ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО
«ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ»
Навчально-науковий інститут управління, економіки та бізнесу
Кафедра публічного адміністрування

«Допущено до захисту»
Завідувач кафедри
_____
І.А.Семенець-Орлова
«____»_____2026 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття другого (магістерського) рівня вищої освіти

на тему:

«ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ»

Виконав: студент групи
Е-9-24-М1ПУА(1.6д)
спеціальності 281 «Публічне управління та адміністрування»
Магеррамов Ельхан Рустемович
Керівник: д.держ.упр., Сіцінський Н.А.

Київ – 2026

АНОТАЦІЯ

Магеррамов Ельхан Рустемович. «Державна політика у сфері захисту критичної інфраструктури в умовах воєнного стану в Україні».

Кваліфікаційна робота на здобуття рівня вищої освіти «магістр» із спеціальності «Публічне управління та адміністрування» - Міжрегіональна Академія управління персоналом – Київ. 2026

У кваліфікаційній роботі визначено теоретико-правові засади державної політики захисту критичної інфраструктури. Досліджено систему управління та практики захисту критичної інфраструктури в умовах воєнного стану. Розкрито напрями підвищення стійкості та вдосконалення державної політики захисту критичної інфраструктури.

Ключові слова: критична інфраструктура, державна політика захисту критичної інфраструктури, воєнний стан, управління ризиками, кіберзахист, державна система захисту.

SUMMARY

Maherramov Elkhan. "State Policy in the Sphere of Critical Infrastructure Protection under Martial Law in Ukraine".

Thesis for obtaining the level of higher education "Master" in "Public Administration" - Interregional Academy of Personnel Management - Kyiv. 2026

The thesis defines the theoretical and legal foundations of the state policy for critical infrastructure protection. It investigates the management system and practices of critical infrastructure protection under martial law. Furthermore, it outlines directions for increasing resilience and improving the state policy for critical infrastructure protection.

Key words: critical infrastructure, state policy for critical infrastructure protection, martial law, risk management, cyber defense, state protection system.

ЗМІСТ

ВСТУП 4
РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ 9
1.1. Поняття критичної інфраструктури, загрози та принципи її захисту 9
1.2. Державна політика захисту критичної інфраструктури: цілі, інструменти, рівні управління 13
1.3. Нормативно-правове забезпечення та стандарти захисту критичної інфраструктури в Україні 16
Висновки до розділу 1 25
РОЗДІЛ 2. СИСТЕМА УПРАВЛІННЯ ТА ПРАКТИКИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВОЄННОГО СТАНУ 28
2.1. Суб’єкти та координація: органи влади, оператори, регулятори, взаємодія 28
2.2. Ризик-менеджмент, планування безперервності та реагування на інциденти та загрози 31
2.3. Кіберзахист та інформаційна безпека критичної інфраструктури: організаційні та технічні механізми 35
Висновки до розділу 2 38
РОЗДІЛ 3. НАПРЯМИ ПІДВИЩЕННЯ СТІЙКОСТІ ТА ВДОСКОНАЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ 41
3.1. Оцінка спроможностей і прогалин: аудит, індикатори, пріоритезація 41
3.2. Посилення міжвідомчої взаємодії, стандартів і підготовки персоналу 44
3.3. Інвестиції у стійкість, відновлення та інтеграція кращих практик управління ризиками 51
Висновки до розділу 3 61
ВИСНОВКИ 64
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 67
ДОДАТКИ 77

ВСТУП

Актуальність теми дослідження. Повномасштабна збройна агресія Російської Федерації проти України радикально змінила безпекове середовище, в якому функціонують об’єкти критичної інфраструктури. Системні ракетні та дронові удари по енергетичних, транспортних, комунальних, цифрових та інших критичних об’єктах, кібератаки на системи управління й інформаційні ресурси, диверсійні дії та загроза подальшого розширення агресії зумовили безпрецедентний рівень ризиків для безперервності надання життєво важливих послуг населенню та Збройним Силам України.

За оцінками уряду України та міжнародних фінансових інституцій, сукупні збитки, завдані інфраструктурі, сягають сотень мільярдів доларів США, при цьому значна частина необхідних на відновлення ресурсів стосується саме секторів, які становлять основу критичної інфраструктури – енергетики, транспорту, житлово-комунального господарства, цифрової інфраструктури. У таких умовах питання формування цілісної, науково обґрунтованої державної політики у сфері захисту критичної інфраструктури в умовах воєнного стану набуває особливої актуальності.

Важливим чинником є також євроінтеграційний курс України. Ухвалення Закону України «Про критичну інфраструктуру» та послідовна імплементація підходів ЄС до стійкості критичних суб’єктів (зокрема положень про ідентифікацію європейської критичної інфраструктури, вимоги до стійкості критичних суб’єктів, високий рівень кібербезпеки) вимагають глибокого осмислення того, яким чином європейські стандарти можуть бути адаптовані до умов тривалої війни й воєнного стану. При цьому постає завдання не лише формального наближення законодавства, а й побудови ефективної системи публічного управління, здатної забезпечити реальний захист та стійкість критичної інфраструктури в умовах багатовимірних загроз.

Проблематика критичної інфраструктури та її захисту вже тривалий час є предметом уваги зарубіжних дослідників. У працях, присвячених аналізу міжгалузевих інфраструктурних залежностей і каскадних відмов, закладено методологічні основи розуміння критичної інфраструктури як взаємопов'язаної системи. Подальші дослідження у сфері безпеки та публічного управління розробили підходи до побудови моделей загроз, організації публічно-приватного партнерства, управління ризиками та формування стійкості критичної інфраструктури. Європейські інституції та спеціалізовані агентства сформували розгалужений корпус аналітичних документів, присвячених політиці захисту й стійкості критичної інфраструктури, оцінці ефективності регуляторних рамок та виробленню нових підходів до управління ризиками.

В українській науці проблеми критичної інфраструктури досліджуються переважно в межах державного управління, безпекознавства, права, енергетичної та інформаційної безпеки. Значний внесок у розроблення концептуальних засад державної системи захисту критичної інфраструктури зроблено фахівцями Національного інституту стратегічних досліджень, які запропонували модель державної системи захисту, окреслили принципи розподілу повноважень та підходи до ідентифікації критичних об'єктів. У низці праць українських авторів досліджено правові аспекти захисту критичних об'єктів, проблеми термінології, інституційної архітектури й адміністративно-правового регулювання, а також питання інтеграції європейських підходів в українське законодавство.

Наукові пошуки щодо захисту, як окремої категорії права, неодноразово були предметом наукових досліджень теоретиків та практиків різних галузей права, а також фахівців з публічного управління та адміністрування. Зокрема, останнім часом до-слідженню питань, дотичних створенню системи захисту критичної інфраструктури України, при-свячені наукові розвідки Д. Бобро, Д. С. Бірюкова, Г. Зубка, С. Кондратова, О. Мельничука, О. Суходолі, які стали науковим підґрунтям дослідження

Разом з тим у наявних дослідженнях питання державної політики у сфері захисту критичної інфраструктури здебільшого розглядалося у «мирному» контексті або на етапі становлення відповідної системи. Воєнний стан, масовані комбіновані (фізичні й кібернетичні) атаки на інфраструктуру, масштабні програми відновлення та євроінтеграційні реформи створюють принципово нові умови, які потребують комплексного аналізу. Відчувається брак системних робіт, що поєднували б теоретико-правовий розгляд державної політики захисту критичної інфраструктури з аналізом реальних управлінських практик в умовах воєнного стану, дії надзвичайних повноважень та реалізації програм відновлення й підвищення стійкості.

Мета і завдання дослідження. Метою роботи є комплексний теоретико-правовий та організаційно-управлінський аналіз державної політики у сфері захисту критичної інфраструктури в Україні в умовах воєнного стану та вироблення науково обґрунтованих пропозицій щодо підвищення її стійкості й ефективності.

Відповідно до поставленої мети в роботі вирішуються такі основні завдання:

– розкрити зміст поняття «критична інфраструктура», систематизувати основні загрози та сформулювати базові принципи її захисту з урахуванням європейських та національних підходів;

– проаналізувати еволюцію та сучасний стан державної політики у сфері захисту критичної інфраструктури, визначити її цілі, інструменти й рівні управління, а також узгодженість із вимогами права ЄС;

– охарактеризувати нормативно-правове забезпечення та стандарти захисту критичної інфраструктури в Україні, виявити прогалини й суперечності в законодавстві та підзаконних актах;

– проаналізувати практики ризик-менеджменту, планування безперервності та реагування на інциденти на об’єктах критичної інфраструктури в контексті сучасних загроз;

– обґрунтувати напрями вдосконалення міжвідомчої взаємодії, стандартизації та підготовки персоналу в сфері захисту критичної інфраструктури;

– розробити пропозиції щодо інвестиційної та відновлювальної політики, орієнтованої на стійкість критичної інфраструктури, із урахуванням міжнародного досвіду та потреб повоєнного відновлення України.

Об'єктом дослідження є суспільні відносини, що виникають сфері забезпечення національної безпеки України в частині захисту критичної інфраструктури.

Предметом дослідження державна політика у сфері забезпечення національної безпеки України в частині захисту критичної інфраструктури.

Методологія та емпірична база дослідження.

Методологічною основою роботи є сукупність загальнонаукових і спеціальних методів пізнання. Використано діалектичний підхід для аналізу розвитку державної політики захисту критичної інфраструктури в динаміці воєнних і політичних змін; системний і структурно-функціональний методи – для дослідження інституційної архітектури суб'єктів захисту критичної інфраструктури та їхніх взаємозв'язків.

Компаративно-правовий метод застосовано для порівняльного аналізу українського законодавства й практик ЄС та НАТО у сфері захисту й стійкості критичної інфраструктури. Формально-юридичний метод використано при аналізі норм національного законодавства, підзаконних актів, стратегічних документів і міжнародно-правових норм, що стосуються критичної інфраструктури й кібербезпеки. Методи аналізу й синтезу, індукції та дедукції, контент-аналізу застосовано при опрацюванні наукових публікацій, аналітичних звітів, матеріалів міжнародних організацій.

Емпіричну базу дослідження становлять: чинні закони України й підзаконні акти у сфері національної безпеки, критичної інфраструктури та кібербезпеки; стратегії й концепції, ухвалені рішеннями Ради національної безпеки і оборони України та указами Президента України; аналітичні доповіді

Національного інституту стратегічних досліджень; міжнародні документи Європейського Союзу і НАТО; статистичні та звітні матеріали Державної служби спеціального зв'язку та захисту інформації України, CERT-UA, Рахункової палати України та міжнародних фінансових інституцій.

Структура роботи. Структура роботи зумовлена логікою досягнення поставленої мети й вирішення визначених завдань. Робота складається зі вступу, трьох розділів, що включають дев'ять підрозділів, висновків, списку використаних джерел та додатків.

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Поняття критичної інфраструктури, загрози та принципи її захисту

У сучасній науці та практиці державного управління поняття «критична інфраструктура» використовується для позначення сукупності об’єктів, систем і мереж, порушення функціонування яких може спричинити тяжкі наслідки для суспільства, економіки, національної безпеки та довкілля. Одними з перших системно окреслили цю проблематику дослідження, присвячені міжгалузевим залежностям інфраструктурних систем та їхнім «каскадним» відмовам, де критична інфраструктура розглядається не ізольовано, а як взаємопов’язана мережа енергетичних, транспортних, інформаційно-комунікаційних, водогосподарських і фінансових систем [1]. У цих роботах підкреслюється, що навіть локальний збій в одному елементі може викликати ланцюг відмов у суміжних галузях, якщо між ними існує сильна технологічна чи організаційна залежність.

Питання захисту об’єктів критичної інфраструктури, його нормативно-правового врегулювання обумовлені посиленням загроз зовнішнього світу, серед яких вирізняють: природні та техногенні загрози, терористичні та воєнні загрози, кібератаки, яким піддаються об’єкти критичної інфраструктури.

З 24 лютого 2022 року – дати, коли російська федерація розпочала повномасштабне вторгнення на територію України та невпинні зазіхан-ня на руйнування об’єктів критичної інфраструктури нашої держави, все більшої актуальності набувають питання захисту об’єктів критичної інфраструктури. Вищезазначеним обумовлене дослідження окреслених питань у даному науковому доробку.

На нормативному рівні в Європейському Союзі перше комплексне визначення критичної інфраструктури було закріплено в Директиві Ради

2008/114/ЄС. У ній під європейською критичною інфраструктурою розуміються об’єкти, системи чи їх частини, розташовані в державах-членах, порушення або знищення яких мало б значний вплив на принаймні дві держави-члени внаслідок втрати життєво важливих функцій, серйозного порушення громадської безпеки або інших значних негативних наслідків [2]. Новіший підхід зафіксовано в Директиві (ЄС) 2022/2557 про стійкість критичних суб’єктів, де акцент робиться не лише на фізичному захисті інфраструктури, а й на забезпеченні безперервності постачання «важливих послуг» у широкому колі секторів, включаючи енергетику, транспорт, банківський сектор, охорону здоров’я, питну воду, цифрову інфраструктуру тощо [3].

В українському законодавстві визначення критичної інфраструктури міститься в Законі України «Про критичну інфраструктуру», де під нею розуміють об’єкти, системи, їх частини, ресурси, послуги і процеси, які є стратегічно важливими для економіки, національної безпеки та оборони, функціонування суспільства і порушення роботи яких може завдати значної шкоди національним інтересам [7]. У подальших наукових працях українських авторів уточнюється, що до критичної інфраструктури доцільно відносити не лише матеріальні об’єкти (підстанції, мости, серверні центри), а й «нематеріальні» елементи – інформаційні ресурси, програмно-апаратні комплекси управління, канали зв’язку, що керують фізичними процесами [16; 19].

У теоретичному плані дослідники виділяють декілька ключових ознак, які дозволяють віднести об’єкт або систему до критичної інфраструктури. По-перше, це значущість для функціонування життєво важливих суспільних процесів: енергопостачання, транспортного сполучення, зв’язку, фінансових операцій, охорони здоров’я, державного управління. По-друге, низька замінність: у разі виходу з ладу об’єкта відсутні або дуже обмежені альтернативи, здатні швидко взяти на себе його функції. По-третє, високий потенціал каскадних наслідків – збій в одному секторі може призвести до проблем у кількох інших (наприклад, відключення електропостачання зумовлює

зупинку насосних станцій, порушення зв’язку, складнощі в роботі лікарень) [1; 24]. Усе це зумовлює потребу в особливому підході до управління ризиками та безпекою таких об’єктів.

Щодо загроз критичній інфраструктурі, сучасні дослідження пропонують так званий «усі загрози» (all-hazards) підхід, у рамках якого враховуються природні, техногенні, антропогенні, терористичні, кібернетичні й гібридні ризики [17; 24]. До природних належать, зокрема, повені, землетруси, екстремальні погодні явища, лісові пожежі, які можуть безпосередньо пошкоджувати об’єкти інфраструктури або спричиняти масові відключення. Техногенні загрози включають аварії на промислових об’єктах, транспортні катастрофи, відмови складного обладнання. Антропогенні та умисні загрози пов’язані з тероризмом, диверсіями, саботажем, організованою злочинністю. Окрему категорію становлять кіберзагрози, спрямовані на системи управління технологічними процесами, інформаційні ресурси та канали зв’язку [4; 23]. Для України в умовах широкомасштабної збройної агресії особливу актуальність мають саме комбіновані загрози, коли одночасно застосовуються ракетні удари, диверсійні дії та кібероперації проти енергетичної, транспортної та цифрової інфраструктури.

Паралельно з переліком загроз у міжнародній та національній практиці сформувалися базові принципи захисту критичної інфраструктури. У документах ЄС підкреслюється, що політика у цій сфері має спиратися на ризик-орієнтований, пропорційний і секторально диференційований підхід: ресурси спрямовуються насамперед на ті об’єкти, порушення роботи яких матиме найбільші негативні наслідки [2; 3; 6]. Додатково наголошується на принципах відповідальності оператора (operational responsibility), багаторівневого управління (multi-level governance) та тісної співпраці держави й приватного сектору, оскільки значна частина об’єктів критичної інфраструктури перебуває у приватній або змішаній власності [22].

У науковій літературі та стратегічних документах поступово відбувається перехід від вузького поняття «захист» (protection) до ширшого поняття

«стійкість» (resilience). Якщо перший акцентує насамперед запобігання інцидентам і фізичному захисту об’єктів, то другий охоплює здатність системи готуватися до інцидентів, витримувати їх, адаптуватися та відновлюватися до прийнятного рівня функціонування [14; 25]. Дослідження, проведені в різних країнах, показують, що повністю усунути всі ризики неможливо, тому стратегія повинна поєднувати превентивні заходи (захист, виявлення загроз) з механізмами управління наслідками та швидкого відновлення.

Українські дослідники, аналізуючи національний контекст, підкреслюють, що для критичної інфраструктури України характерне поєднання «класичних» вразливостей – зношеність основних фондів, висока концентрація потужностей, низький рівень фізичного та кіберзахисту – з новими викликами, пов’язаними з гібридною та повномасштабною війною, тривалими кібератаками, використанням інфраструктури як об’єкта політичного та військового тиску [11; 12; 17]. На цьому тлі принципи захисту критичної інфраструктури включають не лише технічні та організаційні заходи, а й інституційне розмежування відповідальності, створення спеціалізованих координаційних структур, розвиток системи моніторингу та обміну інформацією.

На основі аналізу європейських та українських джерел можна узагальнити такі ключові принципи державної політики у сфері захисту критичної інфраструктури: пріоритет безперервності надання життєво важливих послуг; ризик-орієнтований підхід; багаторівневе управління й розподіл відповідальності між державою та операторами; поєднання превентивних і відновних заходів; розвиток стійкості та здатності до адаптації; тісна взаємодія з приватним сектором і громадянським суспільством; використання міжнародних стандартів і практик [2; 3; 5; 13; 20; 22]. Усе це створює теоретичний та нормативний фундамент для формування державної політики захисту критичної інфраструктури.

1.2. Державна політика захисту критичної інфраструктури: цілі, інструменти, рівні управління

Державна політика захисту критичної інфраструктури формується як відповідь на усвідомлення її ролі для національної безпеки, економічної стабільності та повсякденного функціонування суспільства. У стратегічних документах ЄС і держав-членів основною метою політики в цій сфері визначається забезпечення безперервності надання життєво важливих послуг навіть в умовах серйозних інцидентів, криз чи збройних конфліктів [3; 5; 6]. У цьому контексті захист критичної інфраструктури розглядається як складова ширшої політики національної безпеки, цивільного захисту, кібербезпеки та економічної політики.

На рівні Європейського Союзу еволюція політики захисту критичної інфраструктури проходила кілька етапів. Першим був етап формування Європейської програми захисту критичної інфраструктури (EPCIP), у рамках якої було запроваджено поняття «європейської критичної інфраструктури» та розроблено базові підходи до її ідентифікації й оцінки вразливості [5]. Наступним кроком стало ухвалення Директиви 2008/114/ЄС, яка встановила вимоги до виявлення та позначення європейських критичних інфраструктур у секторах енергетики та транспорту, а також до розробки планів безпеки операторів [2]. Оцінка дії цієї директиви показала, що її сфера застосування є обмеженою, а підхід надто вузько зосереджений на захисті окремих об’єктів, тоді як сучасні ризики потребують системного бачення [6].

Новий етап пов’язаний з прийняттям Директиви (ЄС) 2022/2557 про стійкість критичних суб’єктів, яка розширила перелік секторів, увела поняття «критичного суб’єкта» (critical entity) та спрямувала увагу на управління ризиками, оцінку стійкості та заходи з підвищення здатності до відновлення [3]. Держави-члени зобов’язані розробити національні стратегії, проводити регулярні оцінки ризиків, визначати критичних суб’єктів і забезпечувати контроль за виконанням ними обов’язків щодо управління ризиками, планування

безперервності, взаємодії з компетентними органами. Паралельно Директива NIS2 встановлює вимоги до забезпечення високого рівня кібербезпеки для операторів основних послуг і низки інших суб'єктів, що є важливими для функціонування цифрової та «традиційної» критичної інфраструктури [4].

В Україні державна політика у сфері захисту критичної інфраструктури формувалася під впливом як внутрішніх факторів (зношеність інфраструктури, техногенні загрози, терористичні ризики), так і зовнішніх викликів, насамперед гібридної агресії та війни проти України. У Стратегії національної безпеки України 2015 року серед загроз прямо названо критичну зношеність основних фондів об'єктів інфраструктури, недостатній рівень їхнього фізичного захисту та загрози безпеці критичної інфраструктури [11]. Закон України «Про національну безпеку України» відносить критичну інфраструктуру до ключових об'єктів національної безпеки та передбачає створення державної системи її захисту [8].

Перші концептуальні напрацювання щодо побудови такої системи були здійснені Національним інститутом стратегічних досліджень (НІСД), де в аналітичних доповідях і «Зеленій книзі» було запропоновано структуру державної системи захисту критичної інфраструктури, принципи розподілу повноважень між органами влади та загальні підходи до ідентифікації об'єктів [12; 13; 14]. У цих роботах наголошувалося на необхідності інтеграції національної політики з європейськими підходами, впровадження ризик-орієнтованих методик, формування єдиного інформаційного простору для обміну даними про загрози та інциденти.

На практиці державна політика захисту критичної інфраструктури в Україні реалізується через поєднання нормативно-правових, організаційних, економічних та інформаційних інструментів. До нормативно-правових інструментів належать закони, підзаконні акти, стандарти та методичні документи, що визначають вимоги до безпеки об'єктів, процедури ідентифікації та категоризації, плани безпеки і безперервності, повноваження органів влади й операторів [7–9; 15–18]. Організаційні інструменти охоплюють створення спеціалізованих підрозділів в органах виконавчої влади, формування

міжвідомчих комісій, координаційних центрів, механізмів взаємодії з приватним сектором і міжнародними партнерами. Економічні інструменти включають цільові програми модернізації інфраструктури, бюджетне фінансування заходів безпеки, а також стимулювання інвестицій операторів у підвищення стійкості. Інформаційні інструменти пов’язані зі створенням систем моніторингу, оповіщення, обміну інформацією про загрози та інциденти, а також із розвитком культури безпеки.

Особливістю політики в цій сфері є багаторівнева структура управління. На стратегічному рівні ключову роль відіграють Президент України, Рада національної безпеки і оборони, Верховна Рада України та Кабінет Міністрів України, які визначають засади політики, затверджують стратегії й концепції, ухвалюють базові закони та координують діяльність сектору безпеки й оборони [8; 11; 14]. На галузевому рівні відповідальність покладається на центральні органи виконавчої влади у відповідних секторах (енергетика, транспорт, зв’язок, охорона здоров’я, фінанси тощо), які розробляють і реалізують політику захисту критичної інфраструктури у своїх сферах, взаємодіючи з операторами та регуляторами [17; 18; 21]. На операційному рівні безпосередню відповідальність за безпеку несуть оператори об’єктів критичної інфраструктури – державні, комунальні та приватні підприємства, що зобов’язані впроваджувати системи управління безпекою, оцінки ризиків, планування безперервності та реагування.

У наукових роботах, присвячених українському досвіду, звертається увага на те, що ефективна державна політика захисту критичної інфраструктури потребує поєднання централізованого стратегічного керівництва з децентралізованою відповідальністю операторів та місцевих органів влади [19; 20; 21]. Досвід європейських країн, проаналізований у спеціальних дослідженнях, показує, що успішні моделі передбачають активну участь приватного сектору, чітко визначені обов’язки операторів, регулярні аудити та навчання, а також використання публічно-приватних партнерств, але за умови, що держава зберігає здатність координувати зусилля та встановлювати обов’язкові стандарти [20; 22].

Окремий вимір політики стосується інтеграції захисту критичної інфраструктури з політикою кібербезпеки. Закон України «Про основні засади забезпечення кібербезпеки України» вводить поняття об’єктів критичної інформаційної інфраструктури та встановлює особливий режим їхнього захисту [9]. Стратегія кібербезпеки України, ухвалена рішенням РНБО, визначає завдання щодо виявлення й нейтралізації кіберзагроз для критичної інфраструктури, створення системи реагування на інциденти, розвитку національного сегмента кібербезпекових центрів [10]. У поєднанні з політикою захисту фізичних об’єктів це формує комплексну систему заходів, спрямованих на забезпечення стійкості як фізичних, так і інформаційно-комунікаційних компонентів критичної інфраструктури.

Таким чином, державна політика захисту критичної інфраструктури характеризується багаторівневістю, міжгалузевим характером та інтеграцією з іншими політиками безпеки. Її цілі – гарантування безперервності життєво важливих послуг і мінімізація наслідків інцидентів – реалізуються через поєднання нормативно-правових, організаційних, економічних та інформаційних інструментів, у взаємодії центральної влади, регіональних органів, операторів і міжнародних партнерів [3; 7; 12–14; 20–22].

1.3. Нормативно-правове забезпечення та стандарти захисту критичної інфраструктури в Україні

Нормативно-правова база захисту критичної інфраструктури в Україні формувалася поетапно і нині складається з низки законів, підзаконних актів, стратегічних документів та методичних рекомендацій, які в сукупності створюють рамку для побудови державної системи її захисту. Центральне місце серед законів посідає Закон України «Про критичну інфраструктуру», який визначає основні терміни, принципи, суб’єктів та механізми державної політики в цій сфері [7]. Він установлює, зокрема, порядок ідентифікації об’єктів критичної інфраструктури, визначає критерії їхньої критичності, вводить

поняття операторів критичної інфраструктури та їхніх обов'язків щодо забезпечення безпеки.

Аналізований закон передбачає, що Кабінет Міністрів України затверджує перелік секторів і підсекторів критичної інфраструктури, критерії її віднесення, а також повноваження центральних органів виконавчої влади щодо координації та реалізації політики в цій сфері. Оператори критичної інфраструктури зобов'язані здійснювати оцінку ризиків, розробляти та впроваджувати плани безпеки й безперервності, забезпечувати захист інформації, у тому числі з обмеженим доступом, а також взаємодіяти з компетентними органами у разі інцидентів [7; 16; 18]. У наукових публікаціях зазначається, що прийняття цього закону стало важливим кроком до систематизації правового поля, хоча питання практичної реалізації його положень потребують подальшого розвитку [16–18].

Дослідження окреслених питань доречно розпочати з історико-правового екскурсу передумов ґенези та розвитку нормативно-правового регулювання захисту об'єктів критичної інфраструктури. Основні загрози внутрішньому безпековому середовищу та безпосередні зовнішні виклики, що загрожують національній безпеці України, було сформульовано в Указі Президента України "Про Стратегію національної безпеки України" від 12.02.2007 року № 105/2007 (втратив чинність). У подальшому було прийнято Рішення Ради національної безпеки і оборони України "Про Стратегію національної безпеки України" від 06.05.2015 року, яким передбачалась розробка Урядом комплексних пропозицій щодо реформування органів сектору безпеки і оборони України. Основою для створення системи захисту об'єктів критичної інфраструктури, доцільно, на нашу думку, вважати Концепцію створення державної системи захисту критичної інфраструктури, прийняту Розпорядженням Кабінету Міністрів України від 06.12.2017 року № 1009-р (далі – Концепція). Згідно даної Концепції одним з пріоритетів реформування органів сектору оборони і безпеки України було визначено створення системи захисту критичної інфраструктури. При цьому серед основних проблем, які потребували свого належного розв'язання Концепцією, зазначались такі, як: 1) відсутність єдиної системи захисту

критичної інфраструктури; 2) недостатність та неузгодженість нормативно-правового регулювання з питань захисту систем і об'єктів критичної інфраструктури; 3) відсутність державного органу, відповідального за координацію дій у сфері захисту критичної інфраструктури; 4) невизначеність повноважень державних органів у сфері захисту критичної інфраструктури, правового статусу власників (розпорядників) об'єктів критичної інфраструктури; 5) відсутність методології віднесення об'єктів до об'єктів критичної інфраструктури, порядку їх паспортизації та категоризації; 6) відсутність методології проведення оцінки можливих загроз критичній інфраструктурі; 7) нерозвиненість державно-приватного партнерства у сфері захисту критичної інфраструктури; 8) невизначеність джерел фінансування заходів щодо захисту критичної інфраструктури; 9) недостатній рівень міжнародного співробітництва у сфері захисту критичної інфраструктури.

У травні 2019 року було запропоновано Проєкт Закону "Про критичну інфраструктуру та її захист" (далі – Проєкт Закону), розробка якого була логічним продовженням виконання положень, зазначених у Концепції. Відповідно до пояснювальної записки даного Проєкту Закону його метою було створення умов для формування і ефективної реалізації державної політики у сфері захисту критичної інфраструктури. При цьому необхідність його прийняття обґрунтовувалась, у тому числі, з позицій збройної агресії російської федерації вже на момент подання Проєкту Закону. Тож створення ефективної системи захисту об'єктів критичної інфраструктури започатковане з урахуванням викликів національній безпеці, які обумовлені були не лише загрозами природного чи техногенного характеру, а й збройною агресією російської федерації до її повномасштабного вторгнення, та внаслідок пошкодження інфраструктурних об'єктів у східних та південних регіонах України. Проте зазначений Проєкт Закону було відкликано.

Наступним кроком було прийняття Урядом Постанови "Деякі питання об'єктів критичної інфраструктури" від 09.10.2020 року № 1109, якою був затверджений Порядок віднесення об'єктів до об'єктів критичної

інфраструктури; Перелік секторів (підсекторів), основних послуг критичної інфраструктури держави; Методика категоризації її об’єктів; регламентовано ряд термінів, серед яких “захист об’єктів критичної інфраструктури” визначався через сукупність заходів (організаційних, нормативно-правових, інженерно-технічних та інших), спрямованих на забезпечення безпеки об’єктів критичної інфраструктури.

Згодом прийнято Закон України “Про критичну інфраструктуру” від 16.11.2021 року, яким наразі визначено організаційно-правові засади створення та функціонування національної системи захисту критичної інфраструктури. Даним Законом визначено термін “захист критичної інфраструктури”, який суттєво відрізняється від терміну, що був закріплений вищезгаданою Постановою Кабінету Міністрів України, і передбачає “всі види діяльності, які виконуються перед або під час створення, функціонування, відновлення і реорганізації об’єкта критичної інфраструктури, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об’єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації”. Вважаємо за доцільне зауважити, що термін “захист критичної інфраструктури”, визначений статтею 1 даного Закону, за своїм змістовним наповненням став наближений до терміну “захист критичної інфраструктури”, який міститься в нормативних актах Європейського Союзу, через словосполучення “всі види діяльності” та “нейтралізацію загроз”.

Згаданий вище Проєкт Закону в статті 1 містив термін “державна система захисту критичної інфраструктури”, під якою було визначено систему суб’єктів із забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури. Вважаємо, що термін “національна система захисту критичної інфраструктури”, визначений статтею 1 Закону України “Про критичну інфраструктуру”, дає більш повне уявлення про суб’єктів захисту критичної інфраструктури та елементи національної системи захисту, оскільки визначає останню 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 покладено формування та/або реалізацію державної політики у сфері захисту критичної інфраструктури". Проте не слід оминати увагою і пропозиції, що містились у згаданому Проєкті Закону, та не враховані в чинному законодавстві щодо захисту критичної інфраструктури. Зокрема, відповідно до Порівняльної таблиці Проєкту Закону передбачалось внесення змін до Закону України "Про правовий режим воєнного стану", а саме – термін "воєнний стан" пропонувалось доповнити шляхом додавання словосполучення "захист критичної інфраструктури". Така пропозиція, на нашу думку, була слушною, адже стаття 3 Закону України "Про критичну інфраструктуру" окреслює сферу застосування цього Закону саме через відносини у сфері функціонування та захисту критичної інфраструктури в цілому і її об'єктів – у мирний час. Водночас питання та особливості захисту об'єктів критичної інфраструктури в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, особливого періоду регулюються, в тому числі, Законом України "Про правовий режим воєнного стану". Тож без наведених вище доповнень визначення терміну "воєнний стан" не містить такий стратегічно важливий компонент як "захист критичної інфраструктури".

Державна політика у сфері захисту об'єктів критичної інфраструктури законодавчо передбачає забезпечення безпеки об'єктів критичної інфраструктури відповідно до статті 5 Закону України "Про критичну інфраструктуру". Серед інших завдань, які законодавчо закріплені як мета державної політики у сфері захисту критичної інфраструктури, зазначено такі, як: 1) запобігання проявам несанкціонованого втручання у функціонування об'єктів критичної інфраструктури; 2) прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури. Проте два наступні складові компоненти зазначеної політики є похідними від основної мети – захисту критичної інфраструктури. Слушною, на наш погляд, вбачається думка Ю. В. Желіховської, про те, що захист – це засіб, який настає за порушенням, і тягне за собою відновлення суб'єктивного права. Тож забезпечення захисту об'єктів

критичної інфраструктури може досягатись, у тому числі, через належне нормативно-правове забезпечення і розробку нормативно-технічної бази щодо безпекових питань відносно об’єктів критичної інфраструктури.

З метою реалізації державної політики у сфері захисту об’єктів критичної інфраструктури частина друга статті 13 Закону України “Про критичну інфраструктуру” передбачає функціонування секторальних та функціональних органів у сфері захисту критичної інфраструктури. Після масивних ракетних атак, спрямованих на об’єкти критичної інфраструктури України, які були здійснені російською федерацією восени 2022 року, прийнято Закон України “Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України” від 18.10.2022 року, яким було внесено зміни до статусного Закону України “Про Державну службу спеціального зв’язку та захисту інформації України”. Відповідно до внесених змін Державна служба спеціального зв’язку та захисту інформації України (далі – Держспецзв’язку) наділена повноваженнями уповноваженого органу у сфері захисту критичної інфраструктури України під час дії правового режиму воєнного стану та протягом 12 місяців після його припинення чи скасування.

Згідно змін, внесених до статті 13 Закону України “Про критичну інфраструктуру”, було визначено, що формування та реалізація державної політики у сфері захисту критичної інфраструктури, координація діяльності суб’єктів національної системи захисту покладено на Держспецзв’язку. При цьому стаття 14 Закону України “Про критичну інфраструктуру” виокремлює суб’єктів національної системи захисту критичної інфраструктури і містить невичерпний перелік суб’єктів, до яких віднесено: 1) Кабінет Міністрів України; 2) Апарат Ради національної безпеки і оборони України; 3) Центральну виборчу комісію; 4) Національний банк України; 5) Національну комісію з цінних паперів та фондового ринку, Національну комісію, що здійснює державне регулювання у сфері зв’язку та інформатизації, Національну комісію, що здійснює державне регулювання у сферах енергетики та комунальних послуг; 6) Адміністрацію

Державної служби спеціального зв'язку та захисту інформації України; 7) Фонд державного майна України та інші центральні органи виконавчої влади зі спеціальним статусом; 8) уповноважений орган у сфері захисту критичної інфраструктури України – Держспецзв'язку; 9) Державну службу України з надзвичайних ситуацій; 10) секторальні та функціональні органи та інші міністерства і центральні органи виконавчої влади; 11) Службу безпеки України; 12) правоохоронні та розвідувальні органи, суб'єктів оперативно-розшукової та контррозвідувальної діяльності; 13) Збройні Сили України та інші військові формування; 14) місцеві органи виконавчої влади (військово-цивільні адміністрації); 15) органи місцевого самоврядування; 16) операторів критичної інфраструктури; 17) підприємства, установи та організації, які проводять діяльність, що пов'язана із забезпеченням безпеки та стійкості критичної інфраструктури, незалежно від форми власності.

В результаті аналізу вищенаведених спеціального та статусного законів можна дійти висновку, що Держспецзв'язку наразі набуває статусу першого державного органу, який має повноваження керувати національною системою захисту критичної інфраструктури, координувати міністерства та операторів інфраструктури, вести реєстр об'єктів критичної інфраструктури, оцінювати ризики на національному рівні, створювати бази даних загроз та вразливостей об'єктів критичної інфраструктури, формувати стратегії національної безпеки та кібербезпеки тощо. Повноваження Держспецзв'язку як уповноваженого органу у сфері захисту критичної інфраструктури України обумовлені наявністю введеного воєнного стану та 12 місяцями після його припинення чи скасування.

Важливими елементами нормативного середовища є також Закон України «Про національну безпеку України», який визначає критичну інфраструктуру як одну з ключових складових національної безпеки і передбачає формування державної системи її захисту [8], та Закон України «Про основні засади забезпечення кібербезпеки України», що регулює відносини у сфері захисту критичної інформаційної інфраструктури, інформаційних ресурсів і систем

управління технологічними процесами [9]. У сукупності ці акти задають рамку для інтеграції фізичного та кіберзахисту об’єктів критичної інфраструктури.

Стратегічний рівень нормативно-правового забезпечення представлений, насамперед, Стратегією національної безпеки України та Стратегією кібербезпеки України, ухваленими указами Президента України на підставі рішень РНБО [10; 11]. У цих документах критична інфраструктура розглядається як один із пріоритетних напрямів державної політики безпеки, а серед основних загроз називаються уразливість об’єктів критичної інфраструктури до кібератак, терористичних посягань, фізичного зносу та неефективного управління [11]. Стратегія кібербезпеки, у свою чергу, визначає завдання зі створення системи виявлення й реагування на кіберзагрози, що стосуються критичної інфраструктури, розвитку нормативної бази та інституційної спроможності відповідальних органів [10].

Суттєвий внесок у формування нормативно-правової основи зробили й аналітичні напрацювання НІСД, на базі яких готувалися проєкти законів, концепцій і підзаконних актів. У «Зеленій книзі» з питань захисту критичної інфраструктури в Україні пропонується модель державної системи захисту, яка включає координаційний центр, галузеві органи, операторів і механізми взаємодії між ними [13]. В аналітичній доповіді про державну систему захисту критичної інфраструктури наголошується на необхідності розробки секторних стратегій, впровадження єдиних підходів до оцінки ризиків, створення національної системи моніторингу та обміну інформацією [14].

На рівні підзаконних актів нормативне поле доповнюється постановами Кабінету Міністрів України, що визначають організацію роботи уповноважених органів у відповідних секторах, порядок ведення реєстрів об’єктів критичної інфраструктури, вимоги до розробки та затвердження планів безпеки, а також взаємодію з правоохоронними та силовими структурами. Окремі галузеві міністерства і відомства ухвалюють власні нормативні акти, спрямовані на захист критичних об’єктів у своїй сфері відповідальності (наприклад, у системі Міністерства оборони, енергетики, транспорту, зв’язку) [17; 21].

Юридичний аналіз цих актів, здійснений українськими дослідниками, виявляє низку проблем. Частина з них стосується фрагментації регулювання – різні закони й підзаконні акти не завжди узгоджені між собою, термінологія в окремих документах відрізняється, а повноваження органів – перетинаються або залишаються невизначеними [16–19]. Інші проблеми пов’язані з тим, що низка важливих елементів системи – наприклад, порядок проведення системної оцінки ризиків на рівні держави, спільні процедури обміну інформацією між операторами та державними органами, механізми контролю й аудиту – поки що лише частково врегульовані або реалізуються на основі відомчих документів.

Окремий блок нормативно-правового забезпечення стосується методичного та стандартизаційного підґрунтя. У працях українських авторів пропонуються методики оцінки рівня критичності об’єктів інфраструктури, які враховують, зокрема, масштаби можливих наслідків для населення, економіки, довкілля та національної безпеки, а також ступінь взаємозалежності між різними об’єктами і секторами [15; 17]. Ці методики спираються на міжнародний досвід і стандарти управління безперервністю бізнесу та ризиками, зокрема серію міжнародних стандартів у сфері управління безпекою, безперервністю діяльності й кібербезпекою, які адаптуються до українського контексту [5; 6; 23].

У наукових публікаціях приділяється увага й питанням імплементації європейського права в українське законодавство. Наголошується, що Закон України «Про критичну інфраструктуру» загалом корелює з підходами, закріпленими в європейських директивах, але потребує подальшої конкретизації в частині ідентифікації критичних суб’єктів, запровадження обов’язкових вимог до систем управління ризиками, оцінки стійкості та звітності операторів [2; 3; 16; 18; 20]. Досвід держав-членів ЄС свідчить, що ефективність правового регулювання значною мірою залежить від того, наскільки чітко визначені обов’язки суб’єктів, як працюють механізми контролю та санкцій і чи достатньо ресурсів виділяється на реалізацію вимог.

Додатковий аспект нормативно-правових засад захисту критичної інфраструктури пов’язаний з правами людини та балансом між безпекою і

свободами. Обговорюючи це питання, українські й зарубіжні автори звертають увагу на те, що заходи безпеки (наприклад, відеоспостереження, контроль доступу, моніторинг трафіку) не повинні порушувати гарантовані законом права громадян, а втручання в приватність має бути пропорційним і виправданим з точки зору захисту критично важливих функцій суспільства [22; 24]. Це особливо актуально для сфер, де критична інфраструктура пов'язана з обробкою великих масивів персональних даних (енергетичні лічильники, транспортні системи, цифрові сервіси).

Таким чином, нормативно-правове забезпечення захисту критичної інфраструктури в Україні характеризується поєднанням базових законів, стратегічних документів, підзаконних актів і методичних напрацювань. Прийняття Закону «Про критичну інфраструктуру» стало важливим етапом, що заклав основу для системного розвитку цієї сфери, однак подальша гармонізація законодавства, деталізація вимог до операторів, імплементація європейських стандартів і підвищення інституційної спроможності залишаються ключовими завданнями для підвищення стійкості й безпеки критичної інфраструктури [7–9; 13–19; 21–23].

Висновки до розділу 1

У першому розділі здійснено теоретико-правове узагальнення поняття "критична інфраструктура" та показано, що в сучасному державному управлінні воно описує не суму ізольованих об'єктів, а взаємопов'язану мережу систем і послуг, у якій локальні збої здатні спричиняти "каскадні" наслідки в суміжних секторах. Обґрунтовано, що критичність визначається одночасно значущістю для життєво важливих функцій, низькою замінністю та потенціалом міжсекторальних відмов, а тому підходи до безпеки мають базуватися на пріоритезації найбільш чутливих вузлів і залежностей, а не лише на охороні окремих об'єктів. Уточнено, що посилення ризиків для критичної інфраструктури зумовлене одночасною дією природних, техногенних, умисних і

кіберзагроз, які в умовах війни набувають комбінованого характеру. Показано, що після 24 лютого 2022 року питання захисту критичної інфраструктури в Україні перейшло в режим постійної актуальності, оскільки руйнування або порушення функціонування інфраструктурних систем безпосередньо впливає на життєзабезпечення населення, економічну стійкість і керованість держави; у цьому контексті ключовим стає забезпечення безперервності надання життєво важливих послуг.

У розділі систематизовано європейські підходи до визначення та регулювання критичної інфраструктури і встановлено еволюцію від фокусу на ідентифікації та фізичному захисті об’єктів до управління стійкістю критичних суб’єктів і безперервністю “важливих послуг” у широкому колі секторів. Показано, що зазначена еволюція логічно узгоджується з сучасним ризиковим середовищем і цифровою залежністю інфраструктури, а тому є релевантною для подальшої гармонізації української моделі із підходами Європейського Союзу.

У межах аналізу державної політики у сфері захисту критичної інфраструктури обґрунтовано, що її метою доцільно вважати гарантування безперервності життєво важливих послуг і мінімізацію наслідків інцидентів через поєднання правових, організаційних, економічних та інформаційних інструментів. Встановлено, що управлінська модель цієї політики є багаторівневою: стратегічний рівень формує рамку та координацію, галузевий рівень забезпечує секторальну реалізацію, а операційний рівень покладає безпосередню відповідальність за безпеку й планування безперервності на операторів об’єктів. Підкреслено, що така архітектура передбачає узгодженість дій держави, регуляторів і операторів, а також інтеграцію фізичного захисту з кібербезпековими механізмами як обов’язкову умову результативності політики.

Встановлено, що нормативно-правове забезпечення в Україні має рамковий характер і концентрується навколо Закону України “Про критичну інфраструктуру”, який закріплює понятійний апарат, принципи, суб’єктний склад і загальні механізми національної системи захисту, а також визначає обов’язки операторів щодо оцінювання ризиків, планування безпеки та

безперервності, захисту інформації й взаємодії у разі інцидентів. Показано поетапність становлення регулювання та управлінських рішень, включно з формуванням концептуальних засад і підзаконного нормотворення, що заклало основу для переходу від фрагментарних практик до системної політики.

Разом із тим доведено, що поточна модель нормативного забезпечення зберігає ознаки перехідності: наявні прояви фрагментації та різночитань термінів, нерівномірність секторальних практик, а також неповна деталізація процедур оцінювання ризиків, обміну інформацією, контролю та аудиту. Окремо підкреслено значення методичного та стандартизаційного підґрунтя для забезпечення зіставності оцінок критичності й ризиків у секторах, а також важливість балансу між безпековими заходами та гарантіями прав людини у сферах, де критична інфраструктура пов’язана з обробкою значних масивів даних.

РОЗДІЛ 2.
СИСТЕМА УПРАВЛІННЯ ТА ПРАКТИКИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВОЄННОГО СТАНУ

2.1. Суб’єкти та координація: органи влади, оператори, регулятори, взаємодія

Система управління захистом критичної інфраструктури в Україні в умовах воєнного стану характеризується поєднанням кількох рівнів – стратегічного, галузевого й операційного – та залученням широкого кола суб’єктів публічної влади й недержавних акторів. На стратегічному рівні ключова роль належить Президенту України, Раді національної безпеки і оборони України (РНБО), Верховній Раді України та Кабінету Міністрів України, які формують засади державної політики у сфері національної безпеки загалом і захисту критичної інфраструктури зокрема [8; 11; 14; 21]. У Стратегії національної безпеки України критична інфраструктура визначена як одна з основних складових безпекового середовища, а її вразливість – як суттєва загроза національній безпеці [11]. Закон України «Про національну безпеку України» закріплює обов’язок держави створити державну систему захисту критичної інфраструктури та інтегрувати її в загальну систему сектору безпеки й оборони [8].

Спеціальним правовим фундаментом є Закон України «Про критичну інфраструктуру», який визначив поняття критичної інфраструктури, заклав принципи її захисту, окреслив суб’єктів державної політики та запровадив підхід до ідентифікації об’єктів і операторів критичної інфраструктури [7]. Відповідно до цього закону, Кабінет Міністрів України затверджує перелік секторів і підсекторів критичної інфраструктури, визначає уповноважені органи в цих секторах, а також координує діяльність центральних органів виконавчої влади щодо розроблення і реалізації заходів захисту. Наукові дослідження підкреслюють, що ухвалення цього закону стало переломним моментом переходу від фрагментарного регулювання окремих об’єктів до формування

цілісної системи державної політики у сфері критичної інфраструктури [12; 13; 19].

РНБО України виконує роль координаційного центру на стратегічному рівні: її рішення, введені в дію указами Президента, визначають пріоритети розвитку системи захисту критичної інфраструктури, затверджують базові стратегії й плани, у тому числі щодо кібербезпеки та стійкості [10; 11]. На базі апарату РНБО функціонує Національний координаційний центр кібербезпеки, що забезпечує узгодження дій основних суб'єктів кібербезпеки, у тому числі щодо критичної інформаційної інфраструктури, а також підготовку аналітичних матеріалів для прийняття рішень [9; 27].

На галузевому рівні центральні органи виконавчої влади здійснюють повноваження уповноважених органів у відповідних секторах критичної інфраструктури – енергетики, транспорту, зв'язку, фінансів, охорони здоров'я тощо. У науковій літературі звертається увага на те, що така модель відповідає європейській практиці, коли секторна відповідальність поєднується з міжвідомчою координацією на рівні уряду [20; 34]. Міністерства та відомства розробляють галузеві нормативні акти, визначають критерії критичності об'єктів, координують розроблення планів безпеки й безперервності, здійснюють нагляд за виконанням вимог до операторів. Окремі функції покладаються на незалежні регулятори – зокрема, у сферах енергетики та електронних комунікацій – які встановлюють технічні вимоги, стандарти експлуатації та механізми контролю за операторами інфраструктурних мереж [14; 21].

На операційному рівні ключовими суб'єктами є оператори об'єктів критичної інфраструктури – державні, комунальні та приватні підприємства, що здійснюють експлуатацію відповідних систем і мереж [7; 16]. Законодавство покладає на них обов'язок організувати системи управління безпекою та ризиками, розробляти й впроваджувати плани безпеки, безперервності та реагування на інциденти, забезпечувати захист інформації, у тому числі критичної інформаційної інфраструктури [7; 9; 18]. У роботах українських

авторів наголошується, що саме на рівні операторів відбувається практична реалізація заходів захисту, а ефективність системи загалом значною мірою залежить від їхнього управлінського, фінансового й кадрового потенціалу [15; 17; 18].

Особливу роль відіграють органи, відповідальні за кібербезпеку. Закон України «Про основні засади забезпечення кібербезпеки України» визначає систему суб'єктів кібербезпеки, до якої, зокрема, входять Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ), Національна поліція, Міністерство оборони та Генеральний штаб, розвідувальні органи, а також Національний банк України – у частині захисту фінансової інфраструктури [9]. ДССЗЗІ здійснює функції національного органу у сфері криптографічного й технічного захисту інформації, координує діяльність урядових команд реагування на комп'ютерні надзвичайні події (CERT-UA) та розробляє організаційно-технічну модель кіберзахисту, у тому числі для об'єктів критичної інформаційної інфраструктури [9; 16; 27].

Наукові дослідження підкреслюють, що для ефективної роботи такої багаторівневої моделі необхідні зрозумілий розподіл повноважень і налагоджені механізми координації. Роботи, присвячені аналізу організаційно-правових аспектів захисту критичної інфраструктури в Україні, відзначають ризики дублювання функцій між різними органами, фрагментарність підходів і недостатній розвиток горизонтальної взаємодії [12; 14; 18; 21]. У відповідь на ці виклики пропонуються моделі, які поєднують централізоване стратегічне керівництво (через РНБО, Кабінет Міністрів і спеціалізовані координаційні структури) із децентралізованою відповідальністю операторів та галузевих органів [20; 36].

У міжнародній літературі питання координації розглядається також крізь призму публічно-приватного партнерства. Дослідження підкреслюють, що через значну частку приватної власності у сферах енергетики, транспорту, цифрових послуг держава не може забезпечити захист критичної інфраструктури виключно адміністративними методами; натомість потрібні моделі співуправління, де

приватні оператори залучаються до спільного планування, обміну інформацією, проведення навчань і спільних інвестицій у стійкість [22; 34]. Для України такі підходи набувають особливого значення в умовах повномасштабної агресії, коли від злагодженості дій державних і приватних суб'єктів залежить здатність системи витримувати комбіновані удари по енергетичній, транспортній та цифровій інфраструктурі [14; 26; 36].

Воєнний стан істотно змінює контекст діяльності суб'єктів системи захисту критичної інфраструктури. З одного боку, розширюються повноваження військового командування й органів сектору безпеки та оборони щодо прийняття оперативних рішень, пов'язаних із режимом роботи, евакуацією, маскуванням, розосередженням та охороною об'єктів критичної інфраструктури. З іншого – зростають вимоги до координації між цивільними й військовими структурами, оскільки значна частина об'єктів інфраструктури має подвійне (цивільне й військове) значення, а їх знищення чи виведення з ладу впливає одночасно на обороноздатність і повсякденне життя населення [14; 20; 35; 36]. Дослідження з питань стійкості критичної інфраструктури наголошують, що саме інтеграція цивільного та військового компонентів управління є одним із ключових критеріїв спроможності держави протидіяти сучасним загрозам [25; 31; 35].

Таким чином, система суб'єктів управління захистом критичної інфраструктури в Україні в умовах воєнного стану включає стратегічний рівень (Президент, РНБО, Верховна Рада, Кабінет Міністрів), галузевий рівень (міністерства, відомства, регулятори), операційний рівень (державні, комунальні та приватні оператори), а також спеціалізовані органи кібербезпеки. Їхня ефективна взаємодія залежить від якості координаційних механізмів, чіткості розподілу повноважень і готовності до спільного реагування на комплексні загрози, що підтверджують як українські, так і міжнародні дослідження [12; 14; 20; 22; 34–36].

2.2. Ризик-менеджмент, планування безперервності та реагування на інциденти та загрози

Ризик-менеджмент і планування безперервності діяльності є ключовими елементами сучасних підходів до захисту критичної інфраструктури. У міжнародних стандартах і практиках захисту інфраструктури підкреслюється, що будь-які заходи безпеки повинні будуватися на систематичній ідентифікації загроз, оцінці вразливостей та потенційних наслідків, а також на розробленні планів, які забезпечують продовження або швидке відновлення критичних функцій у разі інцидентів [1; 5; 6; 32; 33]. Стандарти ISO 31000 з управління ризиками та ISO 22301 з управління безперервністю діяльності фіксують базові принципи – контекстність, системність, залучення заінтересованих сторін, цикл «планування–виконання–оцінка–удосконалення» – які дедалі активніше імплементуються у практики захисту критичної інфраструктури різних держав [32; 33].

У сфері критичної інфраструктури ризик-менеджмент має свої специфічні особливості. По-перше, він має враховувати міжгалузеві взаємозалежності: відмова в одному секторі (наприклад, енергетиці) може призвести до каскадних наслідків у транспорті, зв’язку, фінансах та охороні здоров’я, що вимагає комплексного аналізу ризиків на рівні системи в цілому [1; 23; 24]. По-друге, важливо враховувати не лише ймовірність і масштаб окремих подій, а й можливість їхніх комбінацій – одночасних або послідовних ударів по різних елементах інфраструктури. По-третє, у сучасних умовах особливого значення набуває поєднання фізичних і кіберзагроз, коли кібероперації проти систем управління технологічними процесами супроводжуються фізичними атаками на об’єкти інфраструктури [22; 31; 34].

Дослідження українських авторів свідчать, що для України в умовах війни характерний комплексний, «багаторівневий» набір загроз критичній інфраструктурі: від масованих ракетних та дронових ударів по енергетичних об’єктах до кібератак на системи управління, диверсійних дій, внутрішніх техногенних аварій, посилених зношеністю основних фондів і браком ресурсів на їхню модернізацію [14; 16–18; 26]. На цій основі запропоновані моделі загроз, які враховують не лише окремі сценарії, а й їхню комбінацію, що дозволяє

будувати більш реалістичні карти ризиків для національної критичної інфраструктури [26].

Важливою складовою є розроблення та впровадження планів безперервності діяльності (Business Continuity Plans) операторів критичної інфраструктури. У міжнародній практиці такі плани включають визначення критичних функцій, аналіз впливу на бізнес (Business Impact Analysis), розроблення стратегії безперервності (резервування потужностей, альтернативні маршрути, сценарії ручного управління), планів реагування на інциденти й планів відновлення [32; 33]. Для України, де значна частина інфраструктури була спроєктована ще в радянський період і довгий час експлуатувалася без системних підходів до безперервності, імплементація таких практик є складним, але необхідним завданням [14; 18; 20].

Законодавство України у сфері критичної інфраструктури містить вимоги щодо застосування ризик-орієнтованих підходів і планування безперервності. Закон «Про критичну інфраструктуру» передбачає обов'язок операторів здійснювати оцінку ризиків, розробляти плани безпеки й безперервності, узгоджувати їх із компетентними органами та забезпечувати їх актуальність [7; 16]. Закони у сфері національної безпеки та кібербезпеки доповнюють цю рамку, зобов'язуючи суб'єктів забезпечувати захист інформації, систем управління та реагування на кібератаки [8; 9]. Аналітичні матеріали НІСД наголошують, що практична реалізація таких вимог потребує розроблення стандартів і методичних рекомендацій, навчання персоналу та створення інституційної спроможності органів влади оцінювати якість планів безперервності операторів [13; 14; 36].

Окремий напрям – організація реагування на інциденти. Під інцидентами в контексті критичної інфраструктури розуміють події, які призводять або можуть призвести до переривання функціонування об'єктів, погіршення якості послуг, створення загрози життю та здоров'ю людей, довкіллю чи національній безпеці [7; 9; 23]. Система реагування включає кілька рівнів: (1) операторський рівень – оперативні диспетчерські служби, аварійні бригади, внутрішні центри реагування; (2) галузевий рівень – ситуаційні центри міністерств і регуляторів;

(3) державний рівень – координаційні центри при РНБО, ДСНС, ДССЗЗІ та інших органах [11; 14; 27].

У сфері кібербезпеки ключовим елементом є діяльність урядової команди реагування CERT-UA, яка фіксує, класифікує та допомагає усувати кіберінциденти в інформаційних системах державного сектору, а також на об’єктах критичної інфраструктури [27; 30]. Статистика CERT-UA та ДССЗЗІ свідчить про стрімке зростання кількості кіберінцидентів після початку повномасштабної агресії – від кількох тисяч у 2022–2023 роках до понад чотирьох тисяч зареєстрованих кібератак у 2024 році, при цьому поступово зменшується частка інцидентів, що мають критичні наслідки, завдяки посиленню системи реагування [28–30]. Це демонструє значення розвиненої системи моніторингу, раннього виявлення й оперативної реакції на кіберзагрози для стійкості критичної інфраструктури.

У дослідженнях з проблем стійкості критичної інфраструктури підкреслюється, що ризик-менеджмент і планування безперервності мають розглядатися не лише на рівні окремих об’єктів чи операторів, а й на рівні держави в цілому – через проведення національних оцінок ризиків, визначення пріоритетних секторів і «вузьких місць», розроблення сценаріїв реагування на масштабні надзвичайні ситуації [23; 25; 31; 34; 35]. Для України, яка протистоїть повномасштабній агресії, такі оцінки включають сценарії масованих атак на енергетичну систему, транспортні коридори, цифрову інфраструктуру, а також комбінації цих атак із внутрішніми техногенними аваріями.

Наукові праці відзначають, що перехід від концепції «захисту» до концепції «стійкості» означає зміщення акценту з виключно превентивних заходів на інтегрований підхід, який охоплює підготовку, витримування удару, адаптацію та відновлення [14; 25; 31; 36]. У цьому контексті ризик-менеджмент і планування безперервності слугують інструментами, які дозволяють не тільки зменшувати ймовірність інцидентів, а й забезпечувати гнучкість та здатність системи швидко відновлюватися після них.

Таким чином, у системі захисту критичної інфраструктури України в умовах воєнного стану ризик-менеджмент, планування безперервності та реагування на інциденти виступають взаємопов’язаними елементами, що спираються на міжнародні стандарти, національне законодавство та практику операторів. Їх подальший розвиток пов’язаний із поглибленням аналітичної бази, удосконаленням методик оцінки ризиків, навчанням персоналу, інтеграцією фізичних і кіберкомпонентів та підвищенням рівня координації між усіма суб’єктами системи [7–9; 14; 23; 26; 31–33; 36].

2.3. Кіберзахист та інформаційна безпека критичної інфраструктури: організаційні та технічні механізми

Кіберзахист критичної інфраструктури в Україні з початку повномасштабної агресії Російської Федерації набув особливого значення, оскільки інформаційно-комунікаційні системи, системи управління технологічними процесами та критична інформаційна інфраструктура стали одним із головних об’єктів атак [9; 27–29]. У міжнародних документах ЄС та НАТО наголошується, що кібербезпека є невід’ємною складовою захисту критичної інфраструктури, а забезпечення її стійкості в кіберпросторі розглядається як ключовий елемент національної безпеки [3; 4; 34; 35].

Правовою основою кіберзахисту критичної інфраструктури в Україні є Закон «Про основні засади забезпечення кібербезпеки України», який вводить поняття об’єктів критичної інформаційної інфраструктури та визначає особливі вимоги до їхнього захисту [9]. Закон встановлює коло суб’єктів кібербезпеки, їх повноваження та завдання, а також принципи взаємодії між ними. Додаткові вимоги встановлюються законодавством у сфері захисту інформації, державної таємниці, технічного й криптографічного захисту інформації [9; 27]. У подальшому ці норми деталізуються підзаконними актами – постановами Кабінету Міністрів України та наказами ДССЗЗІ, які регламентують порядок

проведення оцінки стану кіберзахисту, виявлення вразливостей, реагування на інциденти, а також експлуатацію засобів технічного захисту інформації [27].

З організаційної точки зору кіберзахист критичної інфраструктури в Україні спирається на діяльність кількох ключових структур. ДССЗЗІ виконує функції національного органу з кіберзахисту, забезпечує роботу урядової команди реагування CERT-UA, координує створення й розвиток національного сегмента системи виявлення вразливостей та реагування на кіберінциденти [27; 30]. CERT-UA здійснює моніторинг кіберпростору, аналіз загроз, обробку інцидентів, надає рекомендації операторам щодо усунення вразливостей і відновлення нормального функціонування систем [30]. Статистичні дані свідчать, що кількість оброблених кіберінцидентів суттєво зросла після 2022 року, при цьому переважна більшість з них пов’язана з діяльністю кібератакувальних угруповань, афілійованих із державою-агресором, та спрямована на органи влади, оборонний сектор, енергетику, телекомунікації й інші критичні сектори [28–30].

Міжнародні аналітичні звіти, присвячені кіберсередовищу України, підтверджують, що з 2022 року фіксується значне зростання кількості кібератак, але водночас – поступове підвищення ефективності системи кіберзахисту та зниження частки інцидентів із важкими наслідками [28; 29]. У звітах підкреслюється, що Україні вдалося створити модель, яка поєднує централізоване управління з активною участю приватного сектору й міжнародних партнерів, а також оперативну мобілізацію волонтерських і професійних ІТ-спільнот [28; 29; 31].

Технічні механізми кіберзахисту критичної інфраструктури включають кілька рівнів. По-перше, це захист мережевої інфраструктури – використання міжмережевих екранів, систем виявлення та запобігання вторгненням, сегментація мереж, захищені канали зв’язку. По-друге, захист кінцевих точок – антивірусні рішення, контроль доступу, моніторинг активності. По-третє, спеціалізовані засоби захисту систем управління технологічними процесами (SCADA, ICS), які враховують специфіку промислових протоколів і високі

вимоги до безперервності роботи [22; 31; 34]. Дослідження з кіберстійкості наголошують, що для критичної інфраструктури важливо не лише запобігати проникненню, а й забезпечувати здатність систем швидко виявляти аномалії, ізолювати уражені сегменти, продовжувати виконання критичних функцій і відновлюватися після атак [25; 31].

Суттєвим компонентом є впровадження систем моніторингу подій інформаційної безпеки та керування інцидентами (SIEM/SOAR), які дозволяють збирати дані з різних джерел, корелювати їх та оперативно реагувати на підозрілі події. У національних документах і рекомендаціях ДССЗЗІ передбачено створення організаційно-технічної моделі кіберзахисту, що базується на мережі сенсорів, центрах моніторингу та реагування, стандартизованих процедурах обміну інформацією між суб’єктами кібербезпеки [27]. Для об’єктів критичної інфраструктури ці вимоги означають обов’язок впровадження комплексних систем захисту, інтегрованих з національними платформами моніторингу.

Організаційні механізми кіберзахисту включають політики безпеки, регламенти доступу, процедури управління вразливостями, навчання персоналу та регулярні аудити. Аналітичні дослідження українських і міжнародних експертів свідчать, що людський фактор залишається однією з головних причин успіху кібератак, і саме тому значна увага приділяється тренінгам, симуляціям фішингових кампаній, підвищенню культури безпеки серед персоналу критичної інфраструктури [23; 24; 29; 31]. Новітні підходи до оцінки стійкості кіберсистем пропонують використовувати набори показників, які враховують не лише наявність технічних засобів захисту, а й рівень готовності до реагування, здатність системи адаптуватися й відновлюватися [31].

Міжнародні рамкові документи, зокрема Директива NIS2 у ЄС, а також рекомендації ENISA, встановлюють вимоги до кіберзахисту постачальників основних послуг, зокрема в енергетичному, транспортному, фінансовому, цифровому й інших секторах критичної інфраструктури [3; 4; 34]. У них підкреслюється обов’язковість впровадження систем управління інформаційною безпекою, проведення регулярних оцінок ризиків, забезпечення звітності перед

компетентними органами та повідомлення про інциденти. Для України імплементація цих підходів означає необхідність гармонізації національного законодавства з європейським правом, посилення вимог до операторів критичної інформаційної інфраструктури та вдосконалення механізмів контролю [7–9; 27; 34; 36].

Важливим напрямом є інтеграція кіберзахисту в ширшу концепцію стійкості критичної інфраструктури. Дослідження у сфері критичної інфраструктури й кібербезпеки наголошують, що повністю усунути ризики кібератак неможливо; завдання полягає в тому, щоб мінімізувати їхні наслідки, забезпечити можливість продовження критичних функцій і відновлення після інцидентів [25; 28; 31]. Для України це означає необхідність будувати системи, здатні працювати в умовах постійного кібертиску, масованих атак, спроб вивести з ладу енергосистему, транспортні вузли чи цифрову інфраструктуру управління.

Таким чином, кіберзахист і інформаційна безпека критичної інфраструктури в Україні в умовах воєнного стану формуються на основі поєднання нормативно-правових вимог, організаційних структур (ДССЗЗІ, CERT-UA, Національний координаційний центр кібербезпеки), технічних засобів захисту, систем моніторингу та реагування, а також заходів із підвищення культури безпеки серед персоналу й користувачів. Міжнародні стандарти та практики, досвід партнерів, аналітичні звіти про кіберзагрози й уроки, отримані в ході відбиття масованих атак, слугують основою для подальшого удосконалення цієї системи й підвищення стійкості критичної інфраструктури України [3; 4; 9; 22; 27–31; 34–36].

Висновки до розділу 2

У розділі узагальнено, що система управління захистом критичної інфраструктури в Україні в умовах воєнного стану є багаторівневою та ґрунтується на поєднанні стратегічного формування політики й координації, галузевого регулювання та операційної відповідальності операторів

інфраструктури. Систематизовано коло ключових суб’єктів і доведено, що результативність цієї моделі визначається не кількістю залучених органів, а чіткістю розподілу повноважень, узгодженістю процедур, наявністю дієвих координаційних механізмів і спроможністю швидко переходити від стратегічних рішень до практичних дій на рівні секторів та операторів. Обґрунтовано, що в умовах значної частки приватної власності в інфраструктурних секторах держава не може забезпечити належний рівень захисту виключно адміністративними інструментами, а тому ключового значення набувають форми співуправління, узгоджене планування, обмін інформацією та спільні тренування, що підсилюють стійкість системи в цілому.

Доведено, що ризик-орієнтований підхід, планування безперервності діяльності та реагування на інциденти становлять ядро сучасної практики захисту критичної інфраструктури й мають розглядатися як взаємопов’язані елементи єдиного управлінського циклу: від ідентифікації загроз і вразливостей до відновлення критичних функцій. Узагальнено специфіку ризиків для воєнного часу, зокрема комбінованість природних, техногенних, умисних і кіберзагроз та їхню здатність формувати каскадні відмови через міжсекторальні взаємозалежності. Показано, що практична стійкість критичної інфраструктури визначається готовністю операторів і державних структур працювати в режимі тривалого навантаження: підтримувати резервування, альтернативні режими управління, аварійні плани, а також налагоджені канали взаємодії між операторськими, галузевими та загальнодержавними рівнями реагування. Окремо узагальнено, що кіберзахист і інформаційна безпека в умовах війни перетворилися на обов’язкову складову загальної системи захисту критичної інфраструктури, а їхня ефективність залежить від поєднання організаційних механізмів, технічних засобів, моніторингу та реагування, а також системної роботи з людським фактором. У підсумку доведено, що перехід від логіки “охорони” до логіки “стійкості” означає зміщення акценту на здатність системи витримувати удари, адаптуватися та відновлюватися, а ключовими умовами такого переходу є інтеграція фізичного та кіберкомпонентів, стандартизація

підходів до оцінки ризиків і планування, а також підвищення координаційної спроможності суб’єктів управління на всіх рівнях.

РОЗДІЛ 3. НАПРЯМИ ПІДВИЩЕННЯ СТІЙКОСТІ ТА ВДОСКОНАЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1. Оцінка спроможностей і прогалин: аудит, індикатори, пріоритезація

Оцінка спроможностей системи захисту критичної інфраструктури та виявлення ключових прогалин є відправною точкою для будь-якої політики підвищення стійкості. У міжнародній практиці та аналітичних документах ООН, ЄС і провідних дослідницьких центрів підкреслюється, що ефективна система захисту критичної інфраструктури неможлива без систематичного вимірювання рівня ризиків, стійкості й результативності вжитих заходів [37; 41]. Така оцінка поєднує кілька взаємопов'язаних компонентів: аудит (зовнішній і внутрішній), систему індикаторів (ключових показників) та механізми пріоритезації, які дозволяють приймати обґрунтовані рішення щодо розподілу обмежених ресурсів.

У дослідженнях, присвячених стійкості критичної інфраструктури, відзначається, що традиційний технічний або відомчий підхід до оцінювання безпеки окремих об'єктів є недостатнім. Натомість необхідно переходити до системної оцінки, яка враховує міжсекторальні залежності, можливість каскадних відмов, а також здатність системи не лише протидіяти інцидентам, а й швидко відновлюватися після них [31; 37; 41]. Для цього використовуються різні рамкові моделі – від загальних стандартів управління безперервністю діяльності (ISO 22301) та ризик-менеджменту (ISO 31000) до спеціалізованих керівництв і чек-лістів, розроблених для аналізу стійкості інфраструктурних систем [32; 33; 37].

Важливу роль відіграє розвиток системи індикаторів стійкості критичної інфраструктури. У низці міжнародних досліджень запропоновано багаторівневі системи індикаторів, які охоплюють технічні, організаційні, соціальні та

економічні аспекти стійкості [24; 38; 40]. Наприклад, виділяються індикатори «жорсткої» стійкості (фізична захищеність, резервування потужностей, наявність альтернативних маршрутів), «організаційної» стійкості (наявність планів безперервності, частота тренувань, рівень координації між суб'єктами), а також індикатори «адаптивності» й «навчання» (швидкість оновлення планів після інцидентів, обсяг інвестицій у модернізацію та кіберзахист) [39; 40]. У європейських галузевих керівництвах окремо наголошується, що індикатори мають бути не лише кількісними, а й якісними, відображаючи готовність персоналу, культуру безпеки та рівень довіри між учасниками системи [37; 40].

Український контекст поступово інтегрує подібні підходи. У працях, присвячених національній системі захисту критичної інфраструктури, пропонуються методики оцінки рівня критичності об'єктів, що враховують масштаби можливих наслідків для населення, економіки, довкілля та національної безпеки, а також ступінь залежності інших об'єктів від конкретної інфраструктури [15; 17; 20]. Низка новіших досліджень та аналітичних документів фокусуються вже не лише на «критичності», а й на «стійкості», тобто здатності системи зберігати або відновлювати функції після інциденту [36; 41; 48]. У цьому контексті актуальним стає перехід від разових обстежень до регулярного моніторингу ключових показників стійкості.

Окремий блок інструментів – аудит. Міжнародний досвід вказує, що верховні органи фінансового контролю (рахункові палати, аудиторські інституції) відіграють важливу роль у незалежній оцінці здатності держави забезпечувати захист критичної інфраструктури [26; 43]. У ряді країн розроблено спеціальні критерії та методики аудиту політики в цій сфері: аналіз відповідності законодавчої бази, інституційної координації, планування й виконання програм, ефективності витрат на заходи безпеки. В Україні, зокрема, здійснювалися аудити експериментальних проєктів із захисту критичної інфраструктури паливно-енергетичного сектору, які виявили як позитивні напрацювання (створення пілотних механізмів захисту), так і суттєві недоліки в координації, плануванні й оцінці результатів [47].

Паралельно формується інститут незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури. Законодавчі й підзаконні акти встановлюють вимоги до аудиторів, порядок їхньої атестації, включення до реєстру, а також визначають загальні підходи до проведення такого аудиту [9; 44; 46]. Офіційні роз’яснення відповідальних органів підкреслюють, що незалежний аудит має бути систематизованим, базуватися на визнаних стандартах і охоплювати не лише технічні вимоги, а й організаційні процеси, підготовку персоналу, управління інцидентами [45; 53]. У поєднанні з внутрішніми аудитами операторів це створює багаторівневу систему контролю за станом безпеки.

Суттєвим завданням є встановлення зв’язку між результатами аудиту, системою індикаторів та процесом пріоритезації. У керівництвах ООН та ЄС щодо побудови стійкості критичної інфраструктури наголошується, що дані аудиту й моніторингу мають бути інтегровані в процес управління ризиками на всіх рівнях – від окремого об’єкта до національної стратегії [31; 37; 41]. Це означає, що на основі кількісних та якісних показників слід визначати, які саме об’єкти, сектори чи регіони потребують першочергових інвестицій, законодавчих змін або посиленої уваги з боку державних органів.

Питання пріоритезації особливо актуальне для України, де ресурси на захист і відновлення критичної інфраструктури обмежені, а масштаби руйнувань – дуже значні [56; 59]. Оцінки, проведені міжнародними фінансовими інституціями, свідчать про сотні мільярдів доларів потреб у відновленні, значна частина яких пов’язана саме з інфраструктурою енергетики, транспорту, житлово-комунального господарства та цифрової інфраструктури [54–56]. У таких умовах застосування ризик-орієнтованих підходів та індикаторів стійкості дозволяє зосередити ресурси на тих об’єктах і проєктах, де кожна вкладена гривня дає найбільший ефект з точки зору зниження системних ризиків.

Окремі дослідження пропонують практичні методики використання індикаторів для пріоритезації, що включають побудову «карт стійкості», інтегральних індексів, матриць ризик–вплив для різних секторів та територій [24;

38; 40]. В українських роботах дедалі частіше підкреслюється, що такі індикатори мають застосовуватися не лише на рівні технічних систем, а й у ширшому контексті – наприклад, при аналізі релокації бізнесу, відновлення промисловості, розвитку «смарт-інфраструктури» міст [36; 48; 59; 60]. Це дає змогу пов’язати політику захисту критичної інфраструктури з політикою регіонального розвитку, відновлення та модернізації економіки.

У підсумку, оцінка спроможностей і прогалин у системі захисту критичної інфраструктури вимагає комплексного підходу, що поєднує незалежний та внутрішній аудит, розвинену систему індикаторів стійкості, а також прозорі механізми пріоритезації. Для України ключовими завданнями залишаються інституціоналізація таких механізмів, забезпечення їх регулярного застосування в державному управлінні й інтеграція результатів оцінки в планування реформ, програм відновлення та інвестицій у стійкість [37; 41; 47; 54–56].

3.2. Посилення міжвідомчої взаємодії, стандартів і підготовки персоналу

Міжвідомча взаємодія, уніфіковані стандарти та системна підготовка персоналу є трьома опорними елементами, без яких захист критичної інфраструктури не може бути ефективним. Досвід країн НАТО та ЄС показує, що навіть за наявності розвиненої нормативної бази та інвестицій у «тверду» інфраструктуру система залишається вразливою, якщо немає чіткого розподілу ролей між суб’єктами, узгоджених процедур реагування та кваліфікованих кадрів [35; 41; 58].

Агресор чудово обізнаний про надмірну залежність України від імпорту енергоносіїв, невирішені проблеми диверсифікації джерел і маршрутів їх постачання, недостатнє використання власного енергетичного потенціалу, низьку ефективність використання паливно-енергетичних ресурсів, відносно повільні темпи впровадження новітніх технологій, тому й надалі, крім суто військових засобів, використовуватиме в тактичній перспективі проблеми

недостатньої реалізації енерготранзитного потенціалу та інтеграції України в європейський енергетичний ринок.

Руйнування або нанесення значних збитків об'єктам критичної інфраструктури у ключових містах (містах-мільйонниках, адміністративно-промислових центрах, вузлах комунікацій, центрах енергогенерації тощо) матиме на меті захоплення контролю над місцевими громадами, здійснення впливу на настрої людей, маніпулювання їхньою свідомістю, кінцевою ціллю чого буде формування протестних настроїв та посилення тиску на центральні органи влади держави з метою примушення їх до прийняття вигідних противнику рішень. Ворог одночасно з маніпулюванням об'єктами критичної інфраструктури намагатиметься маніпулювати також основними цінностями, мотиваційними факторами, культурним базисом, а також стратегічною і комунікаційною інфраструктурою держави.

Агресор буде досягати цього комплексним, збалансованим впливом з використанням "м'якої" та "твердої" сили. Саме тому об'єкти критичної інфраструктури стали об'єктами асиметричних дій ворога, котрий продовжує діяти в парадигмі гібридного конфлікту. Вплив на них у межах оптимальних заходів та кореляцій параметрів простору, часу та ресурсів, за замислом РФ, має призвести до бажаних для неї цілеспрямованих, швидких, каскадних, синергетичних та деструктивних для української критичної інфраструктури порушень у структурах, процесах та результатах функціонування.

Організовуючи протидію ворожому впливу, українське суспільство має пам'ятати, що агресор намагається послабити підтримку Уряду України, застосовуючи не лише кінетичні операції. У міждержавному протистоянні РФ використовує продажність місцевих еліт як інструмент ослаблення та розвалу держави, формує "сіру зону" як театр гібридної війни, заперечує факт ведення гібридної війни, приховано застосовує комплекс гібридних загроз, всеосяжно охоплюючи територію України, зокрема космічний та кіберпростір, і здійснює когнітивний руйнівний вплив на свідомість та психіку людей з метою прискорення поразки у війні нашої держави.

Такі дії прикриваються заходами багатосферного стримування (дипломатичні, інформаційні, розвідувально-агентурні, ідеологічні, зокрема релігійні). Дії РФ синхронізуються за місцем, часом, видами та інтенсивністю використання гібридних загроз на всій території України. Таким шляхом формується внутрішній чинник, котрий у поєднанні з наявністю великих проблем (відсутність у холодну пору року тепла, електрики, питної води, обмеження транспортного сполучення, доступу до медичних, фінансових, соціальних послуг) і відсутністю перспектив щодо їх вирішення у найближчому майбутньому має доповнити чинник активних дій (зовнішній чинник). А цей чинник після Харківського розгрому виглядає все більш примарним, тому має бути негайно посилений чи компенсований за рахунок внутрішнього, що і відбулося вночі з 18 на 19 вересня – агресор завдав ракетного удару по промисловому майданчику Південноукраїнської АЕС.

Слід виділити три рівні:

– національний рівень;

– рівень територіальних громад;

– рівень громадянина.

На національному рівні слід негайно приділити увагу підвищенню ефективності використання енергетичних ресурсів, відшукати альтернативні джерела енергозабезпечення, забезпечити стабільність постачання паливно-енергетичних ресурсів, зокрема шляхом диверсифікації його джерел, забезпечити умови надійного функціонування вітчизняної інфраструктури транзиту та постачання енергоносіїв, створити стратегічні резерви паливно-енергетичних ресурсів. Пріоритет має належати зараз дієвому захисту критичної інфраструктури від ворожих впливів та зловмисних дій, зокрема й у кіберпросторі.

На рівні територіальних громад слід зосередитись на заходах із запобігання аваріям та катастрофам на об’єктах ЖКГ, інших аварійних об’єктах комунальної власності, забезпеченні стабільного функціонування теплових пунктів, систем енергозабезпечення, водопостачання і водовідведення в населених пунктах ОТГ,

створенні фінансових ресурсів для ліквідації наслідків аварій, наданні допомоги комунальним підприємствам всебічно підготуватися до функціонування в умовах воєнного конфлікту високої інтенсивності та в екстремальних умовах холодної пори року. Слід приділити увагу забезпеченню зв'язку та інформування населення, уточнити плани евакуації населення та розробити плани прийому населення, що прибуває до ОТГ з регіонів, які зазнали ворожого впливу та тимчасово малопридатні для проживання. Варто розглянути питання створення територіальних пунктів обігріву, стабільного енергопостачання від мобільних джерел, регулярної доставки питної води, накопичити запаси продовольства тривалого зберігання та такого, приготування якого не потребує значних витрат енергії, подбати про випікання хлібу. Безумовно, обладнати або привести до ладу сховища та укриття для жителів громади лягає на плечі місцевого органу самоврядування. У кожному населеному пункті ОТГ має бути доступ до медичної допомоги. Краща відповідь на надзвичайну ситуацію – чіткий план дій.

На рівні громадянина слід ретельно подбати про автономність виживання родини, створивши необхідні запаси продовольства, пального, медикаментів, зокрема антибіотиків, обладнати в оселі укриття, якщо відсутній доступ до колективного, і там також мати певні запаси на випадок перебування впродовж декількох діб.

Варто підготувати валізу екстреного випадку (вагою 15–20 кг, не більше), поклавши туди документи, готівкові гроші, воду, їжу та змінний одяг, аптечку, засоби гігієни, засоби комунікації: мобільний телефон, пауербанк, універсальний інструмент, засіб для розпалювання, казанок для приготування їжі, таблетки для очищення води, ліхтар; якщо маєте – спальник, намет.

Варто домовитися із сусідами, подбати про одиноких громадян, адже колективне виживання у випадку руйнування об'єктів критичної інфраструктури є ресурсно більш вигідним. Кожен має чітко усвідомлювати, що і як він, його родина, сусіди мають робити за тих чи інших умов.

Захист критичної інфраструктури держави – не лише ППО, не лише комплекс суто військових заходів. Українське суспільство останні 400 років

залишається “суспільством-мішенню” для Росії. Тому для створення нестабільної ситуації в Україні агресор прагне отримати по можливості панування у політичному, соціально-економічному просторах, впливати на наші цінності. Очевидно, що лише у випадку синергії військових та невійськових зусиль стає можливим ефективно організувати і використати “революційну силу” суспільства та скерувати її на зміну військово-політичного керівництва нашої країни. Ось у цьому і полягає сутність атак на об’єкти критичної інфраструктури держави.

У рамках європейської політики стійкості критичної інфраструктури акцентовано на багаторівневому управлінні: стратегічні рішення ухвалюються на рівні урядів і наднаціональних інституцій, галузеві заходи – на рівні профільних міністерств і регуляторів, а безпосередня операційна відповідальність покладається на операторів критичної інфраструктури [3; 40]. Водночас між цими рівнями має існувати розвинена система горизонтальної координації. Наприклад, у документах НАТО щодо стійкості підкреслюється, що ключовою умовою є здатність держави забезпечити безперервність управління, енергопостачання, транспортних та комунікаційних послуг навіть у разі масштабних криз, що потребує узгоджених дій урядових, безпекових, регуляторних органів та приватного сектору [35; 58].

В Україні інституційна архітектура захисту критичної інфраструктури формується на основі законодавчих норм про національну безпеку, кібербезпеку і критичну інфраструктуру [7–9; 14]. Координаційну роль відіграють Рада національної безпеки і оборони України, Кабінет Міністрів України та профільні міністерства, а також спеціалізовані органи у сфері кібербезпеки й захисту інформації. У дослідженнях наголошується, що важливим кроком стало створення окремих координаційних механізмів і робочих груп, які об’єднують представників різних секторів для опрацювання питань захисту критичної інфраструктури [12–14; 21; 23]. Водночас подальшого розвитку потребує практична складова міжвідомчої взаємодії – спільні тренування, обмін інформацією про загрози й інциденти, узгоджені протоколи реагування.

Суттєвим елементом зміцнення взаємодії є стандартизація підходів. Міжнародні стандарти з управління безперервністю, ризик-менеджменту та кібербезпеки (зокрема ISO 22301, ISO 31000 та пов’язані стандарти) розглядаються як основа для гармонізації вимог до операторів критичної інфраструктури, незалежно від галузі [32; 33; 39]. Спеціалізовані галузеві керівництва й національні стандарти деталізують ці вимоги з урахуванням особливостей енергетики, транспорту, цифрової інфраструктури тощо [40; 41]. В Україні відбувається поступова імплементація таких підходів у нормативну базу та відомчі документи, зокрема через посилання на міжнародні стандарти у вимогах до операторів, аудиторів та планів безпеки [7–9; 16–18; 46].

Особливо помітний прогрес спостерігається у сфері кіберзахисту критичної інфраструктури. Аналітичні огляди правового поля наголошують, що Україна протягом останніх років привела низку своїх актів у відповідність до європейських підходів у сфері кібербезпеки, особливо щодо об’єктів критичної інформаційної інфраструктури, процесів реагування на інциденти, ролі національних центрів реагування та спеціалізованих підрозділів [9; 27; 42]. Значний внесок у розвиток стандартів і практик зробили міжнародні проєкти допомоги, спрямовані на посилення кіберстійкості критичної інфраструктури, модернізацію технічних засобів та впровадження кращих практик [28; 43].

Паралельно з розвитком нормативної бази та інституційної структури не менш важливою є підготовка персоналу. У сучасних дослідженнях підкреслюється, що кадровий компонент є однією з трьох основ стратегії зміцнення стійкості поряд із технологічними рішеннями та належним управлінням [36; 50]. Йдеться не лише про технічних фахівців, а й про управлінців, які відповідають за планування безпеки, координацію із суміжними структурами, комунікацію з органами влади та населенням. У збірниках матеріалів науково-практичних конференцій, присвячених резильєнтності критичної інфраструктури, особлива увага приділяється питанням підготовки кадрів, формуванню навичок реагування на інциденти, кризового менеджменту, використання цифрових інструментів моніторингу й кіберзахисту [48; 49].

Українські дослідники пропонують моделі інтегрованої підготовки фахівців із захисту критичної інфраструктури, які поєднують теоретичну підготовку, моделювання сценаріїв, практичні тренування та міжвідомчі навчання [50; 51]. Зокрема, акцент робиться на спільній підготовці персоналу різних складових сил оборони, органів сектору безпеки, операторів критичної інфраструктури й органів місцевого самоврядування, що має забезпечити узгодженість дій у разі кризових ситуацій. Наголошується, що така підготовка повинна охоплювати як «традиційні» аспекти, пов’язані з фізичною безпекою та цивільним захистом, так і сучасні напрями – кіберстійкість, комунікацію в умовах криз, взаємодію з громадськістю та медіа [48; 50–52].

Не менш важливим є системне проведення навчань та тренувань на об’єктах критичної інфраструктури. Методичні матеріали та аналітичні публікації підкреслюють необхідність регулярних комплексних навчань, що включають відпрацювання різних сценаріїв – від природних і техногенних аварій до комбінованих кібер-фізичних атак [22; 23; 52; 53]. Важливо, щоб у таких навчаннях брали участь не лише працівники об’єкта, а й представники органів влади, силових структур, аварійно-рятувальних служб, що дозволяє перевірити й удосконалити механізми взаємодії на практиці.

Додатково в наукових працях звертається увага на необхідність розвитку «культури безпеки» в організаціях, що експлуатують критичну інфраструктуру. Це означає, що вимоги безпеки повинні бути інтегровані в щоденні процеси управління, систему мотивації персоналу, внутрішні процедури обміну інформацією та прийняття рішень [39; 41; 48]. Без такого культурного підґрунтя навіть найкращі формальні стандарти й програми підготовки ризикують залишитися формальністю.

Узагальнюючи, посилення міжвідомчої взаємодії, стандартизації та підготовки персоналу є ключовим напрямом підвищення стійкості критичної інфраструктури. Для України пріоритетними завданнями виступають: завершення інституційного оформлення системи координації; подальша гармонізація національних вимог зі стандартами ЄС і НАТО; розгортання

системи базової й безперервної підготовки персоналу, у тому числі на міжвідомчій основі; а також формування культури безпеки в організаціях-операторах [36; 41; 48–52; 58].

3.3. Інвестиції у стійкість, відновлення та інтеграція кращих практик управління ризиками

Інвестиції у стійкість критичної інфраструктури та інтеграція кращих практик управління ризиками є вирішальним чинником для довгострокової безпеки й розвитку держави. У сучасних дослідженнях наголошується, що витрати на підвищення стійкості необхідно розглядати не як «додатковий тягар», а як інвестиції, які зменшують майбутні збитки від інцидентів, скорочують час відновлення та підвищують конкурентоспроможність економіки [31; 37; 41]. Для України це питання набуває особливої актуальності з огляду на масштаб руйнувань, завданих критичній інфраструктурі внаслідок збройної агресії.

Для українського контексту воєнного часу й післявоєнного відновлення критичної інфраструктури особливо важливо не зводити відбудову до “повернення як було”, а закладати стійкість як обов’язковий параметр інвестиційних рішень – від проєктування та вибору технологій до експлуатації, моніторингу й модернізації. У цьому сенсі доречно використати логіку та формулювання ОЕСР, які підкреслюють гіперзв’язність інфраструктур, каскадність наслідків збоїв, роль інновацій і цифровізації у зміні ризикового ландшафту, а також “вікно можливостей”, що відкривається через зростання інвестицій у відновлення і розвиток інфраструктури, якщо стійкість інтегрується “з самого початку” (OECD, “Good Governance for Critical Infrastructure Resilience”, OECD Reviews of Risk Management Policies).

Критична інфраструктура є основою нашої сучасної та взаємопов’язаної економіки. Порушення роботи критично важливих систем та основних послуг, таких як телекомунікації, енерго- та водопостачання, транспортні та фінансові системи, може призвести до значних економічних збитків. Ці системи є дуже

вразливими до різноманітних потрясінь – від кліматичних і геологічних небезпек до промислових аварій, терористичних і кібератак, які можуть спричинити каскадний негативний вплив на місцевому і навіть глобальному рівнях.

Враховуючи гіперзв'язність цих основних інфраструктурних активів, що посилюється цифровою трансформацією, необхідна комплексна державна політика для посилення стійкості критичної інфраструктури. Мета полягає в тому, щоб обмежити ризик перебоїв у наданні основних послуг і підвищити здатність до швидкого відновлення після шоку. Забезпечення безперервності надання послуг критичної інфраструктури має бути невід'ємною частиною політики управління ризиками як в країнах-членах ОЕСР, так і в країнах-партнерах, як зазначено в Рекомендаціях ОЕСР щодо управління критичними ризиками.

У звіті (OECD, "Good Governance for Critical Infrastructure Resilience", OECD Reviews of Risk Management Policies).розглядається еволюція ландшафту ризиків та політичні корективи, необхідні для посилення стійкості критичної інфраструктури. Аналіз показує, що для ефективного подолання складності та взаємозалежності в інфраструктурі найкраще підходить послідовний, системний підхід. Партнерство між урядом та операторами інфраструктури також може сприяти більшому обміну інформацією та інвестиціям у стійкість. Інструментарій з управління стійкістю критичної інфраструктури надає конкретні рекомендації щодо реформ, зосереджуючи увагу на розбудові стійкості на випередження.

Основні висновки: з середини 2000-х років уряди розробляють і впроваджують державну політику на підтримку захисту критичної інфраструктури. Більшість країн ОЕСР визначили сектори критичної інфраструктури, провели інвентаризацію активів і запровадили нормативно-правові акти, національні програми або механізми стимулювання для посилення стійкості критичної інфраструктури до шокових подій.

Однак ці політики, які здебільшого визначалися порядком денним у сфері безпеки після 11 вересня, не завжди були ефективними у вирішенні проблем

більш складного, взаємопов'язаного з цифровими технологіями середовища двадцять першого століття. Сучасна політика забезпечення стійкості критичної інфраструктури повинна враховувати різноманітні і складні шокові події, більш взаємозалежні системи і країни, а також швидкий темп інновацій в інфраструктурних секторах. Старіння інфраструктури також становить зростаючий політичний виклик.

Інвестиції в інфраструктуру зростають у всьому світі, надаючи країнам можливість переглянути свою політику і підвищити стійкість, одночасно посилюючи стійкість і захист існуючої інфраструктури.

Системний підхід має очевидні переваги при розробці політики щодо критичної інфраструктури. Така політика повинна враховувати всі небезпеки та загрози, забезпечувати координацію між різними секторами (державним і приватним), охоплювати весь життєвий цикл інфраструктури та сприяти транскордонному співробітництву.

Стійкість критичної інфраструктури залежить від співпраці урядів з операторами інфраструктури з державного та приватного секторів. Хоча оператори та уряди погоджуються з необхідністю захисту критично важливих активів і підтримки послуг, їхні погляди на рівень необхідної стійкості, засоби її досягнення та регуляторні вимоги, які повинні застосовуватися, можуть відрізнятися. Ці рішення мають фінансові наслідки і ставлять питання про те, хто буде нести додаткові витрати, пов'язані з інвестуванням у стійкість.

Державно-приватна співпраця між урядами та операторами з метою заохочення діалогу з цих питань є корисною для спільної розробки та впровадження політики забезпечення стійкості та безпеки критичної інфраструктури. Встановлення довіри, забезпечення безпечного обміну інформацією, розробка механізмів розподілу витрат і зміцнення міжнародного співробітництва є одними з ключових завдань, які необхідно вирішити при створенні таких партнерств, і вимагають відповідних механізмів управління.

Уряди можуть обирати з безлічі політичних інструментів для посилення стійкості критичної інфраструктури. Опитування ОЕСР визначило двадцять два

таких інструменти – від нормативно-правових актів і компенсаційних механізмів до добровільних механізмів, заснованих на партнерстві. Урядам важливо знайти правильний баланс між обов'язковими та добровільними механізмами, щоб посилити залучення зацікавлених сторін до цього процесу та забезпечити ефективне інвестування у стійкість.

Приклад фінської системи передачі та розподілу електроенергії ілюструє ефективну модель управління, яка сприяє інвестиціям у стійкість інфраструктури. Фінляндія розробляє рамки співпраці для посилення стійкості критичної інфраструктури, яка наголошує на державно-приватній співпраці, обміні інформацією та досягненні консенсусу щодо розробки політики та встановлення цілей. Ця модель управління дала вражаючі результати в перші роки її впровадження. Тим не менш, з'явилися нові виклики, зокрема вирішення проблем, пов'язаних з витратами для споживачів, різницею в можливостях великих і малих операторів, цифровізацією та зміною клімату.

На шляху до більш структурованого підходу у цьому звіті пропонується Інструментарій з управління стійкістю критичної інфраструктури, який пропонує урядам вирішити наступні сім взаємопов'язаних управлінських викликів:

– створення міжгалузевої структури управління для забезпечення стійкості критичної інфраструктури. Уряди повинні прийняти загальнодержавний підхід до забезпечення стійкості критичної інфраструктури, що охоплює різні ризики та сектори інфраструктури.

– позуміння складних взаємозалежностей і вразливостей в інфраструктурних системах для визначення пріоритетності зусиль з розбудови стійкості. Уряди повинні прийняти методології та метрики для визначення критично важливих функцій, систем та активів, які мають бути пріоритетними для інвестицій у розбудову стійкості.

– встановлення довіри між урядом та операторами шляхом забезпечення обміну інформацією про ризики. Уряди повинні створити платформи для обміну інформацією з операторами критичної інфраструктури для всебічного і

спільного розуміння ризиків і вразливостей, забезпечуючи безпеку і конфіденційність інформації, якою вони обмінюються.

– розбудова партнерств для вироблення спільного бачення та узгодження досяжних цілей у сфері стійкості. Уряди повинні налагодити постійний діалог з операторами критичної інфраструктури з державного та приватного секторів, взявши за відправну точку очікування громадськості.

– визначення комплексу політичних заходів для визначення пріоритетності економічно ефективних заходів з підвищення стійкості на всіх етапах життєвого циклу інфраструктури. Уряди повинні визначити комплекс політичних інструментів на основі аналізу витрат і вигоди, щоб заохотити операторів інвестувати в забезпечення стійкості та досягти поставлених цілей.

– забезпечення підзвітності та моніторингу впровадження політики стійкості критичної інфраструктури. Уряд повинен здійснювати моніторинг впровадження та оцінювати прогрес у досягненні цілей щодо забезпечення стійкості, створивши чітку систему підзвітності для операторів.

– врахування транскордонного виміру інфраструктурних систем. Уряд повинен координувати національну політику стійкості критичної інфраструктури із сусідніми країнами та за її межами, щоб вирішувати питання транскордонної залежності.

Новий ландшафт для інвестицій у критичну інфраструктуру стійкість. Окрім еволюції факторів ризику, сам сектор інфраструктури зазнає значних змін та еволюції, що може вплинути на його стійкість. По-перше, взаємозв’язок і взаємозалежність між інфраструктурними системами та між країнами значно зросли з глобалізацією, що збільшило потенціал для каскадного розвитку шокових подій. По-друге, інновації та технологічний прогрес призводять до появи нових форм і типів інфраструктурних систем – від “розумних міст” до автономних транспортних засобів. Ці нові види “розумної інфраструктури” в основному використовують інновації, спрямовані на зниження витрат і підвищення ефективності, що може мати вплив на ризики і стійкість, які все ще необхідно враховувати та правильно розуміти. Паралельно з появою нової

інфраструктури, у багатьох країнах ОЕСР старіюча інфраструктура створює вразливі місця. По-третє, інвестиції в інфраструктуру зростають у всьому світі, що створює ключову можливість для посилення стійкості з самого початку, за умови, що ці інвестиції інтегрують стійкість у свій дизайн.

Взаємозв'язок і взаємозалежність інфраструктурних активів і систем зростає. Глобальні інвестиції в інфраструктуру, розгортання глобальних ланцюгів доданої вартості, а також розвиток інформаційно-комунікаційних технологій посилили взаємозв'язок і взаємозалежність між секторами та країнами по всьому світу. Збільшення потоків даних, товарів, людей та енергії живить глобальні ланцюги доданої вартості та підтримує економічне зростання. Критична інфраструктура – це центри, вузли і мережі дедалі складнішої павутини взаємозалежностей і взаємозв'язків, через які агенти загроз можуть переміщатися, а наслідки збоїв можуть бути каскадними. Тому збій або порушення роботи однієї системи критичної інфраструктури може мати далекосяжні наслідки в інших секторах або в інших місцях, іноді в глобальному масштабі (OECD, 2011[9]).

Наприклад, масштабні повені 2011 року в Бангкоку суттєво вплинули на автомобільну промисловість Японії, оскільки постачальники, розташовані в зоні затоплення, були виведені з ладу. Транскордонні інфраструктури, такі як високовольтні електромережі, є ще одним способом поширення збоїв. Збої в роботі електроенергетичних або телекомунікаційних систем можуть мати наслідки для інших критично важливих секторів, які залежать від енергопостачання або телекомунікаційних систем, від водоочищення до критично важливих галузей промисловості або державних систем.

Деякі сектори майже повністю залежать від ключової критичної інфраструктури: наприклад, авіаційний сектор залежить від Глобальної системи позиціонування (GPS) для управління маршрутами літаків по всьому світу; глобальний обмін даними залежить від обмеженої кількості підводних кабелів, через які проходить понад 90% світового трафіку даних.

Інновації та цифровізація трансформують інфраструктуру. Інновації трансформують інфраструктурні системи швидкими темпами, що має наслідки для ризиків і вразливостей, які мають бути інтегровані в політику стійкості та безпеки критичної інфраструктури. Від енергетичного до інформаційного та транспортного секторів відбуваються великі трансформації. Енергетичний сектор надає можливості для значних інновацій завдяки зростаючій частці відновлюваних ресурсів, розвитку інтелектуальних мереж, а також більш децентралізованим і локалізованим підходам до виробництва і споживання енергії. Стрімкий розвиток автономних транспортних засобів разом із прогресом у сфері штучного інтелекту обіцяє докорінно змінити транспортний сектор. Інформаційно-комунікаційні технології суттєво змінили спосіб обміну даними та спілкування у нашому повсякденному житті. Розумні міста, що керуються підходом, орієнтованим на дані, мають на меті поєднати інформаційну революцію з інноваційними та взаємопов'язаними міськими послугами, змінюючи вигляд мегаполісів, де проживає більшість населення планети.

Оскільки темпи інновацій продовжують прискорюватися, це має вплив на управління ризиками. Загалом, сучасні інноваційні тенденції свідчать про те, що більш децентралізовані системи та автономні механізми поступово замінюватимуть централізовані мережі з автоматизацією управління та контролю. Такі характеристики можуть посилити стійкість за рахунок надмірності та гнучкості. Однак це також може призвести до появи нових форм вразливостей: збільшення кількості слабких місць у децентралізованих системах і поширеного ризику більш руйнівних кібератак на ці системи, які все більше покладаються на потоки даних і кодування.

Зростаючі інвестиції в інфраструктуру створюють можливості для забезпечення стійкості. На наступні десятиліття заплановані значні інвестиції в нові об'єкти інфраструктури, і це є цінною можливістю забезпечити інтеграцію питань стійкості з самого початку. Нещодавній аналіз ОЕСР свідчить про те, що для покриття потреб в інвестиціях в інфраструктуру на період 2016–2030 років необхідно 95 трильйонів доларів США (OECD, 2017[10]). У багатьох країнах

ОЕСР застаріла інфраструктура потребує інвестицій, а інновації надають можливості для того, щоб ці інвестиції сприяли підвищенню продуктивності.

Для того, щоб такі інвестиції в інфраструктуру були не лише правильними, але й стійкими, необхідно переглянути основні моделі управління інфраструктурою. ОЕСР розробила концепцію кращого управління інфраструктурою (OECD, 2017[11]), яка спрямована на реалізацію правильних проєктів у спосіб, що є економічно ефективним, доступним і викликає довіру у користувачів та громадян. Ця концепція наголошує на необхідності інтегрувати питання стійкості на початковому етапі при розробці цих інвестицій, щоб не лише захистити ці інвестиції від небезпек і загроз, але й забезпечити їхню безперебійну роботу під час стихійних лих.

Зміна клімату вимагатиме також проєктування стійкої інфраструктури, адаптації або модернізації існуючої та розбудови захисної інфраструктури, причому деякі з них вважаються критично важливими. Робота ОЕСР щодо кліматично стійкої інфраструктури (OECD, 2018[12]) містить рекомендації щодо того, як забезпечити кліматичну стійкість за допомогою конкретних проєктів, зміцнення сприятливого середовища для кліматичної стійкості та мобілізації державних і приватних інвестицій [OECD, “Good Governance for Critical Infrastructure Resilience”, OECD Reviews of Risk Management Policies].

Оцінки, проведені міжнародними фінансовими організаціями, свідчать про колосальні потреби у фінансуванні відновлення та модернізації української інфраструктури. Зокрема, останні раунди комплексної оцінки збитків і потреб (Rapid Damage and Needs Assessment) фіксують, що значна частина необхідних інвестицій припадає саме на енергетику, транспорт, комунальну інфраструктуру та об’єкти соціальної сфери, які виконують функції критичної інфраструктури [56]. Окремі дослідження деталізують механізми оцінювання збитків, завданих бойовими діями об’єктам критичної інфраструктури, та підкреслюють необхідність поєднання фінансового й технічного аналізу для планування відновлення [59; 60].

Водночас міжнародні фінансові інституції розглядають відновлення України як можливість для побудови «зеленої» та стійкої інфраструктури, підкреслюючи роль приватних інвестицій та публічно-приватних партнерств [54; 55]. У відповідних звітах наголошується, що приватний сектор може відігравати ключову роль у модернізації енергетичних систем, розвитку відновлюваних джерел енергії, цифрової інфраструктури, модернізації транспортних коридорів та міських мереж, за умови наявності прогнозованої політики, гарантій та прозорих правил гри [54; 55; 57]. При цьому інвестиційні проєкти мають включати елементи підвищення стійкості – резервування потужностей, диверсифікацію джерел, захищені системи управління, кіберзахист, адаптацію до змін клімату.

Окремим напрямом є розвиток галузевих та горизонтальних програм стійкості. Наприклад, у сфері енергетики актуальними стають проєкти зміцнення мереж, створення гнучких і децентралізованих систем, інтеграції відновлюваних джерел з урахуванням вимог безпеки та надійності [23; 41; 57]. У транспортній сфері йдеться про модернізацію ключових коридорів, логістичних вузлів, транспортних вузлів, які мають стратегічне значення для експорту та імпорту, а також для військової мобільності. У цифровій сфері – про розвиток захищених дата-центрів, мереж зв’язку, національних хмарних рішень, систем кіберзахисту для державних органів та операторів критичної інфраструктури [28; 42; 43].

Важливим аспектом політики інвестицій у стійкість є інтеграція кращих практик управління ризиками. Міжнародні та національні документи наголошують, що проєкти модернізації інфраструктури мають ґрунтуватися на системних оцінках ризиків, які враховують природні, техногенні, кібернетичні, а також гібридні загрози [31; 37; 41]. Це передбачає використання методологій, що поєднують аналіз небезпек, уразливостей, можливих наслідків і потенціалу системи до відновлення, а також застосування індикаторів стійкості для оцінки ефективності інвестиційних заходів [24; 38; 40]. У рекомендаціях ООН наголошується на необхідності інтеграції таких підходів у загальнодержавне планування зменшення ризиків лих і адаптації до змін клімату [37].

Українські аналітичні та методичні напрацювання також підкреслюють важливість переходу від «реактивного» до «проактивного» підходу в інвестиціях – від фінансування відновлення після руйнування до заздалегідь спланованих заходів з підвищення стійкості, які здатні запобігти найбільш руйнівним наслідкам інцидентів [14; 20; 36; 48]. Це стосується як державних капітальних вкладень, так і коштів міжнародної допомоги та приватних інвестицій. У цьому контексті важливо, щоб у системі державного управління інвестиційними проєктами були закріплені вимоги щодо оцінки впливу проєкту на стійкість критичної інфраструктури й відповідні критерії відбору.

Значущу роль у практичній реалізації інвестицій у стійкість відіграють галузеві та професійні об’єднання, які ініціюють програми підвищення безпеки в окремих секторах, просувають стандарти, організовують обмін досвідом між українськими та європейськими операторами [22; 57]. Прикладом є ініціативи, спрямовані на посилення безпеки промислових систем керування, розбудову партнерств між промисловістю, постачальниками технологій і державними органами, а також проведення профільних конференцій і воркшопів, присвячених стійкості критичної інфраструктури [48; 57].

Не менш важливий напрям – інвестиції в «м’які» компоненти стійкості: розвиток аналітичних спроможностей державних органів, систем моніторингу, наукових досліджень і вищої освіти в сфері захисту критичної інфраструктури [20; 36; 48; 50]. Створення дослідницьких центрів, розвиток міждисциплінарних освітніх програм, підтримка наукових конференцій і публікацій сприяють накопиченню знань і кращих практик, адаптації міжнародного досвіду до українських реалій, підготовці нового покоління фахівців. Водночас інвестиції в освіту й науку мають бути узгоджені з реальними потребами операторів критичної інфраструктури та органів державної влади.

У підсумку інвестиції у стійкість критичної інфраструктури в Україні повинні ґрунтуватися на комплексному підході, що поєднує:

(1) відновлення зруйнованих об’єктів із одночасною модернізацією й підвищенням рівня безпеки;

(2) впровадження кращих міжнародних практик управління ризиками й індикаторів стійкості;

(3) активне залучення приватного сектору та міжнародних партнерів;

(4) розвиток «м'яких» спроможностей – аналітики, освіти, науки, координаційних механізмів [37; 41; 54–57; 59; 60]. Такий підхід дозволяє перетворити відновлення після руйнувань на інструмент довгострокового зміцнення безпеки, економічної стійкості та інтеграції України в європейський простір безпеки.

Висновки до розділу 3

У третьому розділі узагальнено й системно обґрунтовано напрями підвищення стійкості та вдосконалення державної політики захисту критичної інфраструктури в умовах воєнних загроз і післявоєнного відновлення. Доведено, що результативність цієї політики визначається не окремими "точковими" заходами, а цілісною архітектурою публічного управління, у якій оцінювання, координація, стандарти, підготовка кадрів та інвестиційні рішення функціонують як взаємопов'язані елементи єдиного циклу управління ризиками.

У межах розділу обґрунтовано, що першочерговою умовою підвищення стійкості є регулярна оцінка спроможностей і прогалин, яка поєднує аудит, систему індикаторів та пріоритезацію. Показано, що перехід від відомчого й суто технічного підходу до системної оцінки дає можливість враховувати міжсекторальні залежності, ризик каскадних відмов і реальну здатність до швидкого відновлення. Доведено доцільність побудови багаторівневої системи показників, яка відображає не лише "тверді" компоненти захищеності, а й організаційну готовність, адаптивність і здатність системи навчатися за результатами інцидентів. Узагальнено, що саме зв'язок між аудитом, індикаторами та механізмами пріоритезації забезпечує управлінську логіку розподілу ресурсів у ситуації їх обмеженості та високої вартості помилок у виборі об'єктів і проєктів.

Обґрунтовано, що посилення міжвідомчої взаємодії, уніфікація стандартів і системна підготовка персоналу є другою опорною лінією державної політики, без якої інвестиції та технічні рішення не дають повного ефекту. Доведено, що за умов гібридних впливів і комплексних атак критична інфраструктура потребує не лише захисту об’єктів, а й узгоджених процедур, розподілу ролей, стійких каналів обміну інформацією та відпрацьованих протоколів реагування на різних рівнях управління. Показано, що стандартизація підходів формує спільну “мову” взаємодії, підвищує порівнюваність рішень і забезпечує мінімально необхідний рівень якості управління безпекою незалежно від сектору та типу оператора. Доведено, що кадровий компонент є критично важливим: стійкість підтримується не лише технологіями, а й компетентністю управлінців і фахівців, регулярними навчаннями, спільними тренуваннями та розвитком культури безпеки в організаціях, що експлуатують критичну інфраструктуру.

У третьому розділі також доведено, що інвестиції у стійкість мають бути інтегровані в політику відновлення як обов’язковий критерій, а не як додаткова опція. Обґрунтовано, що відбудова критичної інфраструктури повинна бути спрямована не на відтворення довоєнних моделей, а на модернізацію з урахуванням нових ризиків, цифрової трансформації, зміни кліматичних та кібернетичних загроз і зростання взаємозалежності інфраструктурних систем. Показано, що інвестиційна логіка стійкості передбачає врахування життєвого циклу інфраструктури, поєднання відновлення з резервуванням, диверсифікацією, підвищенням керованості та захищеності систем управління, а також створення умов для залучення приватного сектору й партнерів на прозорих і прогнозованих правилах. Доведено, що найбільшу практичну цінність мають інвестиції, які підкріплюються системними оцінками ризиків та вимірюваними індикаторами результативності, оскільки саме це дозволяє обґрунтовувати пріоритетність проєктів і контролювати досягнення ефекту стійкості.

Узагальнюючи, у третьому розділі обґрунтовано, що підвищення стійкості критичної інфраструктури для України в умовах війни та післявоєнного

відновлення потребує комплексного управлінського рішення, у якому: оцінка й моніторинг забезпечують доказову основу; міжвідомча взаємодія, стандарти і підготовка персоналу створюють узгодженість та операційну спроможність; інвестиції в стійкість формують довгострокову безпеку й економічну стабільність. Доведено, що саме синергія цих складових перетворює політику захисту критичної інфраструктури з реагування на наслідки на проактивну систему запобігання, безперервності функціонування та прискореного відновлення, що є ключовим для збереження керованості держави, життєзабезпечення населення та стійкості економіки.

ВИСНОВКИ

Розкрито зміст поняття “критична інфраструктура” як системи взаємопов’язаних об’єктів, мереж і послуг, безперервність функціонування яких є визначальною для життєзабезпечення населення, стійкості економіки та національної безпеки. Систематизовано основні групи загроз, що впливають на критичні функції, з урахуванням їх багатоприродності, взаємопідсилення та каскадного характеру наслідків в умовах гібридних впливів. Узагальнено та сформульовано базові принципи захисту, орієнтовані на комплексність, ризик-орієнтованість, превентивність, міжсекторальну координацію, пріоритет безперервності надання послуг і відновлюваності, а також узгодження управлінських підходів із європейськими та національними рамками.

Проаналізовано еволюцію державної політики у сфері захисту критичної інфраструктури та визначено її сучасний стан як багаторівневої системи управління, що поєднує стратегічний, галузевий і операційний рівні. Досліджено зміст і логіку цілей політики, які зосереджуються на запобіганні порушенням критичних функцій, зниженні вразливостей, забезпеченні готовності до інцидентів та скороченні часу відновлення. Узагальнено інструменти державного впливу, що охоплюють регулювання, координаційні механізми, планування, моніторинг, партнерства та стимули, і доведено їхню взаємодоповнювальність у межах єдиної управлінської архітектури. Визначено ступінь узгодженості наявних підходів із вимогами права ЄС, окреслено проблемні вузли адаптації та обґрунтовано потребу у підвищенні практичної сумісності процедур, стандартів і механізмів підзвітності.

Охарактеризовано нормативно-правове забезпечення та стандарти захисту критичної інфраструктури в Україні як систему, що формується на перетині сфер національної безпеки, цивільного захисту, кібербезпеки, енергетики, транспорту, зв’язку та інших секторів. Проаналізовано чинні підходи до регулювання та виявлено ключові прогалини й суперечності, пов’язані з фрагментарністю нормативного масиву, різночитанням термінів, нерівномірністю деталізації

вимог у різних секторах, а також недостатньою визначеністю процедур контролю, аудиту та відповідальності. Доведено необхідність посилення нормативної узгодженості, усунення колізій і впровадження більш уніфікованих, результат-орієнтованих підходів до вимог безпеки й стійкості, що забезпечують однакову зрозумілість правил для всіх операторів і суб'єктів управління.

Проаналізовано практики управління ризиками, планування безперервності та реагування на інциденти на об'єктах критичної інфраструктури з погляду їхньої спроможності відповідати сучасному спектру загроз. Досліджено, як поєднання фізичних, техногенних, цифрових і організаційних ризиків створює умови для каскадних порушень та підвищує вимоги до міжсекторальної взаємодії, швидкості прийняття рішень і узгодженості процедур. Визначено ключові напрями підвищення результативності зазначених практик через системність оцінювання, регулярність оновлення планів, інституціоналізацію навчань, інтеграцію даних моніторингу в управлінські рішення та орієнтацію на відновлення критичних функцій у найкоротші строки. Обґрунтовано, що саме перехід від ізольованих об'єктових рішень до системної логіки управління ризиками забезпечує реальне зменшення уразливостей і підвищення стійкості.

Обґрунтовано напрями вдосконалення міжвідомчої взаємодії, стандартизації та підготовки персоналу як трьох взаємопов'язаних і взаємодоповнювальних умов реальної стійкості критичної інфраструктури. Визначено, що вирішальним є не лише формальне розмежування повноважень, а практична здатність діяти за узгодженими протоколами, здійснювати захищений обмін інформацією, проводити спільні тренування та забезпечувати координацію на стратегічному й операційному рівнях. Узагальнено підходи до гармонізації вимог через використання уніфікованих стандартів управління ризиками, безперервності та кіберзахисту, а також доведено значущість кадрової складової, що включає безперервну підготовку, розвиток компетентностей кризового управління і формування культури безпеки в організаціях-операторах. Досліджено, що підвищення якості взаємодії та професійної готовності

персоналу прямо впливає на швидкість реагування, мінімізацію наслідків і здатність системи відновлюватися.

Розроблено та обґрунтовано пропозиції щодо інвестиційної та відновлювальної політики, орієнтованої на стійкість критичної інфраструктури, з урахуванням міжнародного досвіду та потреб повоєнного відновлення України. Доведено, що відбудова має бути спрямована не на просте відтворення довоєнного стану, а на модернізацію із закладанням стійкості як обов'язкового параметра інвестиційних рішень на всіх етапах життєвого циклу інфраструктури. Визначено ключові орієнтири такої політики, що передбачають пріоритетність критичних функцій, ризик-орієнтоване планування, інтеграцію вимог безпеки й кіберстійкості, резервування та диверсифікацію, а також поєднання державних інструментів із залученням приватного сектору й партнерів на основі прозорих правил і підзвітності. Узагальнено, що запропонований підхід перетворює відновлення на інструмент довгострокового зміцнення безпеки, економічної стійкості та управлінської спроможності держави, забезпечуючи підвищення надійності критичних послуг у воєнний і післявоєнний періоди.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Rinaldi S. M., Peerenboom J. P., Kelly T. K. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine. 2001. Vol. 21, No. 6. P. 11–25.

2. 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. Official Journal of the European Union. 2008. L 345. P. 75–82. URL: https://eur-lex.europa.eu

3. 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. Official Journal of the European Union. 2022. L 333. URL: https://eur-lex.europa.eu

4. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union. 2022. L 333. URL: https://eur-lex.europa.eu

5. European Commission. European Programme for Critical Infrastructure Protection (EPCIP). Communication from the Commission COM(2006) 786 final. Brussels, 2006. URL: https://eur-lex.europa.eu

6. European Commission. Evaluation study of Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Final report. Brussels, 2019. URL: https://ec.europa.eu

7. Закон України «Про критичну інфраструктуру» від 16 листопада 2021 р. № 1882-IX. Відомості Верховної Ради України. 2022. № 8. Ст. 49. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

8. Закон України «Про національну безпеку України» від 21 червня 2018 р. № 2469-VIII. Відомості Верховної Ради України. 2018. № 31. Ст. 241. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

9. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

10. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 р. № 96/2016. Офіційний вісник Президента України. 2016. № 8. Ст. 169. URL: https://www.president.gov.ua/documents/962016-19836

11. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 р. № 287/2015. Офіційний вісник Президента України. 2015. № 16. Ст. 905. URL: https://www.president.gov.ua/documents/2872015-19070

12. Бірюков Д. С., Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. Київ: НІСД, 2012. 96 с. URL: https://niss.gov.ua

13. Зелена книга з питань захисту критичної інфраструктури в Україні: зб. матеріалів міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С. І. Кондратов; за заг. ред. О. М. Суходолі. Київ: НІСД, 2016. 176 с. URL: https://niss.gov.ua

14. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки України: аналітична доповідь / О. М. Суходоля та ін. Київ: НІСД, 2020. 64 с. URL: https://niss.gov.ua

15. Бобро Д. Г. Методологія оцінки рівня критичності об’єктів інфраструктури. Стратегічні пріоритети. 2016. № 3. С. 78–86.

16. Газдайка-Васильшин І. Б. Основні терміни проєкту Закону України «Про критичну інфраструктуру та її захист». Право і суспільство. 2019. Вип. 9. С. 15–20.

17. Франчук В. І., Пригунов П. Я., Мельник С. І. Безпека об’єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи. Соціально-правові студії. 2021. Вип. 3. С. 142–148.

18. Солопова І. В. Правові умови захисту об’єктів критичної інфраструктури в Україні: проблеми та перспективи. Південноукраїнський правничий часопис. 2021. № 2. С. 119–125.

19. Яременко О. І., Страхніцький Я. О. Теоретичні підходи до визначення дефініції критичної інфраструктури як об’єкта державного управління. Публічне управління та митне адміністрування. 2022. № 1. С. 76–82.

20. Єрменчук О. П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монографія. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.

21. Теленик С. С. Державна система захисту критичної інфраструктури України: концептуальні засади адміністративно-правового регулювання. Херсон: Видавничий дім «Гельветика», 2020. 602 с.

22. Dunn-Cavelty M., Suter M. Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. International Journal of Critical Infrastructure Protection. 2009. Vol. 2, Iss. 4. P. 179–187.

23. Rehak D., Hromada M., Lovecek T. Personnel threats in the electric power critical infrastructure sector and their effect on dependent sectors: Overview in the Czech Republic. Safety Science. 2020. Vol. 127. Art. 104698.

24. Osei-Kyei R., Tam V. W. Y., Ma M., Mashiri F. Critical review of the threats affecting the building of critical infrastructure resilience. International Journal of Disaster Risk Reduction. 2021. Vol. 60. Art. 102316.

25. Alderson D. L., Darken R. P., Eisenberg D. A., Seager T. P. Surprise is inevitable: How do we train and prepare to make our critical infrastructure more resilient? International Journal of Disaster Risk Reduction. 2022. Vol. 72. Art. 102800.

26. Melnyk D. S. Creating a model of threats to Ukraine’s national critical infrastructure as a basis for ensuring its security and resilience. Bulletin of Kharkiv National University of Internal Affairs. 2024. Vol. 104, No. 1 (Part 1). P. 237–250.

27. Davydiuk O., Potii Yu. National Cybersecurity Governance: Ukraine. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2024.

28. State Service of Special Communications and Information Protection of Ukraine. War and Cyber: Three Years of Struggle and Lessons for Global Security. Kyiv: SSSCIP & ICE Task Force, 2025.

29. Cybersecurity Threat Landscape of Ukraine in 2023. Analytical Report of the Understanding Cyber War Project. 2024.

30. The CERT-UA Team has processed 2,543 cyber incidents over the last year. Analytical Note of CERT-UA and the State Service of Special Communications and Information Protection of Ukraine. Kyiv, 2024.

31. Linkov I., Eisenberg D. A., Plourde K., Seager T. P., Allen J., Kott A. Resilience metrics for cyber systems. Environment Systems and Decisions. 2013. Vol. 33, No. 4. P. 471–476.

32. International Organization for Standardization. ISO 22301:2019. Security and resilience – Business continuity management systems – Requirements. Geneva: ISO, 2019.

33. International Organization for Standardization. ISO 31000:2018. Risk management – Guidelines. Geneva: ISO, 2018.

34. European Union Agency for Cybersecurity (ENISA). Good Practices for Security of Critical Infrastructure and Services. Athens: ENISA, 2016.

35. NATO. Resilience and Article 3. NATO Factsheet. Brussels: NATO Public Diplomacy Division, 2020.

36. Sukhodolia O. M. The resilience of critical infrastructure and public administration challenges. Analytical Paper. Kyiv: National Institute for Strategic Studies, 2023.

37. UNDP. Guidance notes on building critical infrastructure resilience in Europe and Central Asia. Bratislava, 2022. 74 p. URL: https://www.undp.org/

38. Yang Z. et al. Critical infrastructure resilience: a guide for building resilience in the context of multi-hazards. Natural Hazards and Earth System Sciences. 2024. Vol. 24. P. 3723–3743.

39. Jovanovic A. S., Schmid N., Klimek P., Egloff R. Use of Indicators for Assessing Resilience of Smart Critical Infrastructures. IRGC, 2014. 52 p. URL: https://irgc.org/

40. AIIC – Italian Association of Critical Infrastructures. Guidelines for Critical Infrastructures Resilience Evaluation. Rome, 2021. 56 p. URL: https://www.infrastrutturecritiche.it/

41. CSS – Center for Security Studies. Risk and Resilience Report 2024: Critical Infrastructure Resilience. Zurich: ETH Zurich, 2024. 84 p.

42. International Foundation for Electoral Systems (IFES). Ukrainian Cybersecurity Legal Framework: Overview. Kyiv, 2020. 64 p.

43. USAID. APS-CCI-004. Cybersecurity for Critical Infrastructure in Ukraine – Activity. Program Description. Kyiv, 2024. 32 p.

44. Деякі питання проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури : постанова Кабінету Міністрів України від 24.03.2023 р. № 257. URL: https://www.kmu.gov.ua/

45. Незалежний аудит інформаційної безпеки на об’єктах критичної інфраструктури : офіційні роз’яснення Адміністрації Держспецзв’язку, 22.10.2024 р. URL: https://cip.gov.ua/

46. Про затвердження Вимог до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури : наказ Адміністрації Держспецзв’язку від 30.04.2024 р. № 254. URL: https://zakon.rada.gov.ua/

47. Захист критичної інфраструктури енергосектору: Рахункова палата провела аудит реалізації експериментального проекту. Звіт Рахункової палати України, 15.10.2025 р. URL: https://rp.gov.ua/

48. Резильєнтність критичної інфраструктури – 2023 : зб. матеріалів наук.-практ. конф. (Київ, 21 черв. 2023 р.) / ІПМЕ ім. Г. Є. Пухова НАН України. Київ, 2023. 109 с.

49. Юдін О. К. Кібербезпека критичної інфраструктури України: кадрова політика, роль та місце Держспецзв’язку. В кн.: Резильєнтність критичної

інфраструктури – 2023 : зб. матеріалів наук.-практ. конф. Київ, 2023. С. 1084–1090.

50. Інтегрований підхід до підготовки фахівців із захисту критичної інфраструктури в Україні. Journal of Security and Public Safety. 2025. № 2. С. 45–56.

51. Живило Є., Живило І. Об’єднана підготовка персоналу складових сил оборони сфери кібербезпеки в умовах тотальної оборони держави. Теорія та практика державного управління. 2021. № 2 (73). С. 144–153.

52. Гапон Ю. К., Слепужніков Є. Д. Об’єднання теорії та практики – запорука підвищення рівня безпеки хімічних об’єктів та критичної інфраструктури. Матеріали науково-практичної конференції. Харків, 2024. С. 201–208.

53. Захист критичної інфраструктури : методичні підходи та практичні аспекти. Аналітичний матеріал. КНУ ім. Т. Шевченка, 2024. 32 с.

54. World Bank Group. Private Sector Opportunities for a Green and Resilient Reconstruction in Ukraine. Washington, 2023. 120 p.

55. World Bank Group. WBG Support to Ukraine – Update July 2025. Washington, 2025. 40 p.

56. Ukraine Rapid Damage and Needs Assessment IV. Kyiv–Washington : Government of Ukraine; World Bank; European Commission, 2025. 180 p.

57. Safety Strategy for Critical Infrastructure and Critical Industries. Association of Industrial Automation of Ukraine (APPAU). Kyiv, 2022. 24 p. URL: https://appau.org.ua/

58. Шкуропадська Д. Підходи НАТО до забезпечення резильєнтності критичної інфраструктури. Scientia Fructuosa. 2025. № 3. С. 89–104.

59. Помаза-Пономаренко А. Л. Збитки, нанесені бойовими діями об’єктам критичної інфраструктури в Україні: механізми оцінювання та відновлення. Успіхи і досягнення у науці. 2025. № 1 (11). С. 601–611.

60. Чеховська М. М., Лісовська О. Л. Загрози критичній інфраструктурі України в сучасних умовах. Ефективна економіка. 2025. № 2.

61. Бобро Д. Г. Урахування проектних загроз у розбудові державної системи захисту критичної інфраструктури. Стратегічні пріоритети. 2017. № 3. С. 42–51.

62. Зелена книга з питань захисту критичної інфраструктури в Україні: зб. матеріалів міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С. І. Кондратов; за заг. ред. О. М. Суходолі. Київ: НІСД, 2016. 176 с.

63. Зубко Г. Ю. Життєво важлива інфраструктура: підходи до розуміння нового концепту. Visegrad Journal on Human Rights. 2019. № 4. С. 83–89.

64. Кондратов С. І. Про забезпечення координації дії, взаємодії та обміну інформацією при створенні державної системи захисту критичної інфраструктури. Київ: НІСД, 2018. 30 с.

65. Мельничук О. В. Управління критичною інфраструктурою держави: базові методи та критерії ідентифікації об'єктів. Державне управління та місцеве самоврядування. 2019. Вип. 3 (42). С. 13–27. DOI: https://doi.org/10.35432/1993-8330appa1812020201816

66. Суходоля О. М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. Стратегічні пріоритети. 2016. № 3 (40). С. 62–76.

67. Про Стратегію національної безпеки України: Указ Президента України від 12.02.2007 року № 105/2007 (втратив чинність). URL: https://zakon.rada.gov.ua/laws/show/105/2007#n10

68. Про Стратегію національної безпеки України: Рішення Ради національної безпеки і оборони України від 06.05.2015 року. URL: https://zakon.rada.gov.ua/laws/show/n0008525-15#Text

69. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету Міністрів України від 06.12.2017 року № 1009-р. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#n8

70. Про критичну інфраструктуру та її захист: Проєкт Закону України від 27.05.2019 року № 10328. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65996

71. Деякі питання об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 року № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF/ed20201009#Text

72. Про критичну інфраструктуру: Закон України від 16.11.2021 року № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

73. Council Directive 2008/114/EC "On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection". URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32008L0114

74. Про правовий режим воєнного стану: Закон України від 12.05.2015 року № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text

75. Желіховська Ю. В. Співвідношення та розмежування понять "охорона" та "захист". Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція. 2015. № 13. Т. 2. С. 18–21.

76. Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України: Закон України від 18.10.2022 року № 2684-IX. URL: https://zakon.rada.gov.ua/laws/show/2684-20#Text

77. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 року № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text

78. Страхніцький Я. О. Особливості сучасної державної політики у сфері захисту критичної інфраструктури в умовах війни в Україні. У: Модернізація системи державного управління та адміністрування в Україні: досвід Латвійської Республіки: наукова монографія. Рига: "Baltija Publishing", 2023. С. 115–142. DOI: https://doi.org/10.30525/978-9934-26-279-1-5

79. Франчук В. І., Пригунов П. Я., Мельник С. І. Безпека об’єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи. Соціально-правові студії. 2021. Вип. 3 (13). С. 142–148. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3984/1/19.pdf

80. Про оборону України: Закон України від 06.12.1991 року № 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text

81. Конституція України: Закон України від 28.06.1996 року № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

82. Богдан Б. В. Адміністративно-правова охорона населення від інфекційних хвороб: дис. … канд. юрид. наук. Київ, 2021. 215 с.

83. Темченко В. Особливості юридичного змісту термінів “захист” та “охорона” у механізмі забезпечення прав людини. Вісник Академії управління МВС. 2007. № 2–3. С. 58–65.

84. Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України: Постанова Кабінету Міністрів України від 12.07.2022 року № 787 (не набрала чинності). URL: https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#Text

85. Про затвердження Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 22.07.2022 року № 821. URL: https://zakon.rada.gov.ua/laws/show/821-2022-%D0%BF#Text

86. Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури: Розпорядження Кабінету Міністрів України від 19.09.2023 року № 825-р. URL: https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text

87. Про затвердження Методик та Критеріїв і показників оцінки стану захисту об’єктів критичної інфраструктури: Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 14.01.2025 року № 17. URL: https://zakon.rada.gov.ua/laws/show/z0375-25#Text

88. Соколова Ю. В Україні на електростанціях можуть з’явитися датчики для виявлення ракет і дронів. Факти ICTV. 15.12.2022. URL: https://fakty.com.ua/ua/ukraine/20221215-v-ukrayini-na-elektrostancziyah-mozhut-zyavytysya-datchyky-dlya-vyyavlennya-raket-i-droniv-npu/

89. Департамент захисту критичної інфраструктури Держспецзв’язку підготував щорічну оцінку ризиків та загроз. Офіційний веб-сайт Державної служби спеціального зв’язку та захисту інформації України. 24.11.2023. URL: https://cip.gov.ua/ua/news/departament-zakhistukritichnoyi-infrastrukturi-derzhspeczv-yazku-pidgotuvav-shorichnu-ocinku-rizikiv-ta-zagroz

ДОДАТКИ

ДОДАТОК А



Увечері 11 вересня 2022 року ВКС РФ завдали групового ракетного удару шістьма крилатими ракетами "Калібр" з акваторії Чорного моря та ще шістьма крилатими ракетами Х101 з рубежів пуску у повітрі над Каспійським морем по об’єктах енергетичної інфраструктури України.



Не зважаючи на те, що професійно спрацювала українська ППО, котра перехопила 9 з 12 випущених ракет, три уразили Харківську ТЕЦ-5, Зміївську ТЕЦ та Павлоградську ТЕЦ-3. Ушкоджень зазнала також Кременчуцька ТЕЦ. Без води та світла залишилися Харківська, Полтавська, Дніпропетровська і частково Запорізька області



Ушкоджена гідротехнічна споруда у Кривому Розі (фото: офіційна сторінка Президента України)