критичної інфраструктури та компетентні органи публічного управління.

Підтверджуючим прикладом успішності функціонування кластерної моделі у сфері захисту критичної інфраструктури є створений у 2021 році Національний кластер кібербезпеки (The National Cybersecurity Cluster). Це координаційна платформа, яка об’єднує ресурси, можливості та компетенції РНБО України та Фонду цивільних досліджень і розвитку США (CRDF Global), державних установ, міжнародних партнерів та приватного сектору з

метою посилення партнерства, співробітництва та поліпшенню якості освіти у сфері кібербезпеки та оборони України. Основними завданнями Національного кластеру кібербезпеки є підвищення рівня стратегічного потенціалу національної кібербезпеки, розвиток професійної кіберспільноти та забезпечення безпечного кіберпростору України. Діяльність Національного кластеру кібербезпеки спрямована на зміцнення спроможностей, сталий розвиток національного сектору кібербезпеки України та проведення регулярних заходів: координаційних зустрічей, форумів, самітів, освітніх конференцій [170].

Для ефективного відновлення інфраструктури в межах кластерів резильєнтності критичної інфраструктур після екстремальних подій операторам важливо знати фактори (зовнішні, технічні та організаційні), які впливають на процес відновлення та можливість спрогнозувати можливі наслідки. Такі знання допоможуть операторам та інститутам державної влади приймати раціональні рішення на основі реалістичної оцінки швидкості та часу потрібного на відновлення продуктивності інфраструктурного об'єкта. У даному випадку корисним вважаємо підхід до забезпечення резильєнтності критичної інфраструктури на основі «трикутника стійкості». Дана теорія ілюструє втрату продуктивності об'єкта критичної інфраструктури у часі (рис 3.11.).

Цей підхід базується на гіпотезі про те, що якість послуг об'єкта критичної інфраструктури для потреб стейкхолдерів визначено міру Pt (100%), яка в нормальних умовах є стабільною у часі (наприклад електропостачання). Однак, продуктивність (P) може коливатися від 0% до 100%, (залежно від певних факторів впливу) де 100% означає відсутність погіршення якості обслуговування, а 0% означає, що послуга недоступна. Інцидент деструктивного впливу на об'єкт (наприклад ракетний удар), що стався у момент часу T_i, може завдати миттєвої шкоди критичній інфраструктурі, що призведе до негайного зниження продуктивності (від 100% до 0%). Очікується, що у момент часу T_f розпочнеться процес відновлення інфраструктури відбуватиметься з часом, як показано на цьому малюнку, до часу Tr, коли вона буде повністю відремонтована (вказується якістю 100%). «Трикутник вразливості» об'єкта критичної інфраструктури ілюструє обсяг втрати продуктивності та час необхідний на його відновлення, що залежить від превентивних заходів проведених на об'єкті. Таким чином, чим менша площа даного трикутника, тим резильєнтнішою є інфраструктура [343]. Ця гіпотеза підкреслює, що резильєнтність має свої часові виміри, включаючи здатність чинити опір, реорганізовуватися, змінюватися та навчатися у відповідь на загрозу. Багато в чому резильєнтність об'єднує в собі показники ризиків, вразливості, надійності, міцності, живучості, адаптивності, ремонтопридатності об'єктів критичної інфраструктури [344]. Отже, складові описаного «трикутника вразливості»

можуть бути компенсовані тріадою відповідних детермінант резильєнтності – протидія (превентивний захист), адаптація та відновлення.

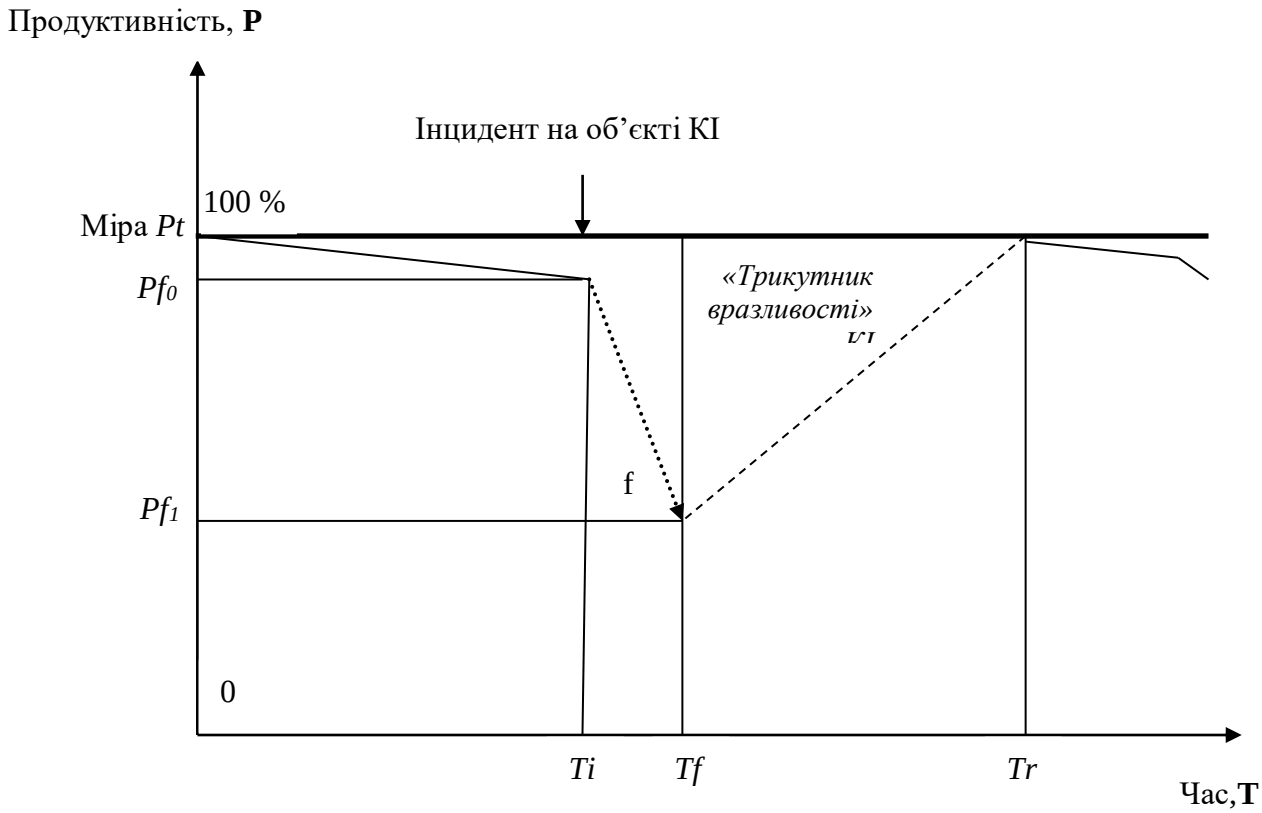


Рис. 3.11. Моделювання втрати продуктивності об'єктом критичної інфраструктури

Джерело: розроблено автором на основі [288], [344]

На основі запропонованої гіпотези, з метою можливості оцінки досягнутої резильєнтності критичної інфраструктури в межах кластерної моделі, варто розглянути можливість застосування певного вимірника. З цією метою можна ініціювати застосування Індексу резильєнтності критичної інфраструктури (stability index – SI), як суми індексу ефективності превентивного захисту, індексу адаптованості до загроз, індексу відновлюваності критичної інфраструктури:

$$SI_{KI} = \mathrm{RI}_{KI}\mathrm{AI}_{KI}\mathrm{PPI}_{KI} \qquad (3.1.)$$

Чим вищий показник індексу, тим вища резильєнтність і тим стійкішою є критична інфраструктура.

Індекс відновлюваності критичної інфраструктури (RI_{KI}) – це співвідношення рівня регенерації функціональності, яке вимірюється як рівень відновленої виробничої потужності (restored production capacity – RPC) до втраченої виробничої потужності (lost production capacity – LPC):

$$RI_{KI} = \frac{\text{RPC}}{\text{LPC}} * 100\% \quad (3.2.)$$

Індекс адаптованості до загроз (IA_{KI}) – відношення часу на відновлення одиниці продуктивності у результаті впливу зафіксованого деструктивного інциденту (performance recovery time – PRT) до часу на відновлення одиниці продуктивності при повторному інциденті того ж характеру (performance recovery time – PRT re-incident):

$$AI_{KI} = \frac{\text{PRT}}{\text{PRT re-incident}} * 100\% \quad (3.3.)$$

Індекс ефективності превентивного захисту (PPI_{KI}) – відношення між реальним рівнем продуктивності критичної інфраструктури (real level of productivity – RLP) після інциденту із урахуванням застосованих превентивних мір до прогнозованого рівня продуктивності цієї інфраструктури (predicted level of productivity – PLP) після надзвичайної ситуації на основі розроблених превентивних заходів.

$$PPI_{KI} = \frac{RLP_{KI}}{PLP_{KI}} * 100\% \quad (3.4.)$$

Рівень продуктивності вимірюється кількістю нормально працюючих компонентів у системі інфраструктури та достатнім рівнем її потужності для виконання своїх функцій.

Важливо також враховувати, що кластерна модель забезпечення резильєнтності критичної інфраструктури має бути інтегрована у систему стратегічного планування національного розвитку. Це передбачає адаптацію елементів національної безпекової політики до місцевих реалій через міжгалузеву взаємодію, цифровізацію процесів управління та впровадження Smart-технологій. Зокрема, застосування інтелектуальних систем моніторингу та раннього попередження (наприклад, на базі AI/IoT) дозволяє підвищити точність прогнозування загроз і оперативність реагування.

Окремої уваги потребує вивчення перспектив та розробка механізмів локального залучення місцевого населення до процесу зміцнення резильєнтності. Створення освітніх програм, підвищення обізнаності щодо принципів захисту критичної інфраструктури, впровадження платформ громадської участі є важливими інструментами для побудови культури безпеки на місцевому рівні. Це також сприятиме зміцненню довіри до органів влади і публічно-приватних ініціатив, що, у свою чергу, дозволить подолати ключові бар’єри ефективного функціонування кластерів, зокрема недовіру та фрагментованість рішень. Ще одним стратегічним кроком є формування системи стандартів та індикаторів оцінки резильєнтності, що мають бути уніфікованими на державному рівні та водночас адаптованими до специфіки різних секторів критичної інфраструктури. Це дозволить здійснювати

порівняльний аналіз, аудити готовності об'єктів до кризових ситуацій та розробляти більш точні інвестиційні програми з фокусом на уразливі регіони.

Отже, пристальної уваги законодавчої влади в Україні потребують питання забезпечення резильєнтності критичної інфраструктури, зокрема комплексне удосконалення правової основи захисту критичної інфраструктури, створення системи державного управління її безпекою, налагодження співробітництва між суб'єктами систем безпеки та сил реагування на надзвичайні ситуації, розвиток публічно-приватного партнерства у сфері критичної інфраструктури, розроблення та запровадження механізмів комунікації між державними інститутами, населенням і приватним бізнесом стосовно загроз та ризиків критичній інфраструктурі, розвиток міжнародного співробітництва в цій сфері та посилення вектору превентивного захисту. Реалізація цих завдань в умовах військового стану та військового вторгнення рф передбачає налагодження тісної співпраці і створення дієвих організаційних механізмів на загальнодержавному рівні, а також на регіональному, місцевому та локальному рівнях, що дозволить активізувати превентивне реагування на кризові ситуації та загрози. З цією метою необхідним є ініціалізація постійно функціонуючих форматів комунікації населення, органів державної і місцевої влади, підприємств і організацій. Це є необхідною умовою ескалації ефективності державної політики у сфері захисту та стійкості критичної інфраструктури. Цього можна досягти за рахунок створення кластерів резильєнтності критичної інфраструктури на основі публічно-приватного партнерства, що посилить ефективність та оперативність реагування на деструктивні явища і дозволяють попередити негативні наслідки. Таким чином, кластерна модель забезпечення резильєнтності критичної інфраструктури України виступає перспективним інструментом інтеграції зусиль держави, бізнесу, наукових установ та громадянського суспільства в умовах багаторівневих викликів безпеці. Її запровадження має розпочинатися з територій відновлення, поступово поширюючись на громади сталого розвитку з урахуванням їхнього потенціалу та готовності. Застосування кластерного підходу дозволяє не лише зміцнити систему реагування на надзвичайні ситуації, а й формує передумови для стійкого економічного та соціального розвитку, підвищення інституційної спроможності та зниження вразливості до зовнішніх і внутрішніх загроз. Запровадження таких ініціатив потребує системних правових змін, фінансової підтримки, стратегічного бачення та формування сталої культури безпеки. Інструменти оцінки, зокрема Індекс резильєнтності критичної інфраструктури, дозволяють об'єктивізувати ефективність заходів та визначати пріоритети для подальших інвестицій. У довгостроковій перспективі кластерний підхід може стати базовою моделлю розбудови безпечного середовища в Україні, сприяти зменшенню наслідків майбутніх криз та забезпечити стабільне функціонування критичних систем як у мирний, так і в надзвичайний періоди.

ВИСНОВКИ

Дослідження орієнтоване на розв’язання важливої квестії щодо теоретичного узагальнення особливостей сучасної державної політики у сфері захисту критичної інфраструктури, обґрунтування доктринальних поглядів у фокусі на вдосконалення системи державного управління забезпеченням безпеки об’єктів критичної інфраструктури та генерування науково-практичних рекомендацій.

1. Сучасні умови функціонування підприємств, зокрема критичної інфраструктури, вимагають глибокої трансформації управлінського мислення. Ефективність управління залежить від здатності менеджерів адаптуватися до змін, що потребує відмови від традиційного адміністративного підходу.Продуктивність підприємств визначається не лише економічними показниками, а й соціально-психологічними факторами, зокрема мотивацією персоналу та здатністю до адаптації. Безпекова діяльність розглядається як невід’ємна частина системи управління, що орієнтована на активну протидію загрозам і забезпечення стійкості. Підприємства критичної інфраструктури повинні діяти як відкриті системи, що постійно взаємодіють із зовнішнім середовищем. Синергетичний ефект управління забезпечує підвищену ефективність завдяки узгодженості керуючих і керованих підсистем. Реалізація інформаційної безпеки має здійснюватися на основі міжнародних стандартів, з урахуванням специфіки підприємства. Система менеджменту інформаційної безпеки повинна базуватися на циклі PDCA, забезпечуючи безперервне вдосконалення. В умовах війни особливо актуальним є антикризове управління, яке базується на превентивності, адаптивності й ефективності. Безпековий менеджмент повинен стати самостійним стратегічним інструментом, тісно інтегрованим у загальну систему управління підприємством. Управління безпекою об’єктів критичної інфраструктури набуло системного, міждисциплінарного характеру, що поєднує принципи ризик-менеджменту, цифровізації, концепції сталого розвитку та адаптивного управління. Реалізація системи управління безпекою потребує не лише технічного забезпечення, а й інтеграції соціальних, екологічних і економічних компонентів, що відповідають глобальним цілям сталого розвитку ООН. Застосування підходу SFM дозволяє оптимізувати управлінські процеси на всіх рівнях – стратегічному, тактичному та оперативному – і сприяє довготривалій експлуатаційній надійності об’єктів. Особливу увагу приділено ризик-орієнтованому підходу, який передбачає виявлення, оцінювання та моніторинг потенційних загроз із урахуванням різних типів невизначеностей. Запровадження інноваційних цифрових технологій (BIM, IoT, CAFM, цифрові двійники) значно підвищує ефективність управлінських рішень, забезпечуючи оперативність реагування, точність прогнозування та прозорість процедур. У розрізі сучасних викликів, таких як кліматичні зміни, техногенні загрози й геополітична нестабільність, зростає роль кризового та

антикризового менеджменту, зокрема в умовах війни. Адаптація інфраструктур до змін середовища, підвищення їх енергонезалежності та безпеки персоналу стають пріоритетними напрямами розвитку. Таким чином, ефективне управління безпекою критичної інфраструктури можливе лише за умови поєднання технологічних інновацій, комплексного бачення ризиків, сталого розвитку та мультиакторної взаємодії між усіма зацікавленими сторонами.

2. За результатами аналізу теоретичних підходів до сутності критичної інфраструктури як об'єкту державного управління є опис атрибутів сучасного безпекового середовища, що закладають фундамент цілепокладання державної політики. Серед таких визначено військову агресію рф, міжнародний тероризм, кібертероризм, сепаратизм, зміни клімату та ризик надзвичайних ситуацій, чергова світова гонка озброєнь, пандемія COVID-19. Обґрунтовано горизонт опису критичної інфраструктури у якості складової національної безпеки України, та приналежність її об'єктів до національної інфраструктури. Проаналізовано світовий досвід, наукові підходи вітчизняних учених а також іноземні наукові теоретизування дефініції «критична інфраструктура», що дало підстави запропонувати авторське бачення змістовного наповнення даної дефініції яке ілюструє множинність функціонально пов'язаних елементів національної інфраструктури у їх фізичній, організаційній інформаційно-комунікаційній структурі, що детермінує виконання державою своїх життєво важливих для суспільства функцій. Авторським формулюванням акцентовано увагу на значимості непорушності функціонування об'єктів критичної інфраструктури для здатності державної влади гарантувати національну безпеку й оборону та уникнути людських жертв, значних матеріальних та екологічних збитків, інших драматичних наслідків. Авторське формулювання підкреслює приналежність об'єктів критичної інфраструктури до сфери національної безпеки та акцентується пріоритетність відповідальності за її збереження саме за державою. Окрім цього зазначене визначення відповідатиме принципам системності, цілеспрямованості, множинності галузей та пріоритетної тріади людина-суспільство-держава у відповідності до антропоцентричного підходу та концепції сталого розвитку.

3. За результатами дослідження теоретико-методичних засад забезпечення захисту критичної інфраструктури ідентифіковано спектр загроз для критичної інфраструктури, серед яких військові загрози, диверсійні (розвідувально-підривна діяльність), терористичні, кіберзагрози, економічні загрози, сепаратизм, викрадення державної таємниці, природні та техногенні (надзвичайні ситуації, аварії та технічні збої, кризові ситуації), колаборантні загрози. Поглиблений аналіз дозволив визначити, що фідбеком до загроз слід вважати управлінські рішення в межах державної політики безпеки. Предикат безпеки узагальнено на основі трьох аспектів – концептуального, практичного та ціннісного. Визначено ключові проблемні

питання, серед яких стратегічна необхідність орієнтації державної політики на формування комплексу організаційних, нормативно-правових, інженерно-технічних, експлуатаційних, наукових та державно-партнерських заходів, що сприятимуть забезпеченню безпеки та стійкості критичної інфраструктури; урахування сучасних обставин військового стану в Україні при розробці державної стратегії захисту критичної інфраструктури; значний відсоток приватної власності у структурі об'єктів критичної інфраструктури, що обмежує можливості адміністрування державними інститутами у даній сфері; просторова розпорошеність об'єктів; тривала відсутність централізованої інформаційної платформи для накопичення інформації про об'єкти критичної інфраструктури; обширність суб'єктного складу та нескоординованість режимів функціонування, планів і процедур реагування на різні набори загроз і ризиків у сфері захисту критичної інфраструктури; тривала відсутність на загальнодержавному рівні затвердженого визначення її сутності, відповідної законодавчої бази та тектологічної системи захисту, що б передбачала урівноваженість у одній системі активностей, спротивів і реагування на випадок виникнення надзвичайних ситуацій на об'єктах критичної інфраструктури, а також слабко відпрацьована практика інтерпретації механізму державно-приватного партнерства у сферу захисту критичної інфраструктури; система законодавчих актів одночасно оперує інтенціями «критично важливі об'єкти інфраструктури» та «критична інфраструктура», що в певних умовах викликає протиріччя та породжує інституційну невизначеність. Мова йде про вектор превентивності державної політики щодо виникнення надзвичайних ситуацій на критично-важливих об'єктах та заплановані заходи щодо локалізації та мінімізації негативних наслідків за умов їх виникнення.

Результатом аналізу понятійно-категорійного апарату є авторське формулювання дефініції «захист критичної інфраструктури» як цілеспрямованої синхронізованої спільної діяльності державних інститутів, власників, операторів а також стейкхолдерів об'єктів критичної інфраструктури із застосування комплексу заходів, спрямованих на профілактику, запобігання, своєчасне виявлення потенційних і нейтралізацію реальних загроз, мінімізацію та ліквідацію наслідків і швидке відновлення функціональної спроможності критичної інфраструктури у разі її пошкодження, що реалізовуються з метою уникнення людських жертв, значних матеріальних та екологічних збитків, або інших деструктивних наслідків які можуть призвести до порушення національної безпеки. Даним тлумаченням змінено кут уваги із процесу захисту критичної інфраструктури до процесів профілактики та превенції кризових ситуацій, диференціювавши відповідальність між державою, власниками, безпосередніми працівниками критичних об'єктів, а також їх стейкхолдерів.

4. Проаналізовано сучасні наукові парадигми формування державної політики у сфері захисту критичної інфраструктури з метою наукового переосмислення логіки формування архітектури ключових постулатів

державної політики та чіткої артикуляції ролі держави у сфері захисту критичної інфраструктури. Результатами наукового пошуку у даному векторі стало визначення основних якостей парадигми, серед яких фундаментальність, багатоплановість, конкретність, здатність віддзеркалювати сутнісні характеристики відповідних об'єктів і процесів, системність, певний ступінь усталеності, суб'єктність, прийнятність для більшості вчених, відтворюваність, дієвість, взаємозалежність із об'єктивною дійсністю та ступенем розвитку суспільства, орієнтація на світоглядні підходи, спроможність поступатися новій парадигмі, що з'явилася внаслідок суттєвих змін в науці. Сутність парадигми у контексті безпекознавства розтлумачено як сукупність теоретичних і методологічних передумов, які визначають конкретний напрям наукового дослідження, який втілюється на визначеному етапі історичного розвитку станом, при якому надійно захищено життєво важливі політичні, економічні, соціальні, екологічні, духовні, військові та інші інтереси країни. Науково обґрунтовано, що в основу інституційного цілепокладання заходів державної політики у сфері захисту критичної інфраструктури варто закласти парадигму національного безпекознавства. Визначено, що вона включає в себе аналіз політики, стратегії, загроз і відповідей національної безпеки країни. Ця парадигма досліджує такі питання, як внутрішня та зовнішня загрози, оборонна політика, розвідка, кібербезпека та інші аспекти, що впливають на безпеку країни, що нерозривно пов'язано із сектором критичної інфраструктури, що є детермінантою національної безпеки.

У результаті проведеного аналізу дійшли висновку, що кожен із проаналізованих парадигмальних постулатів несе у собі еклектичний вимір безпекової трансдисциплінарної парадигми, яку пропонується покласти в основу наукового обґрунтування магістральної основи державної політики у сфері захисту критичної інфраструктури. До основних аспектів зазначеної парадигми пропонується включити ліквідацію протиріч у валідності тлумачень основного тезаурусу сфери критичної інфраструктури, симбіоз наукових знань у формотворчому вимірі міждисциплінарної наукової взаємодії, розгляд варіантів процесу формування державної політики захисту критичної інфраструктури поза формалізованими рамками, зокрема у інноваційних формах міжсекторальної взаємодії, комплексну модернізацію правового поля у напрямку ліквідації рудиментарних елементів та інспірації інноваційного забезпечення, актуалізація трансдисциплінарної та поліпарадигмальної моделі державного управління у даному секторі, відношення між системами дисциплінарного знання в процесі інтеграції та диференціації наук, а також як колективні форми роботи вчених різних галузей знання з дослідження процесу формування та реалізації державної політики захисту критичної інфраструктури, заснованих на принципі організації наукового пізнання, за якого відбуватиметься міждисциплінарний реверс, що дозволить генерувати множинність варіантів вирішення комплексу проблем, пов'язаних із безпекою критичної інфраструктури. У

практичній адаптації зазначених імператив, ключовим визначено іррадацію суб'єктного складу захисту критичної інфраструктури за межі усталених державних інститутів на основі розвитку державно-приватного партнерств, моніторинг оперативної інформації стосовно загроз критичній інфраструктурі та розвиток міжнародного співробітництва.

5. Проведений логіко-семантичний аналіз стрижневих компонентів атрибутиву інституційно-правових аспектів державної політики дозволив виявити синергетичну дуальність її ключових тригерів – механізмів державного управління та механізмів правового регулювання. Екстрапольовано трактування інституційно-правового регулювання реалізації державної політики у сфері захисту критичної інфраструктури як систему організаційно-управлінських і правових заходів, що реалізовують інститути державної влади, за допомогою яких реалізується цілеспрямований (з метою максимізації безпеки об'єктів критичної інфраструктури) адміністративний вплив на суспільні відносини орієнтовані на запобігання диференційованим ризикам, загрозам і небезпекам об'єктам критичної інфраструктури основані на тріаді людина-суспільство-держава. Як основа механізму державної політики у сфері захисту критичної інфраструктури розглядається сукупність об'єктивних залежностей і зв'язків між явищами і процесами саморозвитку і саморуху інституційних засобів правової дійсності, що здатний динамічно змінюватися, носити адаптивний характер відповідно до безпекової реальності мікро- та макросередовища, а також глобальної геополітичної ситуації. Проведено скринінг нормативно-правової бази у сфері захисту критичної політики, що формує магістральну основу інституційно-правового механізму державної політики, що дозволило узагальнити спектр основоположних інститутів, які структурують архітектуру безпекової парадигми об'єктів критичної інфраструктури та ідентифіковано їх повноваження у даній сфері. Серед них мова йде про Президента України, Раду національної безпеки та оборони, Кабінет Міністрів України, Верховну Раду України, Функціональні органи у сфері захисту критичної інфраструктури, Секторальні органи у сфері захисту критичної інфраструктури, Уповноважений орган у сфері захисту критичної інфраструктури, Державну службу захисту критичної інфраструктури та забезпечення національної системи стійкості України, операторів критичної інфраструктури. У практичній реалізації архітектури національної безпеки ідентифіковано комплекс автономних державних систем захисту критичної інфраструктури. Розкрито основні завдання державної політики захисту критичної інфраструктури, серед яких розвиток спроможностей суб'єктів забезпечення державної безпеки щодо превентивного комплексу заходів на об'єктах критичної інфраструктури, контррозвідувального режиму, інтенсифікація боротьби з тероризмом та організованою злочинністю, нарощування технологічних можливостей державної безпеки, прийняття на озброєння новітніх систем апаратних

комплексів та спеціальних засобів, підвищення професійного рівня фахівців із забезпечення безпеки, удосконалення нормативно-правового забезпечення, організаційних засад, упровадження дієвих механізмів взаємодії суб'єктів забезпечення державної безпеки із громадянським суспільством, подальший розвиток міжнародного співробітництва в безпековій сфері з питань захисту об'єктів критичної інфраструктури та запровадження національної системи стійкості.

Здійснено аналіз нормативно-правових актів Верховної Ради України, Президента України, Кабінету Міністрів України та інших профільних інститутів України на предмет закріплення принципів вироблення адміністративно-правових засад та структури адміністративно-правового регулювання у сфері державної політики захисту критичної інфраструктури. За рахунок послідовного аналізу встановлено, що за період 2022-2023 року відбулась суттєва модернізація інституційно-правового забезпечення у сфері захисту критичної інфраструктури, яка інспірує еманацію адміністративних заходів реалізовуваних органами державної влади, серед яких відзначено привенційну значимість таких новелизацій, як внесення відомостей про об'єкт критичної інфраструктури до Реєстру об'єктів критичної інфраструктури розроблення та погодження паспорта безпеки на об'єкт критичної інфраструктури, актів оцінки стану захищеності об'єкта критичної інфраструктури, результати моніторингу безпеки об'єктів критичної інфраструктури, ідентифікація проектних загроз та ризиків об'єкта критичної інфраструктури. Реєстр об'єктів критичної інфраструктури дає уявлення про спектр критично важливих інфраструктурних об'єктів та їх характеристики.

6. Науково обґрунтовано підходи до оцінки інституційної спроможності національної системи захисту критичної інфраструктури, що дозволило проаналізувати її рівень у розрізі спроможностей структурних, організаційних, технічних систем та окремих індивідів, що включає розвиток навичок і компетенцій на всіх рівнях провадження державної політики у сфері захисту критичної інфраструктури крізь діоптрій процесних інституцій – правил, процедур, засобів, інструментів, методів, організацій і ресурсів. Інституційна спроможність національної системи захисту критичної інфраструктури ідентифікована як комплементарність внутрішньої системи профільних інститутів та відповідних інституцій, що детермінує їх здатність синхронно забезпечувати захист об'єктів критичної інфраструктури з метою безперебійності їх функціонування. Виокремлено тріаду базових індикаторів інституційної спроможності: внутрішня синхронізація складових інституційної системи, зовнішня комплементарність складових інституційної системи, конгруентність внутрішніх та зовнішніх складових інституційної системи.

Важливим кроком у досягненні інституційної спроможності національної системи захисту критичної інфраструктури визначено реалізацію стратегічного цільового пента-комплексу спроможності:

правову регламентацію діяльності суб'єктів національної системи захисту критичної інфраструктури, створення системи координації та взаємодії суб'єктів національної системи захисту критичної інфраструктури, запровадження управління ризиками критичної інфраструктури, посилення стійкості національної системи захисту критичної інфраструктури, налагодження міжнародної співпраці, а також еманацію архітектури практичної реалізації зазначених заходів. Проведений аналіз показників інституційної спроможності національної системи захисту критичної інфраструктури в Україні дозволив виявити ряд проблемних питань, зокрема: обмеженість наукових досліджень за участю органів публічного управління відповідальних за політику захисту критичної інфраструктури, відсутність у складі освітніх програм управлінських спеціальностей в закладах вищої освіти та спеціалізованих установах підвищення кваліфікації фахових компетентностей, орієнтованих на управління у сфері захисту об'єктів критичної інфраструктури, повільність інформаційного наповнення Реєстру об'єктів китичної інфраструктури та невиконання секторальними органами у сфері захисту критичної інфраструктури завдань з їх ідентифікації та категоризації об'єктів, відсутність компетентного наглядового органу за результативністю державної політики у сфері захисту критичної інфраструктури, не розроблено План врегулювання кризових ситуацій на випадок масштабних кіберінцидентів та аварій на об'єктах критичної інфраструктури, не врегульовано законодавством порядок залучення волонтерів у сферу кібербезпеки та захисту критичної інфраструктури, Збройні Сили України не мають у своєму складі підрозділів кібервійськ та не проводять навчання з кібероперацій або кіберзахисту, не сформовано перелік об'єктів критичної інформаційної інфраструктури, не розроблено дієву модель міжсекторальної співпраці у сфері захисту критичної інфраструктури та залучення стейкхолдерів.

7. Проаналізовано дієвість сучасної парадигми державної політики у сфері захисту критичної інфраструктури в умовах воєнного стану. Це дало підстави констатувати, що сучасна парадигма національного безпекознавства на основі якої структурується архітектура державної політики у сфері захисту критичної інфраструктури розвивається в умовах масштабних змін геополітичних інтересів у сфері перерозподілу територій та світових ресурсів, що у свою чергу, детермінує боротьбу за центри впливу на найбільш важливі об'єкти критичної інфраструктури, що призводить до безпрецедентних фактів порушення територіальної цілісності та інституціональної належності країн із слабкою системою державної політики захисту та обороноздатності. Встановлено, що підходи до вироблення адміністративно-правових основ сучасної політики у сфері захисту критичної інфраструктури реалізується в умовах воєнного стану та безперервної російської військової агресії. Подано дані систематичного порушення ворогом міжнародних нормативно-правових актів, у тому числі й

у сфері захисту критичної інфраструктури, які забороняють піддавати нападу, знищувати чи виводити з ладу об'єкти, необхідні для виживання цивільного населення. Однак встановлено факти та приведено беззаперечні аргументи, що за одну із стратегічних цілей армія країни агресора обрала саме об'єкти критичної інфраструктури міст України, розташовані у глибокому тилу. Їх дестабілізація проводиться у вигляді бойових ударів по атомних електростанціях, електропідстанціях, об'єктах гідроенергетики, теплової генерації, паливо проводах та ін., що призвело до пошкодження та повної руйнації близько тисячі таких об'єктів. Констатовано, що такі дії призводять до розширення загроз за межі локальної безпекової політики. Доведено, що спланованe руйнування об'єктів життєво-важливої інфраструктури з боку країни агресора здійснюється з метою маніпулювання психологічним та моральним станом цивільного населення, формуючи внутрішній страх, намагаючись доповнити цим процес ведення гібридної війни, спрямованої на руйнацію суверенітету та територіальної цілісності України. Проаналізовано ретроспективи формування сучасної парадигми державної політики у сфері захисту критичної інфраструктури та визначено ряд стратегічних прорахунків, які були допущені у безпековій політиці незалежної України, серед яких прийняття без'ядерного статусу, позиції нейтралітету та позаблокового статусу, прихована демілітаризація та штучна деградація обороноздатності суб'єктів системи забезпечення національної безпеки та захисту критичної інфраструктури, трансформація корупції у системоутворюючий чинник державної влади, добровільне підписання «Угоди між Україною і Російською Федерацією про статус та умови перебування воєнної бази Чорноморського флоту Російської Федерації на території України», відсутність чіткого рішення у питаннях розмежування між росією та Україною акваторії Азовського моря та проведення лінії державного кордону в Керченській протоці. Описані факти, на нашу думку, сприяли стратегічному розбалансуванню військових сил у геопросторовому позиціонуванні України як незалежної держави та детермінували формування та ескалацію стратегічних загроз для національної безпеки та критичної інфраструктури країни.

Аналіз сучасних аспектів парадигми державної політики у сфері захисту критичної інфраструктури в умовах правого режиму воєнного стану в Україні, дозволив виявити, що архітектура безпеки критичної інфраструктури побудована на основі чіткої ідентифікації секторів та формуванні реєстру об'єктів критичної інфраструктури, ідентифікації актуальних загроз, формування суб'єктного складу, удосконаленні інституційного забезпечення державної політики у цій сфері, створенні системи захисту об'єктів критичної інфраструктури, вжитті комплексних заходів із подолання наслідків пошкодження та руйнації критичних об'єктів. Отже, на сучасному етапі модернізації сектору безпеки й оборони країни варто актуалізувати необхідність формування на основі синергії існуючих безпекових структур мультиплікованої державної системи захисту критичної

інфраструктури шляхом переходу до високого рівня координації дій та взаємодії зі стейкхолдерами. Обгрунтовано, що дана система має обов'язково включати сектор превентивного та антикризового управління загрозами та ризиками, який відповідатиме пріоритезації предикату стійкості відносно захисту, що пропагує сучасна парадигма безпекознавства у країна ЄС. Однак даного вектору розвитку в рамках сучасної парадигми державної політики у сфері захисту критичної інфраструктури в Україні не зафіксовано.

Проілюстровано алгоритми відпрацювання дій державними інститутами та суб'єктами реагування на кризові ситуації внаслідок набутого досвіду захисту та відновлення об'єктів енергетичної інфраструктури України та модернізованої нормативно-правової бази. У результаті цього узагальнено методичний підхід до розробки концептуальних засад захисту критичної інфраструктури на основі забезпечення стійкості у штатному режимі, режимі готовності та запобігання, режимі реагування та режимі відновлення. У додаток до цього, структуровано формат інтегрованої безпекової моделі критичної інфраструктури, що передбачає в межах чинної нормативної бази, формувати безпеково-ситуаційні моделі у якості фідбеку до моделі проєктної загрози. Остання прогнозується відповідно до спроєктованого портрету порушника безпеки об'єкта та особливостей самого об'єкта із урахуванням потенційного переліку проєктних загроз (військових, терористичних, суспільних, природних, кібернетичних, техногенних, диверсійних та колаборантних). Перелік доповнено «колаборaційними загрозами», які трактовано як небезпеки, що походять від громадян держави, які співпрацюють із ворогом з метою забезпечення реалізації його інтересів та заподіяння шкоди.

8. Концепція безпеки та стійкості критичної інфраструктури засвідчує необхідність переосмислення традиційних підходів до її захисту в умовах зростаючої складності викликів. У сучасному ризиковому середовищі акцент зміщується з виключної протидії загрозам на забезпечення стійкості – здатності інфраструктури функціонувати у кризових умовах, адаптуватися та швидко відновлюватися. Системний і міждисциплінарний підхід до управління критичною інфраструктурою, заснований на принципах ризик-орієнтованого мислення, відкриває нові можливості для підвищення її ефективності та захищеності. Узагальнення сучасних концепцій забезпечення стійкості критичної інфраструктури свідчить про необхідність інтегрованого підходу, який охоплює всі етапи циклу кризового реагування – від запобігання загрозам до повноцінного відновлення функціонування інфраструктур та суспільних процесів. Впровадження систем управління ризиками, операційної стійкості та антикризового менеджменту має вирішальне значення для підтримання безпеки, неперервності ключових функцій та адаптації до нових викликів. Особливої актуальності ці питання набувають у контексті сучасних загроз – як природного, техногенного, так і воєнного характеру. Розвиток сучасного менеджменту у сфері захисту критичної інфраструктури демонструє зсув парадигми від реактивного до

проактивного та адаптивного підходу. У фокусі опиняється не лише технічна досконалість систем, а й людський, організаційний та інституційний фактор, що визначає здатність інфраструктури до стійкого функціонування в умовах постійно змінюваних загроз. Визначальне значення мають концепції адаптивного управління, стратегічного прогнозування, багаторівневого врядування, інтеграції безпеки та антикрихкості як моделі еволюційної переваги в умовах стресу. Запропонований підхід до управління охоплює повний життєвий цикл реагування на кризи та забезпечує сталість функціонування об'єктів інфраструктури шляхом динамічного поєднання ресурсів, технологій, людського потенціалу й міжсекторальної співпраці. Необхідність врахування людського чинника як ключового елементу безпеки особливо актуалізується в контексті зростаючої складності інфраструктурних систем та інтенсивності загроз. Успішність таких підходів значною мірою залежить від стратегічного бачення, підтримки інституційного середовища, гнучкості управлінських структур та готовності до інновацій. Таким чином, стійкість критичної інфраструктури розглядається як інтегральна властивість, що вимагає системного, комплексного та науково обґрунтованого підходу до управління. Формування випереджальної адаптації, здатної до навчання, гнучкості та інституційної стійкості, є основою безпеки держави в умовах сучасних та майбутніх викликів.

9. Аналіз особливостей іноземної практики реалізації ефективної державної політики у сфері захисту критичної інфраструктури дав підстави зробити висновок, що Україна запозичила досвід американської моделі, опираючись також на досвід ЄС. Також виділено ряд особливостей у іноземній практиці: розвиток освіти та науки у напрямку підготовки спеціалістів у сфері захисту критичної інфраструктури; інформаційний реверс між стейкхолдерами безпеки та стійкості об'єктів критичної інфраструктури, у напрямку акумуляції дієвого досвіду протидії загрозам та ризикам, створення та підтримки зручних систем комунікації; ідентифікація стейкхолдерів захисту об'єктів критичної інфраструктури у сфері приватного бізнесу та розвиток відносин на основі державно-приватного партнерства та кластеризації; політика у сфері захисту критичної інфраструктури більшості країн орієнтована на розвиток потенціалу інвестиційної активності; розробка активних державних стратегії управління ризиками для критичної інфраструктури, що передбачає домінування превентивного захисту.

Встановлено, що сучасна українська парадигма державної політики у сфері захисту критичної інфраструктури розвивається крізь призму положень нової Директиви ЄС 2557 (Директива CER) що сфокусовані на забезпеченні стійкості, а не захисту об'єктів критичної інфраструктури. Зміна акценту пояснюється неможливістю досягнути бездоганної захищеності інфраструктури в умовах активної фази війни, тобто потрібно сфокусувати зусилля на забезпеченні можливостей швидкої регенерації втрачених потужностей у разі надзвичайної деструктивної ситуації. Із проведеного аналізу закордонного досвіду визначено, що спільним знаменником

державної політики у даному напрямку є вектор орієнтований на забезпечення стійкості критичної інфраструктури, що трактується як тристадійний процес антикризового управління, орієнтований на превентивність дій із забезпечення тріади варіантив стійкості: соціальної, організаційної та технологічної. Зазначені складові формують «трикутник стійкості», що є базовим індикатором для оцінки ефективності державної політики захисту критичної інфраструктури. Досягнення стійкості об'єктами критичної інфраструктури детермінує здатність протидіяти, адаптуватися, регенерувати спроможність після потенційно руйнівної події та навчатися на основі аналізу допущених помилок. Така здатність дозволяє запобігати, протистояти, пом'якшувати, абсорбувати, пристосовуватися та відновлюватися після інциденту, який порушує або може порушити роботу критично важливого об'єкта. На основі результатів оціночного огляду закордонного досвіду у сфері державної політики, узагальнено концептуальні положення вектору посилення стійкості критичної інфраструктури на загальнодержавному і регіональному рівнях за рахунок удосконалення політичної та інституційно-правової бази, розвиток кадрового потенціалу, перегляду секторів критичної інфраструктури, інтегрована оцінка ризиків та загроз, моделювання, оперативного планування та розробки сценаріїв дій, посилення ресурсного забезпечення, забезпечення міжсекторальної координації та співпраці, а також створення партнерств зі стейкхолдерами.

У результаті аналізу та порівняння із закордонним досвідом, варто підкреслити унікальність української політики у сфері захисту критичної інфраструктури, що полягає у її адаптивності та еластичності. Це дозволило під час повномасштабного вторгнення рф продемонструвати можливості до оперативного вдосконалення відповідно до новітніх загроз та кооперуватися для посилення національної безпеки. Подальші кроки з її розвитку на національному рівні мають узгоджуватись із розвитком законодавства ЄС в цій сфері.

10. Запропоновано напрями інституційних перетворень у векторі підвищення ефективності державної політики захисту критичної інфраструктури, основоположними із яких вбачається розвиток її поліінституціональності, що передбачає залучення до її реалізації стейкхолдерів об'єктів критичної інфраструктури, без яких неможливо ефективне вирішення кризових ситуацій. Даний феномен передбачає активну участь у формуванні й реалізації державної політики та безпекових заходів у сфері захисту критичної інфраструктури приватного сектору, власників і операторів об'єктів критичних об'єктів, державних урядових установ, місцевого самоврядування, неурядових організацій, секторальних агентств, та науково-дослідних установ і освітніх закладів. Цей процес дозволить посилити інноваційність у розробках безпечних і стійких технологій, а також ефективізацію та скоординованість програм на всіх рівнях управління.

У напрямку забезпечення захисту критичної інфраструктури з позиції

сучасної міжнародної практики, пропонується у якості розширеної альтернативи предикату «стійкість критичної інфраструктури» інтегрувати у сферу державної політики термін «резильєнтність критичної інфраструктури», що трактується як здатність об'єктів критичної інфраструктури протидіяти гібридним загрозам, за рахунок забезпечення посилення здатності країни, суспільства, органів державної влади та об'єктів критичної інфраструктури реалізувати ефективний комплекс заходів, націлених на забезпечення готовності, запобігання, протистояння ризикам та загрозам надзвичайних ситуацій, швидкого відновлення нормального функціонування об'єктів від їх наслідків, а також постійного удосконалення компетентностей персоналу, засвоєння досвіду та залучення приватних інвестицій. Базові атрибути резильєнтності включають «аналіз ризиків/загроз», «передбачення/підготовку», «проходження/витримку», «реагування/ відновлення» та «адаптацію/навчання» та імплікують інституційні трансформації систем захисту крізь призму ресурсних системних детермінант, серед яких визначено фізичний захист і оборону, кіберзахист і оборону, превентивні заходи захисту й оборони та освітньо-науковий підхід. Особливо підкреслено необхідність методологічної дифузії науково-освітнього забезпечення у сферу державної політики захисту критичної інфраструктри з метою досягнення її резильєнтності. Із цією метою запропоновано внести зміни до чинного Класифікатора професій та Стандарту вищої освіти України спеціальностей 281 Публічне управління та адміністрування (D4 – Публічне управління та адміністрування) та 073 Менеджмент (D3 – Менеджмент) в частині доповнення фахових компетентностей орієнтованих на управлінське забезпечення національної системи захисту об'єктів критичної інфраструктури, що дозволить посилити інституційну спроможність у цій сфері.

11. Подано авторські концептуальні пропозиції, що передбачають наочну репрезентацію удосконалення державних механізмів реалізації політики захисту критичної інфраструктури України в умовах воєнного стану, магістральною віхою у даному векторі наукового пошуку стало обґрунтування пропозиції щодо інституційного закріплення механізму колективного підходу до захисту критичної інфраструктури. Запропоновано інноваційну ідею концепції кластерного підходу до забезпечення резильєнтності критичної інфраструктури в умовах воєнного стану в Україні на основі створення «кластерів резильєнтності критичної інфраструктури» (КРКІ), що пропагує ідею створення навколо важливих інфраструктурних об'єктів унікальних інтеграційних об'єднань, спроможних забезпечити синергію безпекових заходів реалізованих в межах співпраці державних інститутів влади, систем захисту та реагування, самих інфраструктурних об'єктів та їх стейкхолдерів. Основними індикаторами зазначених структур визначено інноваційність, географічну близькість, автономність учасників та їх спільний інтерес. Інфраструктурні об'єкти в даному проєкті позиціонуються як тригери формування конкурентних переваг учасників

кластера, що імплікує їм статус «стейкхолдерів». Для створення умов комплексної реалізації моделі кластерного підходу запропоновано інтегрувати у сферу державної політики термін «публічно-приватне партнерство», як систему законодавчо врегульованих і юридично оформлених відносин між органами державної влади, органами місцевого самоврядування, приватним бізнесом (юридичними та фізичними особами), громадськими організаціями для вирішення суспільно значущих проблем на довготривалий період часу, заснованих на узгодженні інтересів і взаємній зацікавленості в досягненні намічених цілей, на довірі і таких, що передбачають добровільне об'єднання ресурсів, спільне ухвалення рішень, раціональний розподіл ризиків і спільну відповідальність за результати на основі договору про спільну діяльність. Розпочати апробацію зазначених ініціатив вбачається доцільним на територіях повоєнного відновлення. Вимірність резильєнтності об'єктів критичної інфраструктури проілюстровано у вигляді «трикутника вразливості» об'єкта критичної інфраструктури, що ілюструє обсяг втрати продуктивності та час необхідний на його відновлення, що залежить від превентивних заходів проведених на об'єкті. Таким чином, чим менша площа даного трикутника, тим резильєнтнішою є інфраструктура. Складові описаного «трикутника вразливості» можуть бути компенсовані тріадою відповідних детермінант резильєнтності – протидія (превентивний захист), адаптація та відновлення. На основі запропонованої гіпотези, з метою можливості оцінки досягнутої резильєнтності критичної інфраструктури в межах кластерної моделі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Азаров С. І., Сидоренко В.Л., Єременко С.А., Пруський А.В., Демків А.М Захист критичної інфраструктури в умовах надзвичайних ситуацій: монографія. за заг. ред. П.Б. Волянського. Київ, 2021. 375 с.
2. Антикризовий механізм сталого розвитку підприємства / за ред. проф. Перерви П. Г., проф. Товажнянського Л. Л.: монографія. Харків, 2012. 705 с.
3. Бараннік В. О. Щодо сприяння розвитку регіональних кластерів в Україні. Національний інститут стратегічних досліджень. 2021. URL: https://niss.gov.ua/sites/default/files/2021-08/klustery.pdf
4. Бевз С. І. Поняття та елементи механізму адміністративно-правового регулювання державного управління господарською діяльністю. Прикарпатський юридичний вісник. Випуск 4(25) том 2, 2018. С. 43-47
5. Бєлай С. В., Євтушенко І. В., Мацюк В. В. Теоретико-методологічні засади підготовки кадрів у сфері захисту критичної інфраструктури України. Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2021. Вип. 2. С. 342-350
6. 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
7. Бжезінський З. К. Україна та Європа. Національна безпека і оборона. 2000. № 7. С. 11-15
8. Бірюков Д. С. Захист критичної інфраструктури в Україні: від наукового осмислення до розробки засад політики. Науково-інформаційний вісник Академії національної безпеки. 2015. № 3-4. С. 155-170.
9. Бірюков Д.С., Кондратов С.І. Стратегія захисту критичної інфраструктури в системі національної безпеки держави. Стратегічні пріоритети. 2012. № 3(24). С. 107–113
10. Бірюков Д.С., Кондратов С.І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. К.: НІСД, 2012. 96 с
11. Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. Стратегічні пріоритети. Серія: Економіка. 2015. № 4. С. 83-93.
12. Бобро Д. Г. Удосконалення методології ранжування об'єктів критичної інфраструктури та їх віднесення до критичної інфраструктури: аналіт. зап. URL:http://www.niss.gov.ua/content/articles/files/krutuchna_infra-a7636.pdf,
13. Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України: аналіт. доп. за заг. ред. О. М. Суходолі. К.: НІСД, 2019. 224 с.
14. Бобро Д. Г. Проектна загроза та паспорти безпеки як ключові елементи системи захисту критичної інфраструктури. URL: https://niss.gov.ua/sites/default/files/2018-07/Presentation_Bobro.pdf
15. Богуцький П. П. Концептуальні засади права національної безпеки

України: монографія. Київ – Одеса: Фенікс, 2020. 376 с.

16. Богуцький П. П. Військово-правова парадигма взаємодії громадянського суспільства та сектору безпеки і оборони. Взаємодія громадянського суспільства з сектором безпеки і оборони: сучасні виклики : тези доп. учасників наук.-практ. конф. (Харків, 21 груд. 2021 р.), С. 9-12.

17. Валіхновський Р. Підходи щодо побудови гуманітарної парадигми забезпечення національної безпеки. Вісник Національної академії державного управління при Президентові України. 2010. № 1. С. 243-253.

18. Велика українська енциклопедія. Державна наукова установа «Енциклопедичне видавництво». URL: https://vue.gov.ua/

19. Великий енциклопедичний юридичний словник. За ред. акад. НАН України Ю.С. Шемшученка. 2-е вид., переробл. і доповн. К.: Вид-во «Юридична думка», 2012. 1020 с.

20. Великий тлумачний словник сучасної української мови . Укл. і гол. ред. В.Т. Бусел. К.: Ірпінь: ВТФ «Перун», 2005. 1728 с.

21. Верголяс О. О. Реформування системи захисту та підвищення стійкості критичної інфраструктури України в розрізі актуальних загроз. URL: https://coolyanews.info.html

22. Вітлінський В. В., Великоіваненко Г. І. Ризикологія в економіці та підприємництві: монографія. К.: КНЕУ, 2004. 480 с.

23. Войтовський К. Щодо розроблення планів забезпечення організаційної стійкості. Національний інститут стратегічних досліджень. URL: https://niss.gov.ua/sites/default/files/2023-02/az_planuvannya-org-stiykosti_24022023.pdf

24. Герасименко П. В. Небезпечний нейтралітет. URL: https://zaxid.net/nebezpechniy_neytralitet_n1541767

25. Гладиш М. Еволюція безпекової парадигми скандинавських держав протягом XX століття. Вісник Львівського університету. Серія: Міжнародні відносини. 2019. Вип. 46. С. 27-36.

26. Гладка О. В. Передумови реалізації адміністративноправової доктрини людино центризму. Адміністративне та інформаційне право. 2017. № 1(3). С.64-73.

27. Гнатюк С. О., Рябий М. О., Лядовська В. М. Визначення критичної інформаційної інфраструктури та її захисту: аналіз підходів. Зв'язок. 2014. № 4. С. 3-7.

28. Гнатюк С. О., Сєйлова Н. А., Сидоренко В. М. Універсальна модель даних для формування переліку об'єктів критичної інформаційної інфраструктури держави. Ukrainian Scientific Journal of Information Security, 2017. vol. 23. issue 2. P. 80–91.

29. Гольцов А .Г. Геостратегія України щодо Російської Федерації. Вісник НТУУ «КПІ». Політологія. Соціологія. Право: збірник наукових праць. 2023. № 1 (57). С. 71-77.

30. Гончар М. Ф. Системи стрес-менеджменту на підприємствах: формування, використання та моделювання: монографія. Львів: Видавництво

Львівської політехніки, 2018. 272 с.

31. Гуцалюк О.М., Бондар Ю.А. Безпековий менеджмент авіаційного транспорту в контексті сталого розвитку національної економіки. Управління економікою: теорія та практика: зб. наук. пр. Київ: ІЄП НАНУ, 2020. С. 82-94

32. Декларація про державний суверенітет України. Документ № 55-XII від 16.07.1990 р. URL: https://zakon.rada.gov.ua/laws/show/55-12#Text

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

34. Дєєва Н. Е., Хмурова В. В. Публічно-приватне партнерство: інтереси зацікавлених сторін. Економіка України. 2018. № 9(682). С. 99-111.

35. Директива Європейського Парламенту і Ради (ЄС) «Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» № 2016/1148 від 06.07.2016 р. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text

36. Директива Ради ЄС «Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту» № 2008/114/ЄС від 08.12.2008 р. URL: https://zakon.rada.gov.ua/laws/show/984_002-08#Text

37. Дмитренко О. А. Інституційна спроможність неурядових організацій в Україні: фінансовий аспект. Науковий часопис НПУ ім. М. П. Драгоманова. 2020. Вип. 28. С. 48 55.

38. ДСТУ ISO Guide 73:2013. Керування ризиком. Словник термінів (ISO Guide 73:2009, IDT). URL: https://khoda.gov.ua/image/catalog/files/dstu%2073.pdf

39. Додатковий протокол до Женевських конвенцій від 12.08.1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 08.06.1977 р. URL: https://zakon.rada.gov.ua/laws/show/995_199#Text

40. 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

41. Домбровська С. М. Механізми забезпечення державної соціальної безпеки в Україні. Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія». Серія: Державне управління. 2015. Т. 254, Вип. 242. С. 28-32.

42. Добиш Т. Є. Теорія антикрихкості в економіці: як країни стають сильнішими через кризи. Актуальні соціально-економічні проблеми в умовах невизначеності: матеріали Всеукраїнської науково-практичної конференції молодих вчених, 18 квітня 2025 р.. Нац. ун-т "Києво-Могилянська академія", Кафедра економічної теорії. Київ : НаУКМА, 2025. С. 44-46..

43. Дранишников Л. В., Сугаль Є. О. Оцінка зовнішнього ризику за допомогою нечіткої логіки. Математичне моделювання. 2017. № 2. С. 63-66.

44. Енциклопедія державного управління: у 8 томах. Нац. акад. держ. упр. при Президентові України. Київ: НАДУ, 2011. Т. 2. С. 13-17.

45. Євсєєв В. О. Можливі шляхи удосконалення захисту критичної інфраструктури України з урахуванням світового досвіду. Збірник наукових праць ХНУПС. 2016. № 4. С. 168-172

46. Єрменчук О. П. Нормативно-правове регулювання діяльності у сфері захисту національної критичної інфраструктури: аналіз та узагальнення нормотворчої практики США. Науковий вісник ДДУВС. 2017. № 3. С. 135-140.

47. Єрменчук О. П. Складові національної інфраструктури. Науковий вісник ДДУВС. 2017. № 4. С. 109-115.

48. Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монограф. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.

49. Заболотний А.В. Юник І.Г. Організаційно-правові аспекти проходження публічної служби та виконання посадових обов'язків на об'єктах критичної інфраструктури в умовах правового режиму воєнного стану в Україні. Інвестиції, практика та досвід. №8. 2024. URL: https://www.nayka.com.ua/index.php/investplan/article/view/3602/3637

50. Закон України No2980-IX від 20.03.2023 р. «Про одноразову грошову допомогу за шкоду життю та здоров'ю, завдану працівникам об'єктів критичної інфраструктури, державним службовцям, посадовим особам місцевого самоврядування внаслідок військової агресії Російської Федерації проти України». URL: https://zakon.rada.gov.ua/laws/show/2980-20/ed20230-320#Text

51. Закон України «Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України» № 2684-IX від 18.10.2022 р. URL: https://zakon.rada.gov.ua/laws/show/2684-20#Text

52. Закон України «Про боротьбу з тероризмом» №638-IV від 20.03.2003 р. URL: https://zakon.rada.gov.ua/laws/show/638-15/ed20030320#Text

53. Закон України «Про військово-цивільні адміністрації» № 141-VIII від 03.02.2015 р. URL: https://zakon.rada.gov.ua/laws/show/141-19#Text

54. Закон України «Про внесення змін до деяких законодавчих актів України щодо засад державної регіональної політики та політики відновлення регіонів і територій» №2389-IX від 09.07.2022 р. URL: https://zakon.rada.gov.ua/laws/show/2389-20#Text

55. Закон України «Про державно-приватне партнерство». № 2404-VI від 01.07.2010 р. URL: https://zakon.rada.gov.ua/laws/show/2404-17/ed20230903

56. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» № 3475-IV від 31.03.2023 р. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text

57. Закон України «Про Державну службу» № 889-VIII від 10.12.2015 р. URL: https://zakon.rada.gov.ua/laws/show/889-19#Text

58. Закон України «Про засади внутрішньої і зовнішньої політики» № 2411-VI від 01.07.2010 р. URL: https://zakon.rada.gov.ua/laws/show/2411-

17#Text

59. Закон України «Про Кабінет Міністрів України» № 794-VII від 03.08.2023 р. URL: https://zakon.rada.gov.ua/laws/show/794-18#Text

60. Закон України «Про критичну інфраструктуру» № 1882-IX від 05.12.2022 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

61. Закон України «Про місцеве самоврядування в Україні» № 280/97-ВР від 21.05.1997 р. URL: http://zakon4.rada.gov.ua/laws/show/280/97-вр/page#Text

62. Закон України «Про національну безпеку України» № 2469-VIII від 31.03.2023 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

63. Закон України «Про Національну систему конфіденційного зв'язку» від 10.01.2002 № 2919-III. URL: https://zakon.rada.gov.ua/laws/show/2919-14/ed20220101#Text

64. Закон України «Про об'єкти підвищеної небезпеки» від 18.01.2001 №2245-III. URL: https://zakon.rada.gov.ua/laws/show/2245-14#Text

65. Закон України «Про органи самоорганізації населення» http://zakon4.rada.gov.ua/laws/show/2625-14

66. Закон України «Про основи національного спротиву» № 1702-IX від 03.08.2023 р. URL: https://zakon.rada.gov.ua/laws/show/1702-20#Text

67. Закон України «Про основи національної безпеки України» від 19.06.2003 № 964-IV. URL: https://zakon.rada.gov.ua/laws/show/964-15#Text (втратив чинність на підставі Закону № 2469-VIII від 21.06.2018)

68. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19/ed20220817#Text

69. Закон України «Про охорону культурної спадщини» від 08.06.2000 № 1805-III. URL: https://zakon.rada.gov.ua/laws/show/1805-14#Text

70. Закон України «Про платіжні системи та переказ коштів в Україні» від 05.04.2001 № 2346-III. URL: https://zakon.rada.gov.ua/laws/show/2346-14#Text

71. Закон України «Про правовий режим воєнного стану» № 389-VIII від 19.10.2023 р. https://zakon.rada.gov.ua/laws/show/389-19#Text

72. Закон України «Про Раду національної безпеки і оборони України» № 183/98-ВР від 29.07.2023 р. URL: https://zakon.rada.gov.ua/laws/show/183/98 вр#Text

73. Закон України «Про систему екстреної допомоги населенню за єдиним телефонним номером 112» від 13.03.2012 № 4499-VI. URL: https://zakon.rada.gov.ua/laws/show/4499-17#Text

74. Закон України «Про стимулювання розвитку регіонів» № 2850-IV від від 08.09.2005 р. URL: https://zakon.rada.gov.ua/laws/show/2850-15#Text

75. Закон України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» № 2064-III від 16.10.2022 р. URL: https://zakon.rada.gov.ua/laws/show/2064-14#Text

76. Залознова Ю. С., Бутенко Н. В., Петрова І. П. Публічно-приватне

партнерство в Україні: стан, проблеми та перспективи розвитку. Економічний вісник Донбасу. 2016. № 2. С. 21-28

77. Звіт про виконання у 2019 році Стратегії реформування державного управління України. URL: https://www.kmu.gov.ua/storage/app/sites/1/zviti-pro-vikonannya/par-report-ukr-web.pdf

78. Звіт про відстеження результативності постанови КМУ «Деякі питання об'єктів критичної інфраструктури» № 1109 від 09.10.2020 р. за підсумками 2022 р. URL: https://cip.gov.ua/ua/news/zvit-pro-povtorne-vidstezhennya-rezultativnosti-postanovi-kabinetu-ministriv-ukrayini-vid-09-zhovtnya-2020-r-1109-deyaki-pitannya-ob-yektiv-kritichnoyi-infrastrukturi

79. Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар. експерт. нарад. Упоряд. Д.С. Бірюков, С.І Кондратов ; за заг. ред. О.М.Суходолі. К.: НІСД, 2016. 176 с

80. Зубко Г. Ю. Система суб'єктів реалізації державної інфраструктурної політики України. Правові новели. 2020. № 11. С. 166-178.

81. Зубар І. В. Операційний менеджмент у забезпеченні сталого розвитку підприємств. Успіхи і досягнення у науці. 2024. № 9. С. 549-558.

82. Зубко Г. Ю. Адміністративно-правові засади формування переліку об'єктів критичної інфраструктури. Держава та регіони. Серія «Право». 2020. № 3(69). Т. 2. С. 36-42.

83. Зубко Г. Ю. Державна інфраструктурна політика України: адміністративно-правові засади регулювання: монографія. Херсон: Видавничий дім «Гельветика», 2020. 412 с.

84. Зубко Г. Ю. Публічно-приватне партнерство у сфері безпеки стратегічної інфраструктури України. Юридичний науковий електронний журнал. 2020. № 2. Т. 2. С. 13-17.

85. Зубко Г. Ю. Система суб'єктів реалізації державної інфраструктурної політики України. Правові новели. 2020. № 11. С. 166-178.

86. Зубко Г. Ю. Сучасні підходи до визначення поняття державної інфраструктурної політики. Науковий вісник Міжнародного гуманітарного університету. Серія «Юриспруденція». 2020. № 48. С. 78-84.

87. Інституціоналізація публічного управління в Україні: наук.-аналіт. доп. за заг. ред. М. М. Білинської, О. М. Петроє. Київ: НАДУ, 2019. 210 с.

88. Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT). Київ: Мінекономрозвитку України, 2015. 74 с.

89. Ігнатієва І. А. Стратегічний менеджмент: теорія, методологія, практика: монографія. Київ : Знання України, 2005. 250 с.

90. Кодекс цивільного захисту України. від 03.04.2022 № 5403-VI. URL: https://zakon.rada.gov.ua/laws/show/5403-17#Text

91. Кодекс цивільного захисту України: Закон України № 5403-VI від 05.10.2023 р. URL: https://zakon.rada.gov.ua/laws/show/5403-17#Text

92. Козловський С. В. Управління сучасними економічними системами, їх розвитком та стійкістю: монографія. В.: Меркьюрі-Поділля, 2010. 432 с.

93. Колпаков В. К., Кузьменко О. В. Нелегальна міграція: генезис і

механізм протидії: монографія. Д: «Наука і освіта», 2002. 371 с.

94. Кондратенко О. Ю. Геоекономічний вимір гібридної війни Російської Федерації проти України. Вісник Київського національного університету імені Тараса Шевченка. Міжнародні відносини. № 2(50). 2019. С.12-19

95. Кондратов С. І., Суходоля О. М. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналіт. доп. за ред. Суходолі. Київ: НІСД, 2020. 28 с.

96. Конституція України: Закон України № 254к/96-ВР від 01.01.2020 р. URL: https://zakon.rada.gov.ua/laws/show/ 254к/96-вр#Text

97. Королюк Н. О., Першин О. В., Грідньова Т. О., Шевченко С. О. Обґрунтування сучасного підходу щодо автоматизації процесів прийняття рішень по управлінню авіацією. Збірник наукових праць Харківського національного університету Повітряних Сил. 2019. №1(59). С. 32-39.

98. Кочетков О. В., Гаур Т. О., Машін В. М. Система оцінки ризиків інформаційної безпеки підприємства на основі нечіткої логіки. Наукові праці ОНАЗ ім. О. С. Попова. 2019. № 1. С. 97-104.

99. Кримінальний кодекс України: Закон України № 341-III від 05.10.2023 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

100. Криштанович М. Ф., Пушак Я. Я., Флейчук М. І., Франчук В. І. Державна політика забезпечення національної безпеки України: основні напрямки та особливості здійснення: монографія. Львів: Сполом, 2020. 418 с

101. Крук С. І. Аналіз стану організаційно-правових механізмів державного управління у сфері забезпечення національної безпеки України. Інвестиції: практика та досвід. 2018. № 20. С. 76 78.

102. Крук С. І. Інституційний і правовий механізми державного управління у сфері забезпечення національної безпеки України. Публічне управління та митне адміністрування. 2018. № 2 (19). С.70-73.

103. Кузмін О. Є., Мельник О. Г., Адамів М. Є. Антисипативне управління підприємствами: процесно-структурований підхід. Економіка: реалії часу. 2012. № 2 (3). С. 71–77

104. Культура безпеки. Серія видань по безпеці. № 75-INSAG-4. Доповідь Міжнародної консультативної групи з ядерної безпеки. Вена: МАГАТЕ, 1991. URL: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub882r_web.pdf

105. Кульчій І. М. Публічно-приватне партнерство як спосіб забезпечення сталого розвитку сільських територій. Проблеми законності: зб. наук. пр. 2017. Вип. 138. С. 99-108.

106. Лазор О.Я., Заболотний А.В., Зубар І.В. Роль критичної інфраструктури у забезпеченні державної політики продовольчої безпеки в Україні. Актуальні питання у сучасній науці. №4 (20). 393-409.

107. Лазор О.Я., Юник І.Г. Перспективи розвитку державно-приватного партнерства у сфері захисту критичної інфраструктури в Україні. Наукові перспективи. №4. 2024. С.246-258

108. Лазор О.Я., Юник І.Г., Заболотний А.В. Державна стратегія повоєнного відновлення та розвитку критичної інфраструктури в Україні. Державне управління: удосконалення та розвиток. №4. 2024. URL: https://doi.org/10.32702/2307-2156.2024.4.2

109. Лазор О. Я., Лазор О. Д. Публічне управління та адміністрування: ретроспектива деяких теоретичних аспектів. Університетські наукові записки. 2015. № 4. С. 111-121

110. Ліпкан В. А. Теорія національної безпеки. 2009. Київ: КНТ. 576

111. Ліпкан В. А. Безпекознавство: Навчальний посібник. К.: Вид-во Європейського університету, 2003. 208 с.

112. Ліпкан В. А., Зубко Г. Ю. Інфраструктурні стратегії: формування нового концепту. Юридичний бюлетень. 2020. № 17. С. 13-20.

113. Ліпкан В. А. Геостратегія сучасної української держави: засади формування Вісник Львівського університету. Серія філос.-політолог. студії. 2022. Вип. 42, с. 268-277.

114. Лойко В. В., Храпкіна В. В., Маляр С. А., Руденко М. В. Economic and legal principles of ensuring the protection of critical infrastructure. Фінансово-кредитна діяльність: проблеми теорії та практики. 2020. № 4 (35). С. 426-238

115. Маркіна І. А. Основи формування системи менеджменту інформаційної безпеки підприємства / І. А. Маркіна, Д. В. Дячков // Проблеми і перспективи розвитку підприємництва. 2016. № 3(1). С. 80-88.

116. Мельник Р. С. Концепція людиноцентризму у сучасній доктрині адміністративного права. Юридичний журнал «Право України». 2015. №10. 157-165.

117. Меморандум про гарантії безпеки у зв'язку з приєднанням України до Договору про нерозповсюдження ядерної зброї. Закон України №998 від 05.12.1994 р. URL: https://zakon.rada.gov.ua/laws/show/998_158#Text

118. Мусієнко В. О., Зінченко М. Е. Технологія ризик-менеджменту як елемент системи забезпечення економічної безпеки суб'єкта господарювання. Економічний вісник Дніпровської політехніки. 2020. № 3. С. 98-108.

119. Мушникова С. А. Побудова поліпарадигмальної моделі ієрархії стратегій управління безпекою розвитку підприємства. Проблеми системного підходу в економіці. 2020. Вип. 1 (75). Ч. 1. С. 130–136.

120. Мушникова С. А. Трансдисциплінарна парадигма й інноваційні трансформації економічного середовища як фундаментальна основа управління безпекою розвитку металургійних підприємств. Бізнес Інформ. 2020. № 4. С. 446-452.

121. Надолішній П. І., Піроженко Н. В. Публічно-приватне партнерство в Україні: теоретикометодологічні засади і умови інституціалізації. Теоретичні та прикладні питання державотворення: зб. наук. пр. 2012. Вип. 10. С. 1 7-52.

122. Назаров М. С. Соціальна стійкість на рівні територіальних громад в

умовах сучасних викликів. Науковий журнал «Політикус». №2. 2022. С.54-59

123. Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України «Про затвердження Змін до Положення про територіальний орган Адміністрації Державної служби спеціального зв'язку та захисту інформації України» № 467 від 31.05.2023 р. URL: https://zakon.rada.gov.ua/laws/show/z1124-23#Text

124. Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України «Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури» № 23 від 15.01.2021 р. URL: https://zakon.rada.gov.ua/rada/show/v0023519-21#Text

125. Наказ Адміністрації Держспецзв'язку «Про затвердження Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» № 94 від 10.01.2023 р. URL: https://zakon.rada.gov.ua/laws/show/z0603-08#Text

126. Наказ Адміністрації Держспецзв'язку «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» № 660 від 10.01.2023 р. URL: https://zakon.rada.gov.ua/laws/show/z0090-15#Text

127. Наказ Адміністрації Держспецзв'язку «Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті» № 20 від 15.01.2016 р. URL: https://zakon.rada.gov.ua/laws/show/z0196-16#Text

128. Наказ Міністерства енергетики України «Про Вимоги з кібербезпеки паливно-енергетичного сектору критичної інфраструктури» № 417 від 15.12.2022 р. URL: https://zakon.rada.gov.ua/laws/show/z0249-23#Text

129. Наказ МОН України «Про затвердження Стандарту вищої освіти України другого (магістерського) рівня вищої освіти ступеня «магістр» за спеціальністю 281 Публічне управління та адміністрування» № 1001 від 04.08.2020 р. URL: https://mon.gov.ua/ua/npa/pro-zatverdzhennya-standartu-vishoyi-osviti-za-specialnistyu-281-publichne-upravlinnya-ta-administruvannya-dlya-drugogo-magisterskogo-rivnya-vishoyi-osviti

130. Наказ МОН України «Про затвердження Стандарту вищої освіти України першого (бакалаврського) рівня вищої освіти ступеня «бакалавр» за спеціальністю 281 Публічне управління та адміністрування» № 1172 від 29.10.2018 р. URL: https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/12/21/281-Publ.upr.ta.administruvannya-bakalavr.21.01.22.pdf

131. Національна парадигма сталого розвитку України. за заг. ред.

академіка НАН України, д.т.н., проф., засл. діяча науки і техніки України Б. Є. Патона. К.: Державна установа "Інститут економіки природокористування та сталого розвитку Національної академії наук України", 2012. 72 с..

132. Національний класифікатор України. Класифікатор професій ДК 003:2010. URL: https://zakon.rada.gov.ua/rada/show/va327609-10#Text

133. Наше спільне майбутнє: Доповідь Міжнародної комісії з навколишнього середовища та розвитку. URL: http://www.un.org/ru/ga/pdf/brundtland.pdf

134. Нестерова М. А. Трансдисциплінарність когнітивістики. Нова парадигма. 2014. № 123. С. 42–49.

135. Нестор О. Ю. Публічно-приватне партнерство: сутність, особливості та проблеми розвитку на тлі пандемії COVID-19. Соціально-економічні проблеми сучасного періоду України: зб. наук. пр. 2021. Вип. 2(148). С. 58-68

136. Ніколаюк С. І., Радченко Р. А. Використання можливостей нечіткої логіки для алгоритмізації дій оперативних працівників під час виявлення та фіксації злочинів. Юридичний часопис Національної академії внутрішніх справ. 2015. № 1. С. 280-293.

137. Носов О. Ю., Черничко Т. В. Нормативно-правове регулювання кластеризації в Україні. Науковий вісник Мукачівського державного університету. Серія «Економіка». Вип. 1(11). С.21-27.

138. Овчарук В. В. Сутність адміністрування на підприємствах. Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство. 2018. Вип. 19(2). С. 115-118.

139. Олизаренко С. А., Перепелица А. В., Капранов В. А. Интервальные нечеткие множества типа 2. Терминология, представление, операции. Системи обробки інформації. Х.: ХУПС, 2011. Вип. 2(92). С. 39-45.

140. Омаров Ш. А. Теоретичні засади формування стратегії сталого розвитку регіонів України. Вісник Чернігівського державного технологічного університету. 2014. № 3 (75). С. 149 157

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

142. Офіціальний веб-сайт The Department of Homeland Security. URL: https://www.dhs.gov/

143. Офіційний веб сайт Єврпейської комісії. URL: https://commission.europa.eu/index_en

144. Офіційний веб-сайт Centre for the Protection of National Infrastructure. URL: http://www.cpni.gov.uk/

145. Офіційний веб-сайт European Cluster for Securing Critical Infrastructures. URL: https://www.finsec-project.eu/ecsci

146. Офіційний веб-сайт European Commission’s Joint Research Centre.

URL: https://joint-research-centre.ec.europa.eu/index_en

147. Офіційний веб-сайт Information Sharing and Analysis Centers. URL: https://www.enisa.europa.eu/

148. Офіційний веб-сайт KSE Institute. URL: https://kse.ua/ua/

149. Офіційний веб-сайт National Cybersecurity and Communications Integration Center. URL: https://www.cisa.gov/

150. Офіційний веб-сайт National Infrastructure Simulation and Analysis Center. URL: https://www.cisa.gov/.

151. Офіційний веб-сайт Nederlands Instituut Publieke Veiligheid. URL: https://nipv.nl/

152. Офіційний веб-сайт Real Estate Information Sharing and Analysis Center. URL: https://www.reisac.org/

153. Офіційний веб-сайт Rządowe Centrum Bezpieczeństwa. URL: https://www.gov.pl/web/rcb/o-rcb2

154. Офіційний веб-сайт Serwis Rzeczypospolitej Polskiej. URL: https://www.gov.pl/

155. Офіційний веб-сайт The Cybersecurity and Infrastructure Security Agency. URL: https://www.cisa.gov/

156. Офіційний веб-сайт US-CERT. URL: https://www.us-cert.gov/

157. Офіційний веб-сайт Академія електронного урядування Естонії (eGA). URL: https://ega.ee/

158. Офіційний веб-сайт Департаменту національної безпеки США. URL: https://www.dhs.gov/

159. Офіційний веб-сайт Державної служби спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua

160. Офіційний веб-сайт Європейського кластеру безпеки критичних інфраструктур. URL: https://www.finsec-project.eu/ecsci

161. Офіційний веб-сайт Збройних Сил України. URL: https://www.zsu.gov.ua/

162. Офіційний веб-сайт Комп'ютерної аварійної служби України CERT-UA. URL: https://cert.gov.ua/

163. Офіційний веб-сайт Конгресу США. Report to Congress of the U.S.-China Economic and Security Review Commission. November 12, ss 127-189. URL: https://www.uscc.gov

164. Офіційний веб-сайт Міністерства внутрішньої безпеки США: DHS Lexicon Terms and Definitions. URL: https://www.dhs.gov/

165. Офіційний веб-сайт Міністерства енергетики України URL: https://www.mev.gov.ua/

166. Офіційний веб-сайт Міністерство захисту довкілля та природних ресурсів URL: https://mepr.gov.ua/

167. Офіційний веб-сайт Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг https://www.nerc.gov.ua/

168. Офіційний веб-сайт Національного агентства України з питань

державної служби. URL: https://nads.gov.ua/

169. Офіційний веб-сайт Національного інституту стратегічних досліджень (НІСД). URL: https://niss.gov.ua/

170. Офіційний веб-сайт Національного Кластеру Кібербезпеки. URL: https://cybersecuritycluster.org.ua/

171. Офіційний веб-сайт НБУ. URL: https://bank.gov.ua/

172. Офіційний веб-сайт ООН. URL: https://www.un.org/ru/

173. Офіційний веб-сайт Програми розвитку ООН в Україні (United Nations Development Programme). URL: https://www.undp.org

174. Офіційний веб-сайт Світового банку. URL: https://www.worldbank.org/

175. Офіційний веб-сайт Служби безпеки України URL: https://ssu.gov.ua/antyterorystychnyi-tsentr-pry-ssu

176. Офіційний веб-сайт Уряду Великобританії. URL: https://www.gov.uk/

177. Офіційний веб-сайт Федерального відомства інформаційної безпеки Німеччини. URL: https://www.bsi.bund.de/

178. Офіційний веб-сайт. Office of Science and Technology Policy. URL: https://www.whitehouse.gov/ostp/

179. Павлов Д. М., Микитюк М. А. Правові та організаційні засади забезпечення захисту критичної інфраструктури у контексті формування нової безпекової парадигми України. Честь і закон. 2020. № 4. С. 69-77.

180. Павлов Д. М. Організаційно-правові засади реформування системи цивільного захисту України у контексті зміни безпекової парадигми. Evropský politický a právní diskurz. 2015. Sv. 2 Vyd. 5. C. 145-149.

181. Панченко К. Механізм державно-приватного партнерства потрібно адаптувати до залучення інвестицій на відбудову зруйнованої інфраструктури. Українська правда. 2022. URL: https://www.epravda.com.ua/columns/2022/07/19/689341/

182. Пасічник В. М. Філософська категорія безпеки як основа нової парадигми державного управління національною безпекою. Демократичне врядування. 2011. Вип. 7. URL: http://nbuv.gov.ua/UJRN/DeVr_2011_7_7

183. Петрашко І. Р. Аналіз регуляторного впливу проекту Закону України «Про критичну інфраструктуру та її захист». URL: https://www.drs.gov.ua/wp-content/uploads/2020/07/5854-ob.pdf

184. Петренко К. Особливості інституційної спроможності громадських об’єднань в Україні. Наукові записки Інституту політичних і етнонаціональних досліджень ім.. І.Ф. Кураса НАН України. 2015. Випуск 4 (78). С. 376-388, с. 377

185. Пирожков С. І., Божок Є. В., Хамітов Н. В. Національна стійкість (резильєнтність) країни: стратегія і тактика випередження гібридних загроз. Вісник Національної академії наук України. 2021. № 8. С. 74–82.

186. Пирожков С. І., Хамітов Н. В. Цивілізаційний проект України: від амбіцій до реальних можливостей. Вісник Національної академії наук

України. 2016. № 6. С. 45–52.

187. Пілько А. Д. Гарда Т. П. Соціально-економічний розвиток регіону: пошук нових орієнтирів та механізмів реалізації в контексті еволюції безпекознавчих парадигм. Бізнес Інформ. 2016. № 10. С. 112-116.

188. Пілько А. Д. Управління територіальною системою: еволюція безпекознавчої парадигми. Моделювання регіональної економіки. 2012. № 2. С. 332-340

189. Політологічний енциклопедичний словник. упоряд. В. П. Горбатенко. - 2-е вид., доп. і перероб. Київ : Генеза, 2004. С. 47

190. Посохов І. М. Аналіз змісту поняття ризик і наукові підходи щодо визначення сутності ризику. Вісник Нац. техн. ун-ту "ХПІ" : зб. наук. пр. Темат. вип.: Технічний прогрес та ефективність виробництва. Харків: НТУ "ХПІ", 2012. № 5. С. 101-108.

191. Постанова КМУ «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» № 1295 від 23.12.2020 р. URL: https://zakon.rada.gov.ua/laws/show/1295-2020- п#Text

192. Постанова КМУ «Деякі питання об’єктів критичної інформаційної інфраструктури» № 943 від 09.10.2020 р. URL: https://zakon.rada.gov.ua/laws/show/943-2020-п#Text

193. Постанова КМУ «Деякі питання об’єктів критичної інфраструктури» № 1109 від 09.10.2020 р.. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-п#Text

194. Постанова КМУ «Деякі питання організації здійснення державно-приватного партнерства» № 384 від 11.04.2011 р. URL: https://zakon.rada.gov.ua/laws/show/384-2011-п#n274

195. Постанова КМУ «Деякі питання паспортизації об’єктів критичної інфраструктури» № 818 від 04.08.2023 р. URL: https://zakon.rada.gov.ua/laws/show/818-2023-п#Text

196. Постанова КМУ «Деякі питання подання інформації у сфері захисту критичної інфраструктури» № 1175 від 14.10.2022 р. URL: https://zakon.rada.gov.ua/laws/show/1175-2022-п#Text

197. Постанова КМУ «Деякі питання проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури» № 257 від 24.03.2023 р. URL: https://zakon.rada.gov.ua/laws/show/257-2023- п#Text

198. Постанова КМУ «Про внесення змін до переліку секторів критичної інфраструктури» № 455 від 09.05.2023 р. URL: https://zakon.rada.gov.ua/laws/show/455-2023- п#Text

199. Постанова КМУ «Про внесення змін до Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України» № 167 від 24.02.2023 р. URL: https://zakon.rada.gov.ua/laws/show/167-2023-п#Text

200. Постанова КМУ «Про внесення змін до Порядку проведення аналізу ефективності здійснення державно-приватного партнерства» № 294

від 22.04.2020 р. URL: https://zakon.rada.gov.ua/laws/show/294-2020-п#Text

201. Постанова КМУ «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» № 518 від 19.06.2019 р. URL:https://zakon.rada.gov.ua/laws/show/518-2019 п#Text

202. Постанова КМУ «Про затвердження категорій об'єктів державної форми власності та сфер державного регулювання, які підлягають охороні органами поліції охорони на договірних засадах» від 21.10.2018 № 975. URL: https://zakon.rada.gov.ua/laws/show/975-2018-п#Text

203. Постанова КМУ «Про затвердження Переліку об'єктів, які підлягають охороні і обороні в умовах надзвичайних ситуацій і в особливий період»: від 24.04.1999 № 675-019. Кабінет Міністрів України. (для службового користування)

204. Постанова КМУ «Про затвердження переліку особливо важливих об'єктів електроенергетики, у тому числі територій забороненої зони та контрольованої зони гідротехнічних споруд, які підлягають охороні відомчою воєнізованою охороною» від 04.07.2018 № 575. URL: https://zakon.rada.gov.ua/laws/show/575-2018-п#n15

205. Постанова КМУ «Про затвердження переліку підприємств, що мають стратегічне значення для економіки та безпеки держави» від 04.03.2015 № 83. URL: https://zakon.rada.gov.ua/laws/show/83-2015-п#Text

206. Постанова КМУ «Про затвердження Положення про єдину державну систему цивільного захисту» № 11 від 09.01.2014 р. URL: https://zakon.rada.gov.ua/laws/show/11-2014-п#Text

207. Постанова КМУ «Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього» № 415 від 28.04.2023 р. URL: https://zakon.rada.gov.ua/laws/show/415-2023-п#Text

208. Постанова КМУ «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних системах» № 1772 від 07.09.2022 р. URL: https://zakon.rada.gov.ua/laws/show/1772-2002-п#Text

209. Постанова КМУ «Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури» № 821 від 22.07.2022 р. URL: https://zakon.rada.gov.ua/laws/show/821-2022- п#Text

210. Постанова КМУ «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» № 563 від 23.08.2016 р. URL: https://zakon.rada.gov.ua/laws/show/563-2016- п#Text

211. Постанова КМУ «Про затвердження Порядку функціонування державної системи фізичного захисту» № 1337 від 30.08.2022 р. URL: https://zakon.rada.gov.ua/laws/show/1337-2011- п#Text

212. Постанова КМУ «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» № 373 від 29.03.2006 р. URL:

https://zakon.rada.gov.ua/laws/show/1772-2002-п#Text

213. Постанова КМУ «Про затвердження Правил техногенної безпеки у сфері цивільного захисту на підприємствах, в організаціях, установах та на небезпечних територіях» від 15.08.2007 № 1051. Кабінет Міністрів України. (для службового користування).

214. Постанова КМУ «Про затвердження Програми діяльності Кабінету Міністрів України» № 471 від 12.06.2020 р. URL: https://zakon.rada.gov.ua/laws/show/471-2020-п#Text

215. Постанова КМУ «Про затвердження Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури» № 1174 від 14.10.2022 р. URL: https://zakon.rada.gov.ua/laws/show/1174-2022- п#Text

216. Постанова КМУ «Про реалізацію статті 85 Закону України «Про відновлення платоспроможності боржника або визнання його банкрутом»» від 15.05.2013 № 339. URL: https://zakon.rada.gov.ua/laws/show/339-2013-%D0%BF#Text (втратила чинність на підставі Постанови КМ № 664 від 24.07.2019)

217. Постанова КМУ «Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України» № 787 від 12.07.2022 р. URL: https://zakon.rada.gov.ua/laws/show/787-2022- п#Text

218. Постанова Національної комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг «Щодо захисту інформації, яка в умовах воєнного стану може бути віднесена до інформації з обмеженим доступом, у тому числі щодо об'єктів критичної інфраструктури» №349 від 26.03.2022 р. URL: https://zakon.rada.gov.ua/rada/show/v0349874-22#Text

219. Постанова Правління НБУ «Про затвердження Положення про визначення об'єктів критичної інфраструктури в банківській системі України» № 151 від 30.11.2020 р. URL: https://zakon.rada.gov.ua/laws/show/v0151500-20#Text

220. Постельжук О. П., Валюх Л. І., Невинна Г. Я., Михальчук Р. Ю. Транснаціональна злочинність і національна безпека: необхідність зміни безпекової парадигми України. Інвестиції: практика та досвід. 2021. № 22. С. 107-113.

221. Потеряйко С. П. Бєлікова К. Г., Твердохліб О. С. Теоретико-методологічне обгрунтування моделі визначення критерію безпеки населення на основі прогнозу функціонування єдиної державної системи цивільного захисту. Інвестиції: практика та досвід. 2021. № 18. С. 40-48.

222. Резнікова О. О., Войтовський К. Є. Лепіхов А. В. Організація системи забезпечення національної стійкості на регіональному і місце вому рівнях : аналіт. доп.; за заг. ред. О. О. Резнікової. Київ: НІСД, 2021. 140 с.

223. Резнікова О. О. Щодо Концепції забезпечення національної стійкості. Аналіт. записка. Серія „Національна безпека". 2020. № 8. С. 1–8.

224. Резнікова О. О. Національна стійкість в умовах мінливого безпекового середовища: монографія. Київ: НІСД, 2022. 456 с.

225. Ризикологія в економіці та підприємництві: монографія. В. В.Вітлінський, Г. І. Великоіваненко. К.: КНЕУ, 2004. 480 с.

226. Рішення РНБО України «Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України» від 01.03.2014 р.URL: https://zakon.rada.gov.ua/laws/show/n0001525-14#Text

227. Розпорядження КМУ «Деякі питання реформування державного управління України». № 831-р від 21.07.2021 р URL: https://zakon.rada.gov.ua/laws/show/831-2021-р#Text

228. Розпорядження КМУ «Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури» № 825-р від 19.09.2023 р. URL: https://zakon.rada.gov.ua/laws/show/825-2023-р#Text

229. Розпорядження КМУ «Про затвердження переліку особливо важливих об’єктів нафтогазової галузі» від 27.05.2009 № 578-р. URL: https://zakon.rada.gov.ua/laws/show/578-2009-р#Text

230. Розпорядження КМУ «Про схвалення Концепції створення державної системи захисту критичної інфраструктури» № 1009-р від 06.12.2017 р. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-п#Text

231. Розпорядженням КМУ «Про затвердження плану пріоритетних дій Уряду на 2023 рік» № 221-р від 14.03.2023 р. URL: https://zakon.rada.gov.ua/laws/show/221-2023- р#Text

232. Рось О. Г. Поняття та сутність нормативно-правового забезпечення інституційної спроможності представницьких органів місцевого самоврядування. Інвестиції: практика та досвід. 2019. № 18. С. 97-100.

233. Рудич Ф. М. Становлення суспільно-політичного устрою в сучасній Україні: політологічний аналіз. Шляхи виходу із кризи. Наукові записки Інституту політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України. 2016. Вип. 5-6. С. 63-88.

234. Садовський М. В. Правові механізми демілітаризації міністерства оборони України, як засіб оборонної реформи та елемент реформування сектору безпеки Юридичний вісник. № 3 (60). 2021. С. 117-121.

235. Синиченко А. В. Сучасна парадигма менеджменту організацій в умовах трансформаційних перебудов. Економіка та суспільство. Випуск 46. 2022. https://economyandsociety.in.ua/index.php/journal/article/view/2084/2012

236. Ситник Г. Інституційно-цивілізаційна парадигма дослідження проблем та державно-управлінських аспектів забезпечення національної безпеки. Вісник Національної академії державного управління при Президентові України. 2011. Вип. 2. С. 25-34.

237. Скопенко Н. С., Євсєєва-Северина І. В. Ризик-менеджмент як необхідна складова системи економічної безпеки виробничих підприємств. Наукові праці Національного університету харчових технологій. 2020. Т. 26,

№ 2. С. 120-129.

238. Словник іншомовних слів. за ред. О. С. Мельничука. К: Голов. ред. УРЕ АН УРСР, 1975. 768 с

239. Соболєв В. М., Соболєва М. В. Інституційна спроможність системи вищої освіти та чинники її забезпечення. Проблеми економіки № 2 (48), 2021. С.63-69.

240. Стратегія національної безпеки України «Україна у світі, що змінюється» URL: https://zakon.rada.gov.ua/laws/show/105/2007 (втратила чинність на підставі Указу Президента № 287/2015 від 26.05.2015)

241. Страхніцький Я. О. Інституційні перетворення у напрямку підвищення ефективності державної політики захисту критичної інфраструктури. Публічне управління та регіональний розвиток. №1 (23) 2024.

242. Страхніцький Я. О. Особливості державної політики захисту критичної інфраструктури в Україні та напрями її удосконалення в умовах війни. Knowledge, Education, Law, Management 2022 № 7 (51). С.104-111.

243. Страхніцький Я. О. Особливості сучасної системи захисту критичної інфраструктури в Україні. Наука, освіта, технології та суспільство: актуальні проблеми теорії та практики: збірник тез доповідей міжнародної науково-практичної конференції (Полтава, 25 травня 2022 р.): у 2 ч. Полтава: ЦФЕНД, 2022. Ч. 1. 63 с.

244. Страхніцький Я. О. Структурно-функціональна характеристика державної політики у сфері захисту критичної інфраструктури в Україні. Публічне управління та митне адміністрування, № 4 (35), 2022. С. 112-117

245. Страхніцький Я. О. Формування наукової парадигми державної політики у сфері захисту критичної інфраструктури. Тези доповідей IX Міжнародної науково-практичної конференції «Управління інноваційним процесом в Україні: напрями розвитку» (м. Львів, 19-21 травня 2022 р.). Львів: Видавництво Львівської політехніки, 2022. URL: https://science.lpnu.ua/mipu/abstracts-2022

246. Страхніцький Я. О. Структурно-функціональна характеристика системи захисту критичної інфраструктури в Україні. Публічне управління та митне адміністрування, № 4 (35), 2022. С.112-117.

247. Страхніцький Я.О. Державна політика у сфері захисту критичної інфраструктури в умовах воєнного стану в Україні. Сучасна парадигма публічного управління: Збірник тез IV Міжнародної науково-практичної конференції (10-12 листопада 2022р.) / За наук. ред. к.е.н., доцента Стасишина А.В. Львів : ЛНУ імені Івана Франка, Львів, 2022. 958 с.

248. Страхніцький Я. О. Кластерний підхід до забезпечення захисту критичної інфраструктури в умовах воєнного стану в Україні. Інвестиції: практика та досвід. № 23. 2023. С. 163-169.

249. Страхніцький Я. О. Концептуальні засади забезпечення резильєнтності об’єктів критичної інфраструктури в умовах гібридних загроз. Глобальні тенденції та національні особливості публічного управління та

адміністрування. Матеріали круглого столу «Глобальні тенденції та національні особливості публічного управління та адміністрування» (м. Вінниця 22 грудня 2023 р.) Вінниця: Вінницький державний педагогічний університет імені Михайла Коцюбинського, 2023. 112 с.

250. Суспільно-політичні процеси. Науково-популярне видання громадської організації «Академія політичних наук». К., 2017. № 2–3. 308 с.

251. Суходоля О. М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. Стратегічні пріоритети. 2016. № 3. С. 62-76.

252. Суходоля О. М. Захист критичної інфраструктури: сучасні виклики та пріоритетні завдання сектору безпеки. Науковий часопис Академії національної безпеки. 2017. № 1-2. С. 50-80.

253. Суходоля О. М. Стійкість енергетичної системи чи стійкість енергозабезпечення споживачів: постановка проблеми. Стратегічні пріоритети. 2018. № 2. С. 101–117.

254. Суходоля О. М. Стійкість критичної енергетичної інфраструктури та життєдіяльності громад : аналіт. доп. Київ : НІСД, 2024. – 160 с.

255. Суходоля О. М. Стійкість здійснення життєво важливих функцій: узагальнення досвіду реагування України на руйнування енергетичної інфраструктури. URL: https://niss.gov.ua/sites/default/files/2023-07/az-dosvid-stiykosti-oes-2_20072023.pdf

256. Теленик С. С. Досвід правового регулювання системи захисту критичної інфраструктури в США. Науковий вісник НАВС. 2018. № 2 (107). С. 358–370.

257. Теленик С. С. Державна система захисту критичної інфраструктури України: концептуальні засади адміністративно-правового регулювання: монографія. Одеса: Видавничий дім «Гельветика», 2020. 602 с.

258. Теленик С. С. Критична інфраструктура як об`єкт адміністративно-правового регулювання. Юридичний часопис Національної академії внутрішніх справ. 2018. № 1 (15). С. 179–189

259. Теленик С. С. Державна система захисту критичної інфраструктури України: концептуальні засади адміністративно-правового регулювання: монографія. Одеса : Видавничий дім «Гельветика», 2020. 602 с.

260. Третьяков О.В., Халмурадов Б.Д., Кічата Н.М., Ремська А.В. Підхід до кількісної оцінки стійкості об’єктів критичної інфраструктури. Системи управління, навігації та зв’язку. 2025. Т1. № 79. С. 178-183.

261. Тертичка В. В. Державна політика: аналіз та здійснення в Україні. К.: Вид-во Соломії Павличко «Основи». 2002. 750 с.

262. Тристороння заява Президентів України, США та Росії. Закон України № 998 від 14.01.1994 р. URL:https://zakon.rada.gov.ua/laws/show/998_300#Text

263. Тундаєв С. М. Поняття та сутність інституційної спроможності правоохоронних органів України щодо протидії діяльності злочинних спільнот та осіб, що перебувають у статусі підвищеного злочинного впливу.

Юридичний науковий електронний журнал. 2022. № 11. С. 684-689

264. Угода між Україною і Російською Федерацією про статус та умови перебування Чорноморського флоту Російської Федерації на території України №643-076 від 20.10.2010 р. URL: https://zakon.rada.gov.ua/laws/show/643_076#Text

265. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14.09.2020 р. «Про Стратегію національної безпеки України» № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020

266. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 06.05.2015 р. «Про Стратегію національної безпеки України» № 287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text

267. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки»» № 56/2022 від 16.02.2022 р. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text

268. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави» № 446 від 26.08.2021 р. URL: https://zakon.rada.gov.ua/laws/show/446/2021#Text

269. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»» № 96/2016. від 15.03.2016 р. URL: https://www.rnbo.gov.ua/ua/Ukazy/417.html?PRINT.

270. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про Стратегічний оборонний бюлетень України» №473/2021 від 17.09.2021 р. URL: https://zakon.rada.gov.ua/laws/show/473/2021#n2

271. Указ Президента України Про рішення Ради національної безпеки і оборони України від 17 жовтня 2023 року «Про організацію захисту та забезпечення безпеки функціонування об'єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій» № 695/2023 від 17.10.2023 р. URL: https://www.president.gov.ua/documents/6952023-48641

272. Франчук, В. І. Теоретико-методологічні та управлінські засади розвитку безпекового середовища. Науковий вісник Львівського державного університету внутрішніх справ (серія економічна). 2023. (2), 63–73.

273. Фадєєва І. Г. Гринюк О. І. Нечітка логіка як інструмент ризик-контролінгу в контексті проактивного управління нафтогазовидобувними підприємствами. Бізнес Інформ. 2019. № 4. С. 212-220.

274. Хаустова В. Є. Омаров Ш. А. Концепція сталого розвитку як парадигма розвитку суспільства. Проблеми економіки. 2018. № 1. С. 265-273.

275. Хитра О. Л. Реагування на кризові ситуації, що загрожую національній безпеці України: адміністративно-правові засади реалізації теорії та досвіду: монографія. Львів: Растр-7, 2019. 398 с.

276. Цивільний кодекс України. Закон України № 435-IV від

16.01.2003 р. URL: https://zakon.rada.gov.ua/laws/show/435-15/ed20030116#Text

277. Цюрупа М. В. Зміна парадигм воєнно-політичного мислення у доктринах та стратегіях воєнної безпеки України XX XXI ст.. Українознавчий альманах. 2021. Вип. 28. С. 120-126.

278. Чалий В. О. Нейтралітет для України – це пастка, адже ми на кордоні з рф. URL: https://hromadske.radio/podcasts/ukraina-vholos/neytralitet-na-kordoni-z-rf-nichoho-ne-zabezpechuie-tse-pastka-chalyy

279. Чумаченко С. М., Троцько В. В. Оцінювання загроз об'єктам критичної інфраструктури. Науковий вісник: цивільний захист та пожежна безпека. 2017. № 1. С. 41-47.

280. Шатун В. Т. Позаблоковий статус держави та українські реалії. Південня правда. 2015. URL: http://www.up.mk.ua/mainpage/show_item/4024

281. Шемшученко Ю. С., Бобровник С. В. Правове регулювання. Юридична енциклопедія: в 6 т. Київ, 2003. Т. 5. П С. С. 40-41.

282. Шарапов В. Формування концепції антикризового менеджменту в умовах воєнного часу. Humanities studies. 2023. Вип. 14. С. 196-207.

283. Шевцова Г. З. Синергетичний менеджмент підприємств: моногр. НАН України, Ін-т економіки пром-сті. Київ, 2016. 454 с.

284. Швиденко Г. О. Система управління інфраструктурою підприємства. Проблеми економіки. 2013. No 2. С. 153–159

285. Яременко О. І., Страхніцький Я. О. Теоретико-методичні основи забезпечення системи захисту критичної інфраструктури держави. Державне управління: удосконалення та розвиток. № 1. 2022. URL: http://www.dy.nayka.com.ua/?op=1&z=2610

286. Яременко О. І., Страхніцький Я. О. Теоретичні підходи до визначення дефініції критичної інфраструктури як об'єкту державного управління. Публічне управління та митне адміністрування. №1 (32). С 76-82.

287. Bhatt G. D. (2000) A resource-based perspective of developing organizational capabilities for business transformation. Knowledge and process management. Vol. 7. № 2. P. 119-129.

288. Bruneau, M, Chang, SE, Eguchi, RT, et al. (2003). A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. Earthquake Spectra. 19(4), 733-752

289. Cantelmi R., Gravio G., Patriarca R. (2021) Reviewing qualitative research approaches in the context of critical infrastructure resilience. Environment Systems and Decisions 41(3) pp. 1-36.

290. Carrillo-Hermosilla J., Unruh G. C. (2006). Technology Stability and Change: An Integrated Evolutionary Approach. Journal of Economic Issues. vol 3. pp. 707-742

291. Cenuşa, D. (2023) Ukraine's critical infrastructure vs. Russia's energy positioning - the «war of nerves». Analysis by Dionis Cenuşa. URL:https://www.ipn.md/en/ukraines-critical-infrastructure-vs-russias-energy-positioning-the-7978_1093693.html#ixzz8GikIr7Au

292. Commission of the European Communities (2005), Green Paper on a European programme for critical infrastructure protection. URL: https://www.ab.gov.tr/files/ardb/evt/1_avrupa_birligi/1_6_raporlar/1_2_green_papers/com2005_green_paper_on_critical_infrastructure.pdf.

293. Communication from the commission on a European Programme for Critical Infrastructure Protection. Commission of the European Communities Brussels, 12.12.2006. COM (2006) 786 final. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786: FIN:EN:PD

294. Coombs T. W. (2021) Ongoing Crisis Communication: Planning, Managing, and Responding, SAGE Publications, 304 p.

295. Council Directive 2008/114/EC of 08.12.2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. URL: http://eur-lex.europa. eu/]

296. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance). URL: http://data.europa.eu/eli/dir/2008/114/oj

297. Critical infrastructure protection. An official website of the European Union. URL: https://joint-research-centre.ec.europa.eu/scientific-activities-z/critical-infrastructure-protection

298. Critical Infrastructure Resilience – 2023: collection of materials of the scientific and practical conference, Kyiv, June 21, 2023, PIMEE of NAS of Ukraine. 2023. 109 p. (Мохора В.В., Коробейнікова Ф.О.)

299. Cyber-Sicherheitsstrategie für Deutschland. Bundesministerium des Innern. Berlin, 2016. URL: https://www.bmi. bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf

300. Department of Homeland Security (2013), Presidential Policy Directive. Critical Infrastructure Security and Resilience. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

301. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557

302. Electricity Information Sharing and Analysis Center. URL: https://www.eisac.com/

303. EMP/GMD. The Science and Technology Directorate. URL: https://www.dhs.gov/

304. European Commission. Guidance Document on Indicators of Public Administration Capacity Building, June 2014, p. 3. URL: https:ec.europa.eu/social/BlobServlet?docId=14144

305. Em El-Koursi, Subhabrata Mitra G. Bearfield Harmonising Safety Management Systemsin the European Railway Sector Safety Science Monitor, I P S O Australia. 2018. Vol. 11 (Is. 2). 14 p.

306. Fekete A., Rhuner J. (2020) Sustainable Digital Transformation of Disaster Risk-Integrating New Types of Digital Social Vulnerability and Interdependencies with Critical Infrastructure. Sustainability. №12(22). pp. 1-18.

307. Foreign Investment Risk Review Modernization Act of 2018. Src.1702.Findings;Sense of Congress. (b) Sense of Congress. (5). URL: https://www.treasury.gov/resourcecenter/international/Documents/Summary-offirrma.pdf

308. Freeman, E. (1984), Strategic Management: A stakeholder approach. Boston: Pitman, 266 p. URL: http://bookre.org/reader?file=1164948&pg=6

309. German Strategy for Adaptation to Climate Change. The Federal Government. URL: https://www.preventionweb.net/files/27772_dasgesamtenbf1-63.pdf

310. Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) URL: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/BSI-Gesetz/bsi-gesetz_node.html

311. Guidance notes on building critical infrastructure resilience in Europe and Central Asia. UNDP 2022. URL: https://www.undp.org/eurasia/publications/guidance-notes-building-critical-infrastructure-resilience-europe-and-central-asia

312. Guide 73:2009, IDT. Київ: Мін.економ.розвитку України, 2014. ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT). Київ: Мінекономрозвитку України, 2015. 74 с

313. Her Majesty the Queen in Right of Canada (2009) National Strategy for Critical Infrastructure. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf

314. Hereinafter, the Directives adopted by President Bush and Obama are cited by: National Security Presidential Directives. George Bush Administration; The official website of the Federation of American Scientists. URL: https://fas.org/irp/offdocs/nspd/index.html

315. Improving Critical Infrastructure Cybersecurity. Executive Order №13636 of February 12, 2013. URL: https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

316. Infrastructure Investment and Jobs Act. Public Law №: 117-58. URL: https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf

317. ISO 22316:2017 Security and resilience – Organizational resilience – Principles and attributes https://www.iso.org/obp/ui/#iso:std:iso:22316:ed-1:v1:en

318. Josse, E., Dubois, V. (2009). Interventions humanitaires en santé mentale dans les violences de masse (1st edition) Bruxelles: Groupe De Boeck. p. 301

319. Kaminska V., Namazova Yu., Strakhnitskyi Y. Public administration mechanisms of formation and implementation of state policy in the field of youth protection. Modern Science -Moderní věda. 2022. №1, pp. 41-49.

320. Krajowego Planu Zarządzania Kryzysowego

https://www.gov.pl/web/rcb/krajowy-plan-zarzadzania-kryzysowego

321. Kubiak M. Kwestie bezpieczenstwa w europejskiej mysli filozoficznej. Wojsko i wychowanie. 2001. № 6. S. 51-55

322. Kuhn. T.S. The Structure of Scientific Revolutions. Chicago, 1962; M., 1975

323. Livre Blanc sur la défense et la sécurité nationale, 2013. Офіційний вебсайт уряду Франції: https://www.gouvernement.fr/en/white-paper-on-defense-and-national-security-2013

324. Merton, R.K. (1968) Social Theory and Structure. London: The Free Press of Glencoe, Collier- MacMillan Limited. P. 22-216.

325. MITRE. Cyber Resiliency Engineering Framework. Deborah J. Bodeau & Richard Graubart. https://www.mitre.org/sites/default/files/media/publicat2.pdf

326. Modernization of the system of public management and administration in Ukraine: the experience of the Republic of Latvia: SECTION 5. Features of the current state policy in the sphere of protection of critical infrastructure in the conditions of war in Ukraine (Strahnitskyi Ya. O.). Scientific monograph. Riga, Latvia : "Baltija Publishing", 2023. 232 p

327. Mu S., Cheng H., Chohr M., and Peng W. (2014) Assessing riskmanagement capability of contractors in subway projects in mainland China. International Journal of Project Management. vol.32. pp. 452–460,

328. Narodowy Program Ochrony Infrastruktury Krytycznej. URL: https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej

329. National Infrastructure Protection Plan – NIPP 2013: Partnering for Critical Infrastructure Security and Resilience. URL: https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf

330. National Risk Assessments: A Cross Country Perspective The evolving practice of National Risk Assessments in OECD countries. URL: https://read.oecd-ilibrary.org/governance/national-risk-assessments/the-evolving-practice-of-national-risk-assessments-in-oecd-countries_9789264287532-3-en#page1

331. National Strategy for Critical Infrastructure Protection (CIP Strategy). URL: https://www.kritis.bund.de

332. National strategy for homeland security. Office of homeland security. July 2002. URL: https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf

333. National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. URL: https://georgewbush-whitehouse.archives.gov/pcipb/physical.html

334. Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) BMI, 2009. URL: http://www.kritis.bund.de

335. NIST Special Publication 800-160. Vol. 2. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach URL: https://nvlpubs.nist.gov/nistpubs/Special Publications/NIST.SP.800-160v2r1.pdf 2.

336. Peters B. G. (2000) Institutional Theory: Problems and Prospects.

Political Science Series. 18 p. URL: https://www.ihs.ac.at/publications/pol/pw_69.pdf

337. Posen B. R. The Security Dilemma and Ethnic Conflict. Survival. Spring 1993. Vol 35. № 1. P. 28.

338. Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

339. Public Management Reviews. Towards an Integrated Public Service. OECD. Ireland. 2008. 377 P. DOI: https://doi.org/10.1787/ 9789264043268-en

340. Public-Private Partnership Handbook. Asian Development Bank. URL: https://www.adb.org/sites/default/files/institutional-document/31484/public-private-partnership.pdf

341. Public-Private Partnerships: Reference Guide Version 3. Washington, DC: World Bank, 2017. URL: https://openknowledge.worldbank.org/handle/10986/2905 2

342. Rehak D., Senovsky P., Slivkova S. (2018) Resilience of Critical Infrastructure Elements and Its Main Factors. Systems. vol 6. pp. 21-30.

343. Rød, B., A. Barabadi, and M. Naseri (2020). "Recoverability modeling of power distribution systems using accelerated life models: Case of power cut due to extreme weather events in Norway. Manage. Eng. vol. 36 (5). pp. 15-33.

344. Rød, B., D. Lange, M. Theocharidou, and C. Pursiainen (2020). From risk management to resilience management in critical infrastructure. Manage. Eng. vol. 36 (4). pp. 1-13.

345. Rotfeld A. D. Europejski system bezpieczenstwa in statu nascendi. Warszawa: PISM, 1990. P. 18

346. Øien K.та Bodsberg L. Safety and Reliability – Safe Societies in a Changing World: Proceedings of ESREL. Trondheim, Norway. 2018. 2018. pp. 12-25.

347. Sicherheitsstrategie für die Güterverkehrs - und Logistikwirtschaf. Das Bundesministerium für Digitales und Verkehr (BMDV). URL: https://bmdv.bund.de/SharedDocs/DE/Publikationen/DG/sicherheitsstrategie.pdf?__blob=publicationFile

348. Strahnitskyi Ya. O. Institutional aspects of state policy implementation in the sphere of critical infrastructure protection in Ukraine. International Scientific Conference Development of Scientific Space in the Context of Global Changes: Conference Proceedings, November 25-26, 2022. Riga, Latvia: «Baltija Publishing». 64 pages.

349. Strahnitskyi Ya. O. Organizational and legal mechanisms of modern state policy in the field of critical infrastructure protection in Ukraine. International scientific conference «Influence of Europeanization on public management and administration in Ukraine» : conference proceedings (October 5–6, 2022. Riga, the Republic of Latvia). Riga, Latvia : "Baltija Publishing", 2022. 104 pages.

350. Trucco P., Cagno E., and Ambroggi M. De, (2012) Dynamic

functionalmodelling of vulnerability and interoperability of Critical Infrastructures, Reliability Engineering and System Safety. vol. 105. pp. 51–63

351. UNISDR Terminology on Disaster Risk Reduction: https://tinyurl.com/59tdbxb

352. Urie Bronfenbrenner. The Ecology of Human Development. Harvard University Press, 1979. 330 p.

353. USA Patriot Act of 2001. URL: https://www.gpo.gov/

354. Ustawa «O zarządzaniu kryzysowym» z dnia 26 kwietnia 2007 r. URL: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20070890590

355. Williamson R.D. Morris J.C. (2021) Lessons from the COVID-19 Pandemic for Federalism and Infrastructure: A Call to Action. Public Works Management and Policy. vol. pp. 6-12.

356. Yang Z., Barroca B., Bony-Dandrieux A., Dolidon H. (2022) Resilience Indicator of Urban Transport Infrastructure A Review on Current Approaches. Infrastructures. vol. 7. URL: https://doi.org/10.3390/infrastructures7030033

357. Zollo M., Winter S. (2002) Deliberate learning and the evolution of dynamic capabilities. Organization science. Vol.13. № 3. P. 3.

358. Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0). URL: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig_2-0.html

359. Mescon M. H., Albert M., Khedouri F. Management. – 3rd ed. – New York: Harper & Row, 1988. – 777 p.

360. Drucker P. F. Management: Tasks, Responsibilities, Practices. – New York: Harper & Row, 1973. – 839 c.

361. Madanat, S. (1993). Optimal infrastructure management decisions under uncertainty. Transportation Research Part C, 1(1), 77-88. https://doi.org/10.1016/0968-090X(93)90021-7

362. Pablo L. Durango-Cohen, Samer M. Madanat,Optimization of inspection and maintenance decisions for infrastructure facilities under performance model uncertainty: A quasi-Bayes approach, Transportation Research Part A: Policy and Practice, Vol. 42, Issue 8, 2008, Pages 1074-1085. https://doi.org/10.1016/j.tra.2008.03.004.

ДОДАТКИ

ДОДАТОК А

Опис показників Національного індексу кібербезпеки (NCSI)

№ п/п	Назва показника
1	2
1. Розробка політики кібербезпеки	
1.1.	Відділ політики кібербезпеки
1.2.	Формат координації політики кібербезпеки
1.3.	Стратегія кібербезпеки
1.4.	План реалізації стратегії кібербезпеки
2. Аналіз кіберзагроз та інформація	
2.1.	Підрозділ аналізу кіберзагроз
2.2.	Публічні звіти про кіберзагрози публікуються щорічно
2.3.	Веб-сайт із кібербезпекою та безпекою
3. Освіта та професійний розвиток	
3.1.	Компетентності кібербезпеки в початковій або середній освіті
3.2.	Програма кібербезпеки рівня бакалавра
3.3.	Магістерська програма кібербезпеки
3.4.	Програма кібербезпеки рівня PhD
3.5.	Професійна асоціація кібербезпеки
4. Внесок у глобальну кібербезпеку	
4.1.	Конвенція про кіберзлочинність
4.2.	Представництво у форматах міжнародного співробітництва
4.3.	Міжнародна організація з кібербезпеки, розміщена в країні
4.4.	Розвиток потенціалу кібербезпеки для інших країн
5. Захист цифрових сервісів	
5.1.	Відповідальність за кібербезпеку для постачальників цифрових послуг
5.2.	Стандарт кібербезпеки для державного сектору
5.3.	Компетентний наглядовий орган
6. Захист основних послуг	
6.1.	Визначено операторів життєво необхідних послуг
6.2.	Вимоги до кібербезпеки для операторів основних послуг
6.3.	Компетентний наглядовий орган
6.4.	Регулярний моніторинг заходів безпеки
7. Електронна ідентифікація та довірчі послуги	
7.1.	Унікальний постійний ідентифікатор
7.2.	Вимоги до криптосистем
7.3.	Електронна ідентифікація
7.4.	Електронний підпис
7.5.	Позначення часу
7.6.	Служба електронної рекомендованої доставки

1	2
7.7.	Компетентний наглядовий орган
8. Захист персональних даних	
8.1.	Законодавство про захист персональних даних
8.2.	Орган із захисту персональних даних
9. Реагування на кіберінциденти	
9.1.	Підрозділ реагування на кіберінциденти
9.2.	Відповідальність за звітність
9.3.	Єдина контактна точка для міжнародної координації
10. Управління кіберкризою	
10.1.	План управління кіберкризою
10.2.	Навчання з управління кіберкризою національного рівня
10.3.	Участь у міжнародних навчаннях з кіберкризи
10.4.	Оперативна підтримка волонтерів у кіберкризах
11. Боротьба з кіберзлочинністю	
11.1.	Кіберзлочини криміналізовані
11.2.	Підрозділ боротьби з кіберзлочинністю
11.3.	Підрозділ цифрової криміналістики
11.4.	Цілодобовий контактний пункт для боротьби з міжнародною кіберзлочинністю
12. Військові кібероперації	
12.1.	Підрозділ кібероперацій
12.2.	Навчання з кібероперацій
12.3.	Участь у міжнародних кібернавчаннях

Джерело: узагальнено авторами за даними [157]

ДОДАТОК Б

Перелік секторів критичної інфраструктури

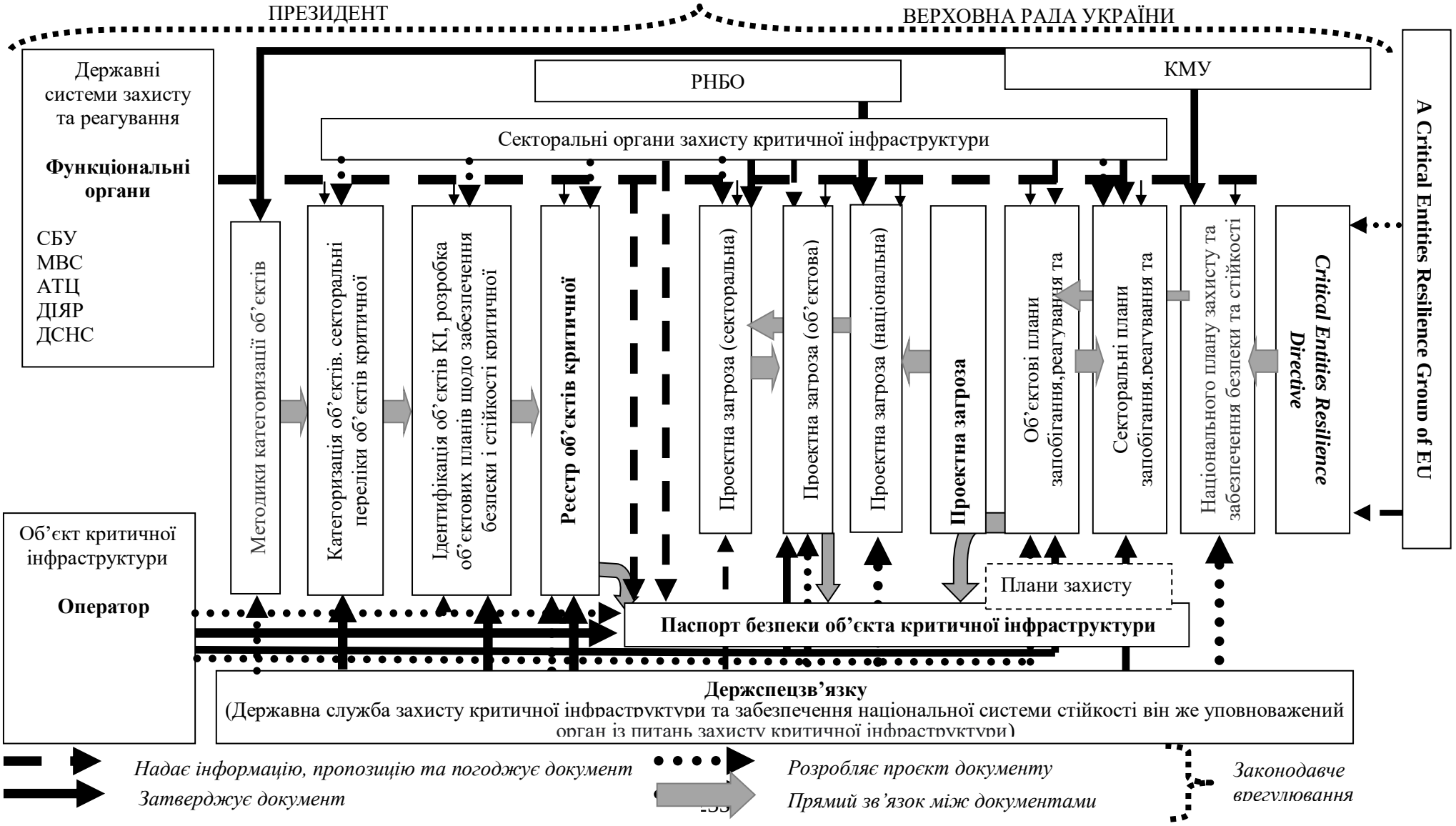
№ п\п	Сектор	Підсектор	Секторальний орган
1	**2**	**3**	**4**
1	Паливно-енергетичний сектор	електро-енергетика, вугільно-промисловий комплекс, торфодобування, нафтова промисловість, газова промисловість, ядерна енергетика,	Міненерго
2	Цифрові технології	електронні довірчі послуги та електронна ідентифікація; електронні комунікації; електронне урядування	Мінцифри
3	Захист інформації	-	Держспецзв'язку
4	Системи життєзабезпечення	комунальні послуги	Мінрегіон
5	Харчова промисловість та агропромисловий комплекс	-	Мінагрополітики
6	Державний матеріальний резерв	-	Мінекономіки
7	Охорона здоров'я	медична допомога; громадське здоров'я; фінансове забезпечення охорони здоров'я; інформаційні технології у сфері охорони здоров'я; фармацевтична промисловість; медична наука	МОЗ
8	Ринки капіталу та організовані товарні ринки	-	НКЦПФР
9	Фінансовий сектор	-	Мінфін
10	Транспорт і пошта	авіаційний транспорт; автомобільний та міський електротранспорт, у тому числі метрополітен; залізничний транспорт; морський та річковий транспорт; поштовий зв'язок;	Мінінфраструктури
11	Промисловість	хімічна промисловість; металургійна промисловість; оборонна промисловість; космічна промисловість; авіаційна промисловість; суднобудівна промисловість	Мінстратегпром
12	Сектор громадської безпеки	громадська безпека; екстрена допомога населенню за єдиним телефонним номером 112	МВС
13	Цивільний захист населення і територій	служби порятунку (атестовані аварійно-рятувальні служби згідно із законодавством)	МВС

1	2	3	4
14	Міграція (імміграція та еміграція)	-	МВС
15	Охорона навколишнього природного середовища	управління, використання та відтворення поверхневих водних ресурсів, розвиток водного господарства; поводження з радіоактивними відходами; охорона, раціональне використання і відтворення об'єктів природно-заповідного фонду	Міндовкілля
16	Сектор оборони	зберігання боєприпасів; виробництво боєприпасів	Міноборони
17	Національна безпека	-	СБУ
18	Правосуддя	-	ДСА
19	Тримання під вартою	-	Мін'юст
20	Наукові дослідження та розробки	дослідницька інфраструктура наукових установ та закладів вищої освіти	МОН
21	Фінансовий сектор	банківська система; ринок небанківських фінансових послуг (крім ринків капіталу та організованих товарних ринків); ринок платіжних послуг	Національний банк
22	Вибори та референдуми	-	Центральна виборча комісія
23	Соціальний захист	пенсійне забезпечення; соціальне страхування; соціальна допомога і соціальні послуги; інформаційна система соціальної сфери	
24	Інформаційні послуги	засоби масової інформації	МКІП
25	Державна влада та місцеве самоврядування	-	Держспецзв'язку

Джерело: [193]

ДОДАТОК В

Інституційна модель безпеки та стійкості критичної інфраструктури



Джерело: узагальнено авторами

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІННИЦЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ МИХАЙЛА КОЦЮБИНСЬКОГО

НАУКОВЕ ВИДАННЯ

ЯРЕМЕНКО Олександр Іванович – кандидат наук з державного управління, доцент, доцент кафедри публічного управління та менеджменту, декан факультету права, публічного управління і менеджменту ВДПУ імені Михайла Коцюбинського

СТРАХНІЦЬКИЙ Ярослав Олександрович – доктор філософії з публічного управління та адміністрування, співробітник УСБУ у Вінницькій області

ЗУБАР Іван Валерійович – кандидат економічних наук, старший викладач кафедри публічного управління та менеджменту ВДПУ імені Михайла Коцюбинського

НАМАЗОВА Юлія Ісмаілівна – доктор філософії з публічного управління та адміністрування, асистент кафедри публічного управління та менеджменту ВДПУ імені Михайла Коцюбинського

МЕНЕДЖМЕНТ ПІДПРИЄМСТВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ СУЧАСНИХ БЕЗПЕКОВИХ ВИКЛИКІВ

Монографія

Викладено в авторській редакції

Підписано до друку __.__.2025 Формат 60×84/16.
Папір офсетний. Друк лазерний.
Гарнітура Times New Roman
Ум. др. арк. 14,8.
Тираж 200 прим. Зам. №____
Віддруковано ТОВ «Видавництво-друкарня Діло»
Вінницька обл., Вінницький р-н,
с. Зарванці, вул. Кільцева 13, 23222.
Свідоцтво про внесення до Державного реєстру видавців,
виготовлювачів і розповсюджувачів видавничої продукції
ДК № 7482 від 19.10.2021.