МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

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

Кваліфікаційна робота
на правах рукопису

ХАРЧЕНКО АЛЛА МИКОЛАЇВНА
(прізвище, ім'я, по батькові здобувача вищої освіти)

УДК 368.914(477)
(індекс)

КВАЛІФІКАЦІЙНА РОБОТА

ПЛАНУВАННЯ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: УПРАВЛІНСЬКІ ПІДХОДИ ТА ВИКЛИКИ

(тема роботи)

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

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

А. М. ХАРЧЕНКО
(підпис, ініціали та прізвище здобувачвищої освіти)

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

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

Житомир – 2025

Висновок кафедри економічної теорії, інтелектуальної власності та публічного управління
за результатами попереднього захисту: **ХАРЧЕНКО Алла Миколаївна** допущена до захисту

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

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

«___» _____ р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти ___**ХАРЧЕНКО Алла Миколаївна**__ захистила
(прізвище ,ім'я, по батькові)

кваліфікаційну роботу з оцінкою:
сума балів за 100-бальною шкалою _____
за національною шкалою _____

Секретар ЕК
_____-_____ _____ Анастасія ПРУТ
(науковий ступінь, вчене звання) (підпис) (власне ім'я, прізвище)

АНОТАЦІЯ

ХАРЧЕНКО А. М. Планування та забезпечення безпеки критичної інфраструктури: управлінські підходи та виклики. – Кваліфікаційна робота на правах рукопису. Кваліфікаційна робота на здобуття освітнього ступеня магістра за спеціальністю 281 – Публічне управління та адміністрування. – Поліський національний університет, Житомир, 2025.

Кваліфікаційна робота присвячена вивченню планування та забезпечення безпеки критичної інфраструктура, управлінських підходів і викликам. Актуальність теми зумовлена необхідністю підвищення ефективності планування роботи критичної інфраструктури в мінливих умовах, попереджувати виникнення небезпечних природних явищ, природних лих, технічних збоїв, зловмисних дій і швидкого відновлення після них. У роботі проведено аналіз чинної нормативно-правової бази, зарубіжного досвіду, організаційних підходів та сучасних проблем функціонування критичної інфраструктури.

Виявлено, що формування нормативно-правового регулювання питань захисту критичної інфраструктури зумовлено низкою чинників, яким піддаються об’єкти критичної інфраструктури, а саме: природні, техногенні загрози, воєнні дії на території країни, збройна агресія, кібератаки, терористичні загрози.

Ключові слова: нормативно–правова база, управління безпекою, критична інфраструктура, воєнний стан, об’єкти критичної інфраструктури, суб’єкти захисту, загрози та ризики для критичної інфраструктури, системи захисту критичної інфраструктури.

SUMMARY

KHARCHENKO A. Planning and Ensuring the Security of Critical Infrastructure: Management Approaches and Challenges. – Qualification work on the rights of the manuscript. Qualification work for obtaining a master's degree in specialty 281 «Public management and administration» – Polissia National University, Zhytomyr, 2025.

The qualification thesis is dedicated to the study of planning and ensuring the security of critical infrastructure, with a focus on managerial approaches and challenges. The relevance of the research is driven by the necessity to enhance the efficiency of planning and managing critical infrastructure in a constantly evolving environment, ensuring resilience and rapid recovery following accidents, technical failures, malicious activities, natural disasters, and other hazardous phenomena. The study includes an analysis of the existing legal and regulatory framework, international best practices, organizational approaches, and contemporary challenges in critical infrastructure management.

The research establishes that the formation of a regulatory framework for critical infrastructure protection is influenced by a range of factors, including natural and technological threats, terrorist risks, armed aggression and military conflicts within the country, as well as cyberattacks targeting critical infrastructure assets.

Keywords: regulatory framework, critical infrastructure facilities, critical infrastructure, security management, martiallaw, protection subjects, threats and risks to critical infrastructure, critical infrastructure protection systems,.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. В умовах сьогодення світ стикається зі складними викликами та надзвичайними подіями різного походження. Засоби масової інформації щодня повідомляють про різні катаклізми природного та техногенного походження, конфлікти, терористичні акти, в результаті яких завдається значна шкода. Швидкий розвиток суспільства з застосуванням новітніх технологій спричиняє залежність людей від послуг, що надаються енергетичними, телекомунікаційними, транспортними та іншими інфраструктурами. Доступність суспільства до цих послуг на сьогоднішній день не залежить від географічного розташування місця проживання (перебування) та сприймається як один з показників якості життя. Поняття «критична інфраструктура» в Україні, в порівнянні з іншими європейськими країнами, з'явилося досить недавно, тому першочерговим завданням сьогоднішнього уряду є забезпечення національної безпеки критичної інфраструктури. Особлива увага приділяється енергетичній, транспортній, інформаційній, комунікаційній сферам.

Питання захисту об'єктів критичної інфраструктури гостро постає на рівні держави в умовах пов'язаних з проведення воєнних дій, адже вони стають дуже вразливими до загроз і не здатні самостійно чинити опір. Збитки і наслідки, які наносяться об'єктам критичної інфраструктури викликають значні порушення в роботі критично важливих структур. Це передбачає застосування складних механізмів державного управління, які спрямовані на захист об'єктів критичної інфраструктури. .

Питання планування та забезпечення безпеки критичної інфраструктури досліджувалося численними науковцями, які розглядали різні аспекти цієї проблематики, зокрема Д. С. Бірюков, О. М. Суходоля, С. П. Іванюта, О. П. Єрменчук, В. І. Франчук, П. Я. Пригунов, С. І. Мельник, Г. Ю. Зубко. У науковій літературі акцент робиться на стратегічному плануванні, впровадженні взаємодії і координації між суб'єктами національної системи

захисту критичної інфраструктури, вдосконалення законодавства з питань захисту об'єктів критичної інфраструктури, забезпечувати стійкість критичної інфраструктури, обмін досвідом з дружніми країнами – партнерами.

Метою дослідження є аналіз управлінських підходів до планування безпеки критичної інфраструктури, основних викликів, ризиків, загроз з якими стикається сфера критичної інфраструктури.

Завдання дослідження: проаналізувати підходи до визначення критичної інфраструктури у міжнародному та національному законодавстві, провести класифікацію об'єктів критичної інфраструктури, зробити аналіз нормативно-правової бази, існуючих механізмів, моделей у сфері захисту критичної інфраструктури, проаналізувати сучасні ризики та загрози для критичної інфраструктури, провести оцінку потенційних наслідків пошкодження об'єктів критичної інфраструктури, рекомендувати наступні напрями та шляхи вдосконалення у плануванні і забезпеченні безпеки критичної інфраструктури.

Об'єктом дослідження є управлінські підходи до планування та забезпечення безпеки критичної інфраструктури.

Предметом дослідження є механізми державного контролю та нагляду, які впливають на ефективність функціонування критичної інфраструктури.

Методологія дослідження. Теоретичною та методологічною основою дослідження стали системний підхід, аналіз нормативно–правової бази, порівняльний аналіз міжнародного досвіду, а також міждисциплінарний підхід, який об'єднує економіку, право та інформаційні технології.

Перелік публікацій. Проблеми та досягнення в системі інфраструктурного забезпечення Житомирської територіальної громаді (місто Житомир, 27-28 червня 2024 р.); Управління інфраструктурним забезпеченням територіальних громад: безпековий аспект (м. Одеса, 29-30 листопада 2024 р.); Публічне управління критичною інфраструктурою: інституційно-правові аспекти (м. Житомир, 12 грудня 2024 р.).

Практичне значення результатів. Результати дослідження можуть бути використані для розробки нових законодавчих документів, що займаються

питанням захисту об’єктів критичної інфраструктури, а також для вдосконалення і пошуку ефективних рішень у відновленні об’єктів критичної інфраструктури та чіткого розподілу відповідальності за захист кожного об’єкта критичної інфраструктури.

Елемент наукової новизни кваліфікаційної роботи полягає у визначенні можливостей застосування іноземного досвіду та сучасних інформаційних технологій у сфері захисту вітчизняної критичної інфраструктури.

Інформаційною базою дослідження є праці вітчизняних і закордонних вчених в галузі захисту об’єктів критичної інфраструктури, нормативно-правові документи, інформація органів виконавчої влади, ресурси Internet-мережі.

Структура роботи. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ ЗАСАДИ ПЛАНУВАННЯ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Концептуальні підходи до визначення критичної інфраструктури та її елементів

Перші згадки у міжнародному обговоренні та нормативно-правових документах термін «критична інфраструктура» були описані у директиві PDD–63 (Presidential Decision Directive) у 1996 році, яку підписав Білл Клінтон 42-й президент Сполучених Штатів Америки. В законодавстві США поняття «критична інфраструктура» пояснюється як класифікація важливих для країни фізичних засобів і віртуальних активів, часткове порушення і знищення яких призведе до порушення національної безпеки, безпеки здоров'я населення і економіки країни [1]. У 1996 році США до критичної інфраструктури відносили телекомунікації, електроенергетичні системи, нафту, газ та їх зберігання, фінанси, транспорт, системи водопостачання, аварійні служби, безперервність керування. У 2003 році до сформованого переліку було додано продукти харчування, охорону здоров'я, хімічну промисловість,небезпечні матеріали, що збільшило кількість критичних секторів до 14, а у 2013 році – до 16.

Розглянемо як трактують та розуміють термін «критична інфраструктура» в інших країнах світу. У прийнятій Німеччиною «Стратегії національної безпеки: Інтегрована безпека для Німеччини» визначення «критична інфраструктура» трактується як засоби фізичні і організаційні, що життєво важливі для економіки і суспільства, порушення/збій яких призведе до збою (дефіциту) поставок ресурсів, що призведе до гострих наслідків [2].

У законодавстві Польщі в документі під назвою «Про антикризове управління» розуміють критичну інфраструктуру як «системи та їх функціонально пов'язані об'єкти, включаючи будівельні об'єкти, заклади, прилади, визначальні служби, що забезпечують безпеку держави, громадян,

державного управління і підприємств приватної форми власності» [3]. У даному визначенні увага приділяється стабільності роботі державних органів.

У Великій Британії термін «критична інфраструктура» трактується як «критичні елементи інфраструктури» до яких відносять мережі, системи, процеси, активи та людський ресурс, що керує цими процесами, втрата або шкідливий вплив на них приведе до порушення основних їх функцій і відбудеться невідворотний вплив на національну безпеку і оборону країни [4].

В незалежній Україні уперше термін «критична інфраструктура» з'явився у 2006 р. у тексті «Рекомендацій парламентських слухань з питання розвитку інформаційного суспільства». У Стратегії національної безпеки «Україна у світі, що змінюється» (2012 р.) [5] термін «критична інфраструктура» вживався при визначенні методів забезпечення безпеки енергетичної та інформаційної сфер. Детально критичну інфраструктуру викладено у «Рішенні Ради національної безпеки і оборони України «Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України» від 01.03.2014».

Поняття «критична інфраструктура» також зазначено в Указі Президента № 287/2015 «Про Стратегію національної безпеки України» [6], у якому визначено ризики та загрози для безпеки критичної інфраструктури. У 2014–2015 роках прийнято збірник матеріалів міжнародних експертних нарад, до яких залучалися українські і світові експерти за сприяння Національного інституту стратегічних досліджень, під назвою «Зелена книги з питань захисту критичної інфраструктури в України». Документ трактує визначення «критична інфраструктура України» як сукупність ресурсів і систем для функціонування та надання послуг, негативний вплив на які приведе до порушення національної стійкості і безпеки [7].

Досліджували питання визначення терміну «критична інфраструктура» науковці Д.С. Бірюков, О.М. Суходоля, С.І. Кондратов та інші. З посиланням на вітчизняне законодавство, науковці трактують критичну інфраструктуру як

важливі державні об’єкти підвищеної безпеки та стратегічного значення, які потребують особливої охорони в умовах надзвичайної ситуації.

У 2021 році Верховна Рада України приймає Закон України «Про критичну інфраструктуру» (1882-IX від 16.11.2021), який визначає поняття «критична інфраструктура» як сукупність об’єктів критичної інфраструктури, які мають найвищу ступінь важливості для функціонування та безперебійної роботи національної економіки та суспільства [8]. З прийняттям Закону 1882-IX в Україні почала створюватися система критичної інфраструктури, яка включає об’єкти оборони та об’єкти, що надають важливі послуги та комунікацію, а саме: системи водопостачання, транспортні центри, телекомунікаційні мережі, медичні установи, виробництво і зберігання харчових продуктів,електростанції, та інші об’єкти. Безпека зазначених об’єктів, їх функціонування, забезпечення безперебійної роботи, захист базових потреб суспільства та забезпечення їхнього сталого функціонування одне з головних завдань країни.

Згідно статті 1 ЗУ «Про критичну інфраструктуру» «об’єкти критичної інфраструктури – підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров’я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних матеріальних та фінансових збитків, людських жертв» [8].

Згідно із Законом України «Про критичну інфраструктуру» до життєво важливих функцій та/або послуг належать:

- урядування та надання найважливіших публічних (адміністративних) послуг;
- енергозабезпечення (у тому числі постачання теплової енергії);
- водопостачання та водовідведення;
- продовольче забезпечення;

- охорона здоров’я;
- фармацевтична промисловість;
- виготовлення вакцин, стале функціонування біолабораторій;
- інформаційні послуги;
- електронні комунікації;
- фінансові послуги;
- транспортне забезпечення;
- оборона, державна безпека;
- правопорядок, здійснення правосуддя, тримання під вартою;
- цивільний захист населення та територій, служби порятунку;
- космічна діяльність, космічні технології та послуги;
- хімічна промисловість;
- дослідницька діяльність [8].

Для забезпечення безпеки і стійкості критичну інфраструктуру виділяють за секторами. «Секторальний перелік об’єктів критичної інфраструктури» складає і веде секторальний орган [8]. У постанові Кабінету міністрів України від 09.10.2020 № 1109 перелічено сектори/підсектори основних послуг критичної інфраструктури держави. Даний перелік містить список секторальних органів, згідно якого до секторальних органів належать: Міненерго, Мінцифри, Мінрегіон, Мінекономіки, Мінінфраструктури, Мінстратегпром, Мінфін, МВС, МОЗ, НСЗУ, НКЦПФР.

Об’єкти критичної інфраструктури поділяються за критеріями визначених у пункті 3 статті 8 ЗУ «Про критичну інфраструктуру». Існують категорії критичності, які визначають рівень важливості об’єктів.

Згідно пункту 2 статті 10 Закону № 1882–IX від 16.11.2021 розділяють 4 «категорії критичності об’єктів критичної інфраструктури:

1) І категорія критичності – особливо важливі об’єкти, які мають загальнодержавне значення, значний вплив на інші об’єкти критичної інфраструктури та порушення функціонування яких призведе до виникнення кризової ситуації державного значення;

2) II категорія критичності – життєво важливі об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення;

3) III категорія критичності – важливі об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації місцевого значення;

4) IV категорія критичності – необхідні об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації локального значення» [8 ,ст. 10].

Секторальні органи, згідно вимог секторальної специфіки і законодавства України, проводять категоризацію об’єктів критичної інфраструктури.

1.2. Теоретичні основи управління безпекою критичної інфраструктури

Протягом усього часу існування людство стикається з безліччю загроз та ризиків. З роками їх кількість збільшувалася, зростав рівень небезпеки і з часом це переросло в проблему. Основними для всього світу є ризики та небезпеки техногенного та природного характеру, пандемії, збройні конфлікти, кіберзагрози та ін. В сучасному світі критична інфраструктура має вчасно реагувати на негативні виклики для виконання нею основних функцій та надання критично важливих послуг. Багато загроз становлять значний ризик і для України. Зокрема, це стосується об’єктів та послуг критичної інфраструктури без яких неможливе функціонування держави та безпека населення.

Аналізуючи визначення «ризик», можна зазначити, що ризик – це ситуація, що виникає при несприятливих умовах та характеризується невизначеним результатом та важкістю наслідкам.

У дослідженнях і наукових роботах А. Карпіньяно, Д. Гроссо, Р.Джербоні, А Болонья, К. Пурсіайнен, Б. Рьод., М. Теохаріду, Г.Джаннопулос приділяли увагу класифікації, систематизації і аналізу ризиків та їх подоланні.

Керуванням ризиком називають процес спрямований на ухвалення рішень та вжиття заходів для зміни ризику. Механізм управління ризикам – це набір інструментів, методів, форм і засобів взаємодії між учасниками управління ризиків з метою розробки та впровадження управлінських рішень для запобігання появі ризиків, зменшення їх наслідків та подолання їх впливу [9].

Управління ризиками об’єктів критичної інфраструктури передбачає створення ряду інструментів. Можна умовно розділити їх наступним чином:

– правові – сприяння створенню законодавчої бази, правового врегулювання, ідентифікації загроз та розв’язання питання управління забезпеченням безпеки об’єктів критичної інфраструктури;

– організаційні – створення спеціалізованого органу, який відповідає за забезпечення безпеки критичних об’єктів, координацію його діяльності та співпрацю з іншими організаціями, підприємствами, а також юридичними та фізичними особами;

– техніко–технологічні та програмні – формування системи технологічних, технічних, програмних чинників, яку забезпечує захист критичних об’єктів інфраструктури від серйозних загроз ризиків, а також зменшує негативні наслідки їх застосування;

– фінансові – визначення фінансування та резерву для запобігання ризиковим ситуаціям у критичній інфраструктурі незалежно від їх походження

– наукові – наукові обґрунтування базових методів, форм, принципів, інструментів та заходів для запобігання та захисту критичних інфраструктурних об’єктів;

– військово–оборонні – використання спеціальних засобів для запобігання та виявлення ворожих злочинних дій проти критичної інфраструктури;

– інформаційні – створення та поширення інформаційних повідомлень про форми, прояви, наслідки збільшення ризиків для критично важливих об’єктів заходи для їх запобігання, виявлення ворожих інформаційних викликів та загроз;

– освітні – навчання фахівців (вузьких спеціалістів),їх підготовка з управління ризиками на об’єктах критичної інфраструктури;

– дипломатичні – встановлення меж втручання в соціальні та суспільно значимі системи та активи вирішення конфліктів, що загострюють загрози критичній інфраструктурі.

Для врегулювання проблем, пов’язаних з об’єктами критичної інфраструктури, в Україні прийнято ряд законодавчих актів, серед яких, закон України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX, указ президента України «Про стратегію забезпечення державної безпеки» від 16.02.2022 № 56/2022.

Закон України «Про критичну інфраструктуру» (далі – Закон) визначає основні завдання та функції забезпечення безпеки критичної інфраструктури. Під поняттям «безпека критичної інфраструктури» розуміється рівень захищеності критичних систем, який гарантує їх функціонування, неперервність в роботі, можливість відновлення, цілісність , стійкість.

Стаття 22 Закону передбачає, що для створення ефективного функціонування системи захисту критичної інфраструктури країни Кабінет Міністрів України, центральні органи виконавчої влади, органи місцевого самоврядування розробляють та затверджують плани та програми реагування на кризові ситуації. Кабінет Міністрів України встановлює правила управління ризиками безпеки на об’єктах критичної інфраструктури першої категорії та встановлює вимоги щодо управління ризиками безпеки. Національний банк України несе відповідальність за банки та інших учасників, які діють на ринках фінансових послуг [8].

Таблиця 1.1

Понятійний апарат системи захисту критичної інфраструктури

Поняття	Зміст визначення поняття
Безпека об'єкта критичної інфраструктури	стан об'єкта критичної інфраструктури, у межах якого забезпечується його функціонування, цілісність, самодостатність і стійкість та діяльність спрямована на попередження, виявлення, ліквідацію загроз чи небезпеки критичній інфраструктурі, у разі їх реалізації – відновлення чи відшкодування за завданні збитки
Цілісність об'єкта критичної інфраструктури	внутрішня єдність усіх елементів об'єкта, яка забезпечує пов'язаність їх між собою так, що жоден із них не може бути усунений, модифікований або доданий з порушенням політики безпеки системи, а стосовно навколишнього оточення дозволяє виступати як одне ціле
Самодостатність об'єкта критичної інфраструктури	наявність у розпорядженні суб'єктів управління відповідних ресурсів та уникнення залежності від джерел їх походження, що може становити загрозу, а також їх використання на рівні, необхідному для збереження параметрів життєдіяльності системи
Стійкість об'єкта критичної інфраструктури	наявність необхідних умов, елементів та системних зв'язків між ними на рівні, достатньому для стримування дії загроз та відновлення після їх дії
Загроза об'єкту критичної інфраструктури	дія дестабілізуючих природних і суб'єктивних факторів, що спричиняє збитки соціальнійсистемі чи конкретній фізичній особі
Небезпека об'єкту критичної інфраструктури	деструктивні граничні зміни, спричинені реалізацією загрози в соціальній системі, що призводить до кризового стану
Механізми попередження загрози	сукупність відповідних видів діяльності, методів та засобів, пов'язаних з розробкою нормативних, організаційних документів та управлінських рішень з питань безпеки підприємства та їх застосування для попередження виникнення або дії загрози
Механізми виявлення загрози	сукупність відповідних видів діяльності, методів та засобів, пов'язаних зі збором і аналізом інформації про загрози та документування протиправних дій у відповідному часі та просторі
Механізми ліквідації загрози	сукупність видів безпекової діяльності та відповідних конфіденційних методів, методів роботи у надзвичайних ситуаціях, а також засобів, пов'язаних з ліквідацією (припиненням) загроз на будь-якій стадії її реалізації
Механізм відновлення діяльності, відшкодування за завданні збитки	сукупність видів безпекової діяльності та відповідних методів й засобів, необхідних для відновлення процесів, кількісних чи якісних показників діяльності, зв'язків та цілісності підприємства після реалізації загрози, а також відшкодування за завданні збитки

Джерело: побудовано на основі [8, 26].

На виконання вимог абзацу другого частини першої статті 22 Закону Адміністрацією Держспецзв'язку, як органом виконавчої влади, який відповідає і здійснює повноваження уповноваженого органу у галузі захисту критичної інфраструктури, розроблено проєкт постанови Кабінету Міністрів

України «Про затвердження Вимог щодо управління ризиками безпеки на об’єктах критичної інфраструктури першої категорії критичності». Даний проєкт визначає ряд дій для ефективного зниження та контролю ризиків безпеки, уникнення можливих загроз, а також зменшення наслідків кризових ситуацій та інших подібних небезпек.

Метою створення системи управління ризиками безпеки є інтеграція управління ризиками у важливі види діяльності та функції критичної інфраструктури, включаючи прийняття рішень оператором критичної інфраструктури [10].

Стратегія забезпечення державної безпеки(далі – Стратегія) аналізує небезпеки та виклики, які ставлять під загрозу національну безпеку України, визначає стратегічні напрями та завдання державної політики у сфері безпеки як основу для розробки та впровадження відповідних заходів.

В Стратегії зазначено, що в нашій державі відбувається збільшення загроз для критичної інфраструктури через тимчасову окупацію частини території України, вплив гібридних дій від суб’єктів розвідувально-підривної діяльності, погіршення технічного стану інфраструктури та спроби несанкціонованого втручання у її роботу, включаючи фізичні та кіберзагрози. Одним з основних завдань у сфері безпеки, які постають перед державою, є здійснення заходів з перевірки і запобігання протиправним діям іноземних агентів та організацій, спрямованих на завдання шкоди державній безпеці шляхом контролю за стратегічно важливими об’єктами та інфраструктурою [11].

ВИСНОВКИ ДО РОЗДІЛУ 1

В законодавстві України визначення «критична інфраструктура» вживається як комплекс об’єктів критичної інфраструктури. Прийняття Закону № 1882–IX поклало початок створення системи критичної інфраструктури в Україні, якої до того часу не було. Об’єкти критичної інфраструктури є об’єкти,

системи, їх складові, які є необхідними для національної безпеки, оборони та економіки країни. Порушення їх функціонування може призвести до завдання шкоди життєво важливим національним інтересам.

Основне призначення об’єктів критичної інфраструктури полягає в задоволенні основних потреб громадян та виконання ключових функцій держави при будь-яких ситуаціях: мирний час, надзвичайна ситуація, військовий конфлікт та умовах війни. Категоризація об’єктів критичної інфраструктури здійснюється секторальними органами у сфері захисту критичної інфраструктури до яких належать:Міненерго, Мінцифри, Мінрегіон, Мінекономіки, Мінінфраструктури, Мінстратегпром, Мінфін, МВС, МОЗ, НСЗУ, НКЦПФР.

У воєнних умовах важливість захисту об’єктів критичної інфраструктури ще більше підсилюється через те, що вразливість цих об’єктів негативно впливає на стійкість держави та її здатність до протидії.

Досвід дружніх країн вказує на чітке визначення і реєстр критично важливих об’єктів, а також осіб та уповноважених органів відповідальних за їх захист. Виконавчими органами влади, які здійснюють дії для захисту критичної інфраструктури виступають Збройні сили України, Служба безпеки України, Національна гвардія України, Державна служба з питань надзвичайних ситуацій, Національна поліція України, місцеві органи виконавчої влади, органи місцевого самоврядування, а здійснення заходів щодо забезпечення стійкості виконують оператори критичної інфраструктури.

РОЗДІЛ 2.
АНАЛІЗ СУЧАСНИХ УПРАВЛІНСЬКИХ ПІДХОДІВ ДО ПЛАНУВАННЯ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1. Державне регулювання у сфері захисту критичної інфраструктури

Важливість захисту критичної інфраструктури останнім часом значно зросла в силу багатьох обставин, які виникають як з зовнішніх так і внутрішніх джерел. Закон України «Про критичну інфраструктуру» трактує визначення захист критичної інфраструктури як дії, що спрямовані на вчасне виявлення та запобігання загроз безпеці об’єктів критичної інфраструктури під час їх функціонування, мінімізацію і ліквідацію наслідків у разі їх реалізації.

Законодавство України про критичну інфраструктуру та її захист складають Конституція України, Закон України «Про критичну інфраструктуру», постанова КМУ від 22.07.2022 № 821 «Про затвердження порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури», постанова КМУ від 14.10.2022 № 1174 «Про затвердження Регламенту обміну інформацією між суб’єктами національної системи захисту критичної інфраструктури», постанова КМУ від 09.10.2020 № 1109 «Деякі питання об’єктів критичної інфраструктури», постанова КМУ від 14.10.2022 № 1175 «Деякі питання подання інформації у сфері захисту критичної інфраструктури», наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 15.01.2021 № 23 «Про затвердження Методичних рекомендацій щодо категоризації об’єктів критичної інфраструктури», міжнародні договори України, інші нормативно-правові акти.

Постанова Кабінету міністрів України від 09.10.2020 № 1109 «Деякі питання об’єктів критичної інфраструктури» встановлює критерії і інструменти класифікації об’єктів як частини критичної інфраструктури, визначає список секторів (підсекторів) та основних послуг, які має надавати держава у сфері

критичної інфраструктури, а також процедуру віднесення об’єктів критичної інфраструктури до різних рівнів категорій критичності. Ця постанова розроблена з урахуванням вимог законодавства Європейського Союзу.

Закон України «Про критичну інфраструктуру» встановлює правила для забезпечення роботи та захисту критичних інфраструктур у період без війни. У надзвичайних ситуаціях, надзвичайному та воєнному стані правила захисту визначаються законами України «Про правовий режим воєнного стану», «Про правовий режим надзвичайного стану, «Про функціонування єдиної транспортної системи України в особливий період» та «Про оборону України». Забезпечення кіберзахисту та кібербезпеки критичної інфраструктури регулюється постановою Кабінету міністрів України «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» від 07.09.2022 № 518-2019-п.

Закон України «Про критичну інфраструктуру» визначає основи створення операційного управління національною системою захисту критичної інфраструктури та національної безпеки. Кабінет міністрів України відповідає за здійснення державної політики щодо захисту критичної інфраструктури. Секторальні та функціональні органи у сфері захисту критичної інфраструктури відповідають за формування та впровадження державної політики в окремих секторах критичної інфраструктури.

Формування державної політики, її реалізацію та співпрацю суб’єктів національної системи захисту критичної інфраструктури здійснює уповноважений орган у сфері захисту критичної інфраструктури. Постановою КМУ від 12.07.2022 № 787 «Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України» було визначено Уповноважений орган у сфері захисту критичної інфраструктури, а саме, Державна служба захисту критичної інфраструктури та забезпечення національної системи стійкості.

Згідно з законодавством України, суб’єктами національної системи захисту критичної інфраструктури можуть бути установи, організації, державні

та приватні підприємства та місцеві органи влади, які мають стратегічне значення для національної безпеки. Приватні компанії, що надають послуги у важливих сферах для підтримки життєдіяльності країни також є суб'єктами національної системи захисту критичної інфраструктури.

Захист критичної інфраструктури вимагає вживання комплексу заходів з метою запобігання, виявлення та усунення наслідків надзвичайних ситуацій, які можуть стати причиною порушення функціонування цих об'єктів. Ці заходи проводяться як у період миру, так і в умовах війни [12].

Статтею 14 Закону № 1882-IX суб'єктами національної системи захисту критичної інфраструктури є: Кабінет Міністрів України, Рада національної безпеки і оборони України, Центральна виборча комісія, Національний банк України, Національна комісія з цінних паперів та фондового ринку, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг, Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, Фонд державного майна України і інші органи виконавчої влади зі спеціальним статусом, уповноважений орган у сфері захисту критичної інфраструктури України – Держспецзв'язку, Державна служба України з надзвичайних ситуацій, секторальні та функціональні органи, міністерства і центральні органи виконавчої влади, Службу безпеки України, правоохоронні та розвідувальні органи, суб'єкти оперативно-розшукової та контррозвідувальної діяльності, Збройні Сили України, військові формування, місцеві органи влади (військово-цивільні адміністрації), органи місцевого самоврядування, оператори критичної інфраструктури, підприємства, установи та організації, які займаються діяльністю, що пов'язана із забезпеченням безпеки та стійкості критичної інфраструктури [8].

До основних визначень згідно законодавства України належать:

– оператори критичної інфраструктури – юридична особа та/або фізична особа, яка здійснює управління об'єктом критичної інфраструктури на правах

власності, оренди або на інших законних підставах і несе відповідальність за його поточне функціонування;

– секторальний орган у сфері захисту критичної інфраструктури – це орган нашої держави, який відповідно до законодавства займається розробкою та реалізацією державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури;

– уповноважений орган у сфері захисту критичної інфраструктури України – відповідає за розробку та впровадження державної політики в галузі захисту критичної інфраструктури, здійснює управління національною системою захисту критичної інфраструктури та координує діяльність міністерств і операторів критичної інфраструктури з питань стійкості та захисту об'єктів критичної інфраструктури [8].

Рис. 1.1. Національна система захисту критичної інфраструктури: суб'єктний підхід

Джерело: власні дослідження автора

Захист та стійкість критичної інфраструктури забезпечується шляхом впровадження режимів її функціонування:

– штатний режим;

– режим готовності та запобігання загроз;

– режим реагування на виникнення кризової ситуації;

– режим відновлення штатного функціонування [8].

Секторальні органи, відповідальні за критичну інфраструктуру, мають можливість ухвалювати рішення про введення режимів критичної інфраструктури (ст. 15 Закону № 1882-IX).

Вагомим чинником у захисті критичної інфраструктури є фінансування та залучення інвестицій. Фінансування здійснюється за рахунок коштів державного, місцевого бюджету, коштів операторів критичної інфраструктури та банківських кредитів, позик, коштів міжнародної допомоги та ін. Щороку Верховна Рада України приймає Державний бюджет в якому планують видатки на оборону і національну безпеку. У 2025 році обсяг видатків планується в сумі понад 2,2 трлн. грн. (близько 26% ВВП), з яких на забезпечення функціонування операторів критичної інфраструктури в галузі цивільної авіації – 0,8 млрд. грн., будівництво та реконструкція об’єктів інфраструктури залізничного транспорту – 4,4 млрд. грн., державного фонду регіонального розвитку – 1 млрд. грн., експлуатаційного утримання автомобільних доріг загального користування (мова зокрема про потреби військових та медиків) – 12,6 млрд. грн., будівництва водозаборів та магістральних водогонів для забезпечення водою Миколаєва (продовжуємо долати наслідки російського тероризму і підриву дамби Каховської ГЕС) – 8 млрд. грн. Також держава спрямує 36,4 млрд. грн. для громад, що зазнали негативного впливу у зв’язку з повномасштабною збройною агресією Росії завдяки Єдиному проєктному портфелю екосистеми Dream (унікальна державна електронна екосистема). Основною метою державного бюджету є запровадження нового підходу керування державними інвестиціями та ефективне використання коштів держави спрямовуючи їх на найважливіші проєкти, що відповідають цілям країни в умовах війни [13].

2.2. Організаційні моделі управління безпекою критичної інфраструктури

Для запобігання виникненню кризових ситуацій необхідно визначити важливість інфраструктурних об’єктів, які забезпечують надання основних послуг у всіх галузях економіки і сферах діяльності. Головним критерієм віднесення об’єктів до об’єктів критичної інфраструктури є розуміння наскільки порушення його функціонування або декількох пов’язаних між собою об’єктів критичної інфраструктури можуть викликати негативні наслідки, призвести до кризових ситуацій в екологічній, енергетичній, економічній, фінансовій безпеці, вплинути на стан обороноздатності держави і порушити систему управління нею.

Основні принципи роботи національної системи захисту критичної інфраструктури включають: узгодженість, безпека, захист конфіденційної інформації, цілісність, міжнародне співробітництво.

Статтею 7 Закону № 1882-IX визначено такі рівні управління захистом критичної інфраструктури країни:

– загальнодержавний рівень (впровадження державної стратегії щодо захисту критичної інфраструктури);

– регіональний рівень (контроль та управління критично важливими об’єктами);

– місцевий рівень (організаційне та інженерно-технічне забезпечення ключових об’єктів інфраструктури);

– рівень об’єктів (попередження кризових ситуацій, управління резервами та протидія загрозам).

На загальнодержавному рівні управління українською системою захисту критичної інфраструктури відповідають Кабінет Міністрів, органи влади, центральні органи виконавчої влади та Національний банк України. У їх функції входить розробка планів захисту та безпека критичної інфраструктури.

Планування захисту критичної інфраструктури реалізується у межах повноважень Збройними Силами України, Службою безпеки України, Національною поліцією України, Національною гвардією України, Державною службою України з питань надзвичайних ситуацій.

При Міністерстві розвитку громад, територій та інфраструктури України працює Робоча група з ідентифікації та категоризації об'єктів критичної інфраструктури (далі – Робоча група). Секторальним органом Робочої групи виступає Мінінфраструктури. Робочою групою здійснюється збір і аналіз даних про критично важливі об'єкти, узагальнюється інформація про їх функціонування, ідентифікує їх і категоризує, а також складає перелік таких об'єктів.

Центральна та місцеві органи виконавчої влади здійснюють управління на регіональному та галузевому рівні.

Місцеві урядові структури та військово-цивільні органи управління відповідають за:

– розроблення та затвердження місцевих програм захисту критичних об'єктів і підвищення стійкості місцевих громад до надзвичайних ситуацій;

– розроблення, затвердження та погодження із зацікавленими органами місцевих планів співпраці між ключовими суб'єктами у загрозливій ситуації, планів відновлення діяльності критичної інфраструктури, програм навчання населення з захисту у разі виникнення загроз;

– оцінкою рівня захищеності та безпеки об'єктів критичної інфраструктури через моніторинг їх стану.

Секторальні органи разом із оператором критичної інфраструктури проводять класифікацію об'єктів критичної інфраструктури своїх секторів (підсекторів) згідно з процедурою класифікації об'єктів критичної інфраструктури, та передають інформацію до реєстру об'єктів критичної інфраструктури.

Для виконання вимог закону України «Про основні засади забезпечення кібербезпеки України» та пункту 5 Методики категоризації об'єктів критичної

інфраструктури, затвердженої постановою КабМіну № 1109, Державною службою спеціального зв'язку та захисту інформації України були схвалені Методичні рекомендації щодо категоризації об'єктів критичної інфраструктури (далі – Методичні рекомендації). Методичні вказівки формулюють значення інфраструктурних об'єктів для забезпечення основних послуг у всіх галузях економіки та впровадження заходів щодо захисту цих об'єктів від можливих кризових ситуацій. Постанова Кабінету Міністрів України від 28.04.2023 № 415 передбачає ведення Реєстру об'єктів критичної інфраструктури. Реєстру об'єктів критичної інфраструктури є найбільш захищеним в країні і відокремлений від Інтернету з міркувань безпеки. Доступ до нього неможливий і ведеться вручну в зв'язку з без пековою ситуацією в країні.

Обов'язок забезпечення захисту об'єктів критичної інфраструктури покладено на операторів критичної інфраструктури. Оператори критичної інфраструктури на кожному критично важливому об'єкті розробляють план заходів захисту забезпечення стійкості критичної інфраструктури, в який входять заходи фізичного захисту , протидія загрозам, контроль за ризиками безпеки та їх зменшення, забезпечення безпеки інформації та кібербезпеки. З метою захисту критично важливих об'єктів оператори критичної інфраструктури забезпечують страхування ризику настання кризової ситуації.

ВИСНОВКИ ДО РОЗДІЛУ 2

Останнім часом безпекове середовище значно ускладнилося та вплинуло на якість життя населення України. Початково, захист критичної інфраструктури був спрямований на кліматичні, фізичні, природні загрози,але з часом з'явилися нові. В умовах сьогодення, сукупність засобів захисту критичної інфраструктури має швидко реагувати на загрози будь-якого типу, або їх комбінації.

Державна служба спеціального зв’язку та захисту інформації України, на період воєнного стану, уповноважена здійснювати захист критичної інфраструктури. В її обов’язки входить: виконання державної політики у галузі захисту критичної інфраструктури; є держателем та адміністратором Реєстру об’єктів критичної інфраструктури; направляє процес захисту критичної інфраструктури України; дозволяє узгодити дії суб’єктів системи; допомагає обмінюватися інформацією; створює єдину базу даних загроз та вразливостей критичної інфраструктури; забезпечує паспортизацію та захист об’єктів критичної інфраструктури.

Планування та керування системою захисту критичної інфраструктури України здійснюється на загальнодержавному, регіональному, місцевому та на рівні об’єкта критичної інфраструктури. Кожен рівень здійснює заходи з захисту критичної інфраструктури в межах своїх повноважень.

РОЗДІЛ 3.
ПЕРСПЕКТИВИ ВДОСКОНАЛЕННЯ СИСТЕМИ ПЛАНУВАННЯ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1. Сучасні загрози та ризики для критичної інфраструктури

Сучасний світ досить уразливий. Щороку на усіх континентах нашої планети відбувається велика кількість негативних процесів і явищ таких як, пожежі, грози, землетруси, урагани, дорожньо-транспортні пригоди, аварії, вибухи, авіаційні катастрофи. Всі ці явища мають згубну дію або позбавляють життя людей. Серед найбільших катастроф можна виділити аварію на Чорнобильській АЕС, Великий землетрус у Японії, ураган Харві в США, обвал Генуезького мосту в Італії, кібератаки на українську електромережу.

Нині на території України зберігається високий рівень техногенної та природної небезпеки та вірогідності виникнення надзвичайної ситуації. Причинами можуть бути стихійні лиха, аварії, катастрофи, забруднення океану, зміна клімату, епідемії, війни, терористичні акти. Для їх запобігання та усунення наслідків велике значення мають такі показники як джерела надзвичайних ситуацій та фактори, що впливають на стійкість роботи об’єктів критичної інфраструктури.

У Стратегії національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015) визначено наступні загрози безпеці критичної інфраструктури [6]:

1) основні фонди критичної інфраструктури України знаходяться у поганому стані та не мають достатнього рівня захисту;

2) низький рівень безпеки критичної інфраструктури від терористичних актів і диверсій;

3) неефективне керівництво безпекою критичної інфраструктури та систем життєзабезпечення.

Основними наслідками у випадку реалізації загроз критичній інфраструктури можуть бути часткове або абсолютне припинення надання важливих послуг населенню, суб'єктам господарювання, органам влади, серед яких забезпечення електроенергією, водопостачання та водовідведення, послуги зв'язку, транспортні перевезення та багато інших.

Загрози критичної інфраструктури розподіляються на три групи:

– аварії й технічні збої (порушення технологічних процесів, надмірність строків експлуатації техніки та обладнання, порушення правил їх експлуатації);

– небезпечні явища або процеси геофізичного, геологічного, гідрологічного, атмосферного та іншого витоку таких масштабів, які викликають катастрофічні ситуації, що характеризуються різким порушенням життєдіяльності населення, руйнуванням і знищенням матеріальних цінностей, страху і гибелі людей;

– шкідливі дії здійснювані групами або окремими особами, такими як терористи, злочинці та диверсанти, шпигунство, а також воєнні дії.

В Україні є велика проблема щодо зношеності основних фондів. Внаслідок аварій і технічних збоїв є загроза появі надзвичайних ситуацій на об'єктах електроенергетики, мережах життєзабезпечення, об'єктах підвищеної небезпеки, які використовують небезпечні речовини у великих кількостях. В житлово-комунальній сфері існує аварійність тепло та водопровідних мереж, що призводить до неефективності використання та втраті тепла і води при доставці до кінцевого споживача, підвищенню тарифів на послуги.

До природних явищ і лих слід відмітити метеорологічні та надзвичайні погодні умов (урагани, смерчі, посуха, зливи, заморозки, снігопади), гідрологічні морські та прісноводні явища, виверження вулканів, землетруси, пандемії у людей, тварин, ураження сільськогосподарських рослин хворобами і шкідниками[14]. На протязі останніх десятиліть частота метеорологічних загроз в Україні збільшилась. Підтоплення, обледеніння, посухи несуть за собою небезпечні наслідки для критично важливих об'єктів та процесу їх відновлення.

Надзвичайно небезпечними є поєднані загрози, втілення яких матиме руйнівні наслідки через взаємозалежність елементів критичної інфраструктури. Критична інфраструктура є комплексною системою, тому коли постраждає один компонент, це може призвести до порушень у роботі інших об'єктів.

Значне зростання вчинення дій терористичного характеру на критичні об'єкти в Україні пов'язане з воєнно-політичною ситуацією, оскільки наша країна відстоює територіальну цілісність і суверенітет. Такі дії відбуваються на об'єктах електричної, ядерної енергетики, транспортне забезпечення (об'єкти залізниці), мости. Найбільш масштабною загрозою останніх років, внаслідок злочинних дій з боку російських військ, таких як мінування і підрив, стало знищення греблі Каховської гідроелектростанції 6 червня 2023 року. У зоні катастрофи опинилося приблизно 16 тисяч людей, 80 населених пунктів, частину яких затопило. Підрив Каховської ГЕС спричинив жахливі гуманітарні та екологічні наслідки та вплинуло на роботу Запорізької атомної гідроелектростанції. Щоб відновити Каховську ГЕС, яку підірвали російські війська, треба залучити мільярди доларів та євро.

Відносно новим видом загрози є кібератака. Кібератаки здійснюють як окремі особи, так і цілі організації в політичних, кримінальних або особистих цілях для знищення засекреченої інформації чи отримання доступу до неї. Вони спрямовані на пошкодження важливих документів і систем у корпоративній або персональній комп'ютерній мережі, а також отримання доступу до них. Сервери державних, фінансових установ, політичних партій, компаній, воєнні об'єкти, мережі телекомунікацій стають жертвами кібератак. Вперше кібератаку на енергетичну систему України здійснено у грудні 2015 року, зловмисникам вдалося вивести її з ладу. Російські хакери атакувати комп'ютерні системи управління найбільших трьох енергопостачальних компаній. Друга, з наслідками для України, кібератака сталась у грудні 2016 року. За одну годину сталося відключення підстанції «Північна» енергокомпанії «Укренерго». Частина споживачів правого берега міста Києва та найближчих районів області залишилися без електричної енергії. Найбільше

постраждали споживачі АТ «Прикарпаттяобленерго» через першу кібератаку, яка вимкнула близько 30 підстанцій. Протягом шести годин без світла залишалось 230 тисяч мешканців [18].

Наступним інцидентом кібератаки була подія 12 грудня 2023, коли стався масштабний збій у роботі провідного оператора мобільного зв'язку України «Київстар». На території усієї країни у абонентів «Київстар» з'явилися проблеми з мобільним зв'язком і Інтернетом, що призвело до неможливості підключення мереж інших операторів в межах внутрішнього роумінгу. Двадцять чотири мільйони абонентів залишились без зв'язку. Неполадки в обладнанні «Київстар» викликали серйозні інфраструктурні проблеми по всій Україні [19].

За даними ДСНС України з початку війни Росія завдала таких втрат на українській території:

– зруйновано житлових будинків у Донецькій області – 89 тис. 342, Київській – 26 тис. 192, Харківській – 6 тис. 157, Миколаївській – 5 тис. 449, Запорізькій – 3 тис. 612 будинків;

– зруйновано повністю близько 22 тисячі споруд критичної інфраструктури, майже 140 тисяч певною мірою зруйновано;

– офіційна кількість загиблих серед цивільного населення – 4 731 тис.;

– близько 10 тисяч пожеж виникли унаслідок обстрілів [20].

З 2014 року об'єкти критичної інфраструктури зазнали серйозних пошкоджень і руйнувань. З часом масштаби руйнувань поширилися по всій країні та нанесли суттєві збитки економічній ситуації України, зокрема, в енергетичній, транспортній, залізничній, дорожній, авіаційній, портовій сферах, великим і середнім приватним підприємствам, державним компаніям. Багато об'єктів, таких як електростанції, водопровідні системи, транспортні мережі та комунікаційна інфраструктура, залишаються позбавленими функціональності або працюють на мінімальному рівні продуктивності через руйнування та несправності [21].

Поточний стан об’єктів критичної інфраструктури, спричинений масштабними руйнуваннями, потребує невідкладних заходів з відновлення та модернізації, при цьому важливим є скоординованість дій усіх структур, які будуть задіяні для відновлення на загальнодержавному, регіональному та місцевому рівнях.

3.2. Шляхи вдосконалення системи планування та забезпечення безпеки критичної інфраструктури

Головним завданням об’єктів критичної інфраструктури є забезпечення основних потреб людей, їх стабільність і безперебійність у роботі у звичайний час та в нестабільних умовах. Умови війни підсилюють важливість захисту об’єктів критичної інфраструктури, оскільки вразливість таких об’єктів може негативно впливати на міцність країни та можливість супротиву.

В умовах війни захист об’єктів критичної інфраструктури набуває додаткової актуальності, оскільки вразливість об’єктів критичної інфраструктури негативно впливає на стійкість держави та її здатності до опору. Практика інших країн вказує, що актуальним є визначення переліку об’єктів критичної інфраструктури та осіб уповноважених органів відповідальних за їх захист.

Вперше проблемою захисту критично важливих об’єктів почали займатися у Великій Британії. Британське Міністерство внутрішніх справ у 1999 році створило координаційний безпековий центр національної інфраструктури. У 2007 році на його заміну створено окремий центр із захисту національної критичної інфраструктури при уряді. У законодавстві Великої Британії велика увага приділяється боротьбі з терористичними та кіберзагрозами, захисту об’єктів, що відносяться до критичних та інших важливих галузей для економіки країни.

У Сполучених штатах Америки (США) створено при Міністерстві внутрішньої безпеки США урядовий орган, що здійснює захист критичної інфраструктури та Агентство з питань кібербезпеки та безпеки інфраструктури – здійснює опір загрозам критичній інфраструктурі. У своєму законодавстві США визначають об'єкти критичної інфраструктури як комплекс фізичних, віртуальних систем і засобів, які є критично важливими для держави, оскільки порушення їх діяльності може спричинити серйозні проблеми у сферах оборони, економіки, охорони здоров'я та безпеки нації.

Двосторонній фонд урядів Ізраїлю та Сполучених штатів Америки створили спільний проєкт розвитку кібертехнологій для критично важливої інфраструктури. Даний проєкт спрямований на розробку засобів захисту від шкідливих кібератак та інноваційних рішень для захисту критично важливої інфраструктури, щоб задовольнити національні потреби Ізраїлю та США у сфері кібербезпеки у таких галузях як енергетичний комплекс, виробничі підприємства, морські порти, авіація, малі і середні підприємства. Відділ розвитку та технологій міністерства внутрішньої безпеки США, Національний кіберпідрозділ Ізраїлю та Фонд BIRD спільно заснували програму BIRD Cyber для зміцнення кібербезпеки та захисту критично важливих об'єктів в Ізраїлі та США, які можуть стати мішенями кіберзагроз та щоденними спробами злому [46].

Відповідальною особою у діяльності критичної інфраструктури Франції є прем'єр-міністр, за організаційне забезпечення відповідає генеральний секретаріат з оборони і національної безпеки.

У Франції за координацію діяльності галузі критичної інфраструктури відповідає прем'єр-міністр, а на організаційному рівні ці функції виконує генеральний секретаріат з оборони і національної безпеки, який підпорядковується безпосередньо прем'єр-міністру. Законодавство Франції вважає критичними всі сектори, що забезпечують важливі соціальні, економічні процеси країни включаючи управління державним сектором, збройні сили, промисловість, виробництво, судочинство та ін. [22].

Держави – члени ЄС приділяють особливу увагу посиленню стійкості своєї критичної інфраструктури. Для цього уряди багатьох європейських країн розробляють стратегічні завдання. Європейський Союз проголосив нові пріоритети політики забезпечення стійкості функціонування критичної інфраструктури та надання життєво важливих послуг на ринку ЄС. Нові стратегічні цілі та завдання Єврокомісії та держав-членів визначено в Рекомендаціях Ради ЄС, спрямованих на посилення зусиль Європейського Союзу щодо підвищення стійкості критично важливих об'єктів інфраструктури. Рада Європейського Союзу у 2022 році ухвалила «Рекомендації зі скоординованого підходу до стійкості критичної інфраструктури» та оновили правила спрямовані на захист критичної інфраструктури.

В Україні у 2014 році Законом України № 1882-IX було приведено у відповідність деякі питання захисту об'єктів критичної інфраструктури, а саме:

– створення реєстру об'єктів, яким необхідно захист;

– делегування функцій контролю і координації з питань захисту на Кабінет Міністрів України;

– визначено Державну службу спеціального зв'язку та захисту інформації України відповідальною за захист в мирний час, у воєнний час – Генеральний штаб Збройних Сил України [23].

Але, нажаль, в умовах воєнного стану, чіткий алгоритм захисту критичної інфраструктури та ефективне реагування на загрози збройного ураження відсутні. Важливим завданням сьогодення є посилення рівня захисту і безпеки об'єктів критичної інфраструктури (протиповітряне прикриття), кіберзахист.

На думку фахівців центру безпекових досліджень Національного інституту стратегічних досліджень підсилити захист об'єктів критичної інфраструктури України можна за допомогою [22]:

– вжиття додаткових невідкладних системних заходів з посилення безпеки об'єктів критичної інфраструктури з боку відповідних органів державної влади, керівників державних та приватних підприємств і установ, з належним ресурсним забезпеченням (всі критично важливі об'єкти, особливо

ті, що відновлюються, повинні бути оснащені надійними захисними спорудами);

– розвитку інтегрованої системи протиповітряної оборони для захисту об’єктів критичної інфраструктури та паливно–енергетичного сектору як одного з головних стратегічних завдань захисту держави під час збройної агресії та в післявоєнний період;

– уточнення місії інтегрованої системи протиповітряної оборони з посилення захисту об’єктів критичної інфраструктури, зокрема об’єктів паливно-енергетичного сектору;

– узгодження дій органів влади всіх рівнів щодо захисту об’єктів критичної інфраструктури, маскування, забезпечення захисними спорудами та інших заходів безпеки;

– чіткого розподілу відповідальності за захист кожного об’єкта критичної інфраструктури, моніторингу рівня його захисту та своєчасного прийняття необхідних рішень [22].

З огляду на загрози й виклики, які все більше посилюються, подальший розвиток воєнної ситуації в Україні вимагає концептуального перегляду засад діяльності всієї національної системи захисту критичної інфраструктури. Відповідно потреби забезпечення захисту й безпеки національної критичної інфраструктури вимагають чіткого розуміння змісту сучасних загроз та їхніх проявів, побудову актуальної моделі загроз для організації ефективної протидії.

Лідером у пошуку удосконалення наявних систем управління і створення нових є технології. Сучасні технології, такі як, генеративний ШІ, інформаційні (ІТ) та оперативні технології (ОТ) забезпечують інтеграцію об’єктів критичної інфраструктури до загальної системи керування та збору даних, завдяки автоматизації допомагають покращити процес прийняття рішень, якість обслуговування, підвищують продуктивність. Мережа ОТ здійснює диспетчерське керування, автоматизацію будівель та розподілення системи керування. Вони використовуються для моніторингу та управління двигунами, датчиками або контролерами, постійно збирають і надсилають відповідні дані.

Для поліпшення системи організації та планування безпеки критичної інфраструктури пропонується:

– вдосконалення законодавства з питань захисту об’єктів критичної інфраструктури з метою конкретизації невідкладних завдань, чіткого визначення переліку загроз національній критичній інфраструктурі та її об’єктам;

– створення чіткої структури органів виконавчої влади відповідальної за сектори критичної інфраструктури, перелік об’єктів критичної інфраструктури і плани їх захисту, обсяг необхідних для захисту сил і засобів, внесення пропозицій і змін до законодавчих актів;

– покладення функцій захисту на правоохоронні органи, що мають військові підрозділи, які забезпечать охорону і оборону об’єктів критичної інфраструктури;

– створення чітких і прозорих правил і вимог, які дозволять приватному сектору економіки розуміти коло зобов’язань і відповідальності у питанні захисту об’єктів критичної інфраструктури та яку допомогу може надати держава;

– обмін досвідом з дружніми країнами-партнерами з можливістю укладання спільних договорів у питанні захисту критичної інфраструктури.

Для впровадження сучасних цифрових технологій у систему захисту критичної інфраструктури необхідно забезпечити фінансування з різних джерел. Одним із основних джерел є державний бюджет. Іншим важливим джерелом фінансування можуть стати міжнародні гранти та кредити. Уряд України може співпрацювати з міжнародними фінансовими організаціями, такими як Світовий банк, Європейський банк реконструкції та розвитку, або Європейський Союз. Ці установи часто підтримують реформи в країнах, що розвиваються, шляхом надання фінансових ресурсів і технічної допомоги. Гранти можуть бути використані для впровадження інновацій.

ВИСНОВКИ ДО РОЗДІЛУ 3

Загрозу для стабільного функціонування будь-якої держави несуть стихійні лиха, катаклізм, диверсії, військові дії, кібератаки. Особливо небезпечними є комбіновані загрози, що можуть спричинити катастрофічний ефект для усіх елементів критичної інфраструктури. За останні роки об’єкти критичної інфраструктури зазнали серйозних пошкоджень і масштабних руйнувань, серед яких, електростанції, водопровідні системи, транспортні мережі та комунікаційна інфраструктура та функціонують на мінімальному рівні продуктивності.

Поточний стан об’єктів критичної інфраструктури, спричинений масштабними руйнуваннями, потребує невідкладних заходів з відновлення та модернізації. Враховуючи зарубіжний досвід та рекомендації центру безпекових досліджень Національного інституту стратегічних досліджень у системі організації та планування забезпечення безпеки критичної інфраструктури запропоновано наступні заходи у плануванні і забезпеченні безпеки критичної інфраструктури:

– в умовах воєнного стану удосконалювати законодавство щодо захисту критичної інфраструктури;

– запровадження чіткого механізму функціонування секторів критичної інфраструктури та секторальних органів у сфері захисту критичної інфраструктури;

– здійснити ефективну координацію між різними рівнями управління які здійснюють захист об’єктів критичної інфраструктури;

– пошук ефективних рішень у відновленні зруйнованих об’єктів критичної інфраструктури та чіткого розподілу відповідальності за захист кожного об’єкта критичної інфраструктури.

ВИСНОВКИ

Під поняттям «критичної інфраструктури» розуміють об’єкти, які мають надзвичайну важливість для функціонування економіки та суспільства країни. До них можна віднести електростанції, системи водопостачання, місця виготовлення та зберігання харчових продуктів , важливі вузли транспортного сектору, телекомунікації, медичні установи та інші об’єктів, що мають пріоритет.

Безпека таких об’єктів, збереження їх функціональності є пріоритетом держави. Галузі критичної інфраструктури між собою тісно пов’язані. Виведення з ладу окремого об’єкту вплине на роботу інших об’єктів та мереж. Навіть при наявності надійних засобів для захисту таких об’єктів, потрібні особливі міри безпеки та тісна взаємодія з міжнародними партнерами для створення відповідних умов. Посилення загроз у всьому світі зумовили актуалізацію питання захисту систем.

Захист об’єктів критичної інфраструктури в Україні являє собою систему заходів у законодавчих, організаційних, технологічних інструментах спрямованих на гарантування безпеки та стійкості критичної інфраструктури. Стійкість критичної інфраструктури – можливість надійно виконувати свої функції у нормальних умовах, швидке відновлення після аварій і налаштування до змін, технічних проблем, кібератак, катастроф і інших небезпек.

Виникнення ризиків для критичної інфраструктури природного характеру, техногенні катастрофи, терористичні атаки, хакерські атаки, потребує проведення відповідних заходів, що спрямовані на запобігання і подолання таких атак. Державна служба захисту критичної інфраструктури та Державну службу спеціального зв’язку та захисту інформації регулює політику заходів з захисту, забезпечуючи правильну координацію та належну співпрацю між різними суб’єктами захисту критичної інфраструктури.

Лідером у пошуку удосконалення наявних систем управління і створення нових є технології. Вони використовуються для моніторингу та управління

об’єктами критичної інфраструктури. З метою удосконалення планування забезпечення безпеки критичної інфраструктури пропонуються наступні кроки:

– вдосконалення законодавства з питань захисту об’єктів критичної інфраструктури з метою конкретизації невідкладних завдань, чіткого визначення переліку загроз національній критичній інфраструктурі та її об’єктам;

– створення чіткої структури органів виконавчої влади відповідальної за сектори критичної інфраструктури, перелік об’єктів критичної інфраструктури і плани їх захисту, обсяг необхідних для захисту сил і засобів, внесення пропозицій і змін до законодавчих актів;

– покладення функцій захисту об’єктів критичної інфраструктури на правоохоронні органи, що мають у своєму розпорядженні збройні формування, які здатні забезпечити виконання завдань охорони і оборони об’єктів критичної інфраструктури;

– створення чітких і прозорих правил і вимог, які дозволять приватному сектору економіки розуміти коло зобов’язань і відповідальності у питанні захисту об’єктів критичної інфраструктури та яку допомогу може надати держава;

– обмін досвідом з дружніми країнами – партнерами з можливістю укладання спільних договорів у питанні захисту критичної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Яременко О. І., Страхніцький Я. О. Теоретичні підходи до визначення дефініції критичної інфраструктури як об'єкту державного управління. Публічне управління у сфері державної безпеки та митної справи, № 1 (32), 2022. URL: http://customs-admin.umsf.in.ua/archive/2022/1/13.pdf.

2 National Strategy for Critical Infrastructure Protection (CIP Strategy). URL: https://www.kritis.bund.de

3 Ustawa ozarzą dzaniu kryzysowym. Dz. U. 2007 Nr 89 poz. 590. URL: http://isap.sejm.gov.pl/isap.nsf/

4 Офіційний веб-сайт Centre for the Protection of National Infrastructure. URL: http://www.cpni.gov.uk/

5 Стратегія національної безпеки України «Україна у світі, що змінюється». URL: https://zakon.rada.gov.ua/ laws/show/105/2007

6 Указ Президента України «Про рішення Ради національної безпеки і оборони України від 06.05.2015 р. «Про Стратегію національної безпеки України» № 287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text

7 Зелена книга з питань захисту критичної інфраструктури в Україні: зб. Матеріалів міжнар. експерт. нарад. Упоряд. Д.С. Бірюков, С.І Кондратов ; за заг. ред. О.М. Суходолі. К.: НІСД, 2016. 176 с

8 Закон України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX. Відомості Верховної Ради України. 2022. № 3. С. 20. URL: https://zakon.rada.gov.ua/laws/show/1882-20

9 Вікіпедія: вільна енциклопедія. URL: https://uk.wikipedia.org/wiki Керування_ризиком

10 Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України. Проєкт постанови Кабінету Міністрів України «Про затвердження Вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури І категорії критичності». URL: https://cip.gov.ua/ua/draft-acts/proyekt-pkmu-vimog-shodo-upravlinnya-rizikami-bezpeki-na-ob-yektakh-

kritichnoyi-infrastrukturi-i-kategoriyi-kritichnosti

11 Указ Президента України «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки» від 16.02.2022 № 56/2022. URL: https://https://zakon.rada.gov.ua/laws/show/56/2022#Text

12 Суб'єкти критичної інфраструктури: все, що варто знати. URL:https://www.kyivpost.com/uk/post/28283

13 Офіційний сайт Міністерства розвитку громад та територій України. URL: https://https://mtu.gov.ua.

14 Постанова кабінету міністрів України «Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього» від 28.04.2023 № 415. URL: https://zakon.rada.gov.ua/rada/show/415-2023-%D0%BF#n15.

15 Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України від 151.01.2021 № 23 «Про затвердження Методичних рекомендацій щодо категоризації об'єктів критично інфраструктури». URL: https://https://zakon.rada.gov.ua/rada/show/v0023519-21#Text

16 Безпека життєдіяльності: Навч. посіб. / За ред. В.Г. Цапка. 2-ге вид., перероб. і доп. К.: Знання–Прес, 2003. 397 с.

17 Бедрій. Я.І. Безпека життєдіяльності: Навчальний посібник. Київ: Кондор, 2009. 286 с.

18 Іванюта С. П. Загрози критичній інфраструктурі та їхвплив на стан національної безпеки (моніторинг реалізації Стратегії національної безпеки). Аналітична записка.URL:https://www.niss.gov.ua/doslidzhennya/nacionalna-bezpeka/zagrozi-kritichniy-infrastrukturi-ta-ikh-vpliv-na-stan-nacionalnoi

19 Українські оператори зв'язку можуть отримати статус критично важливих об'єктів.URL: https://deps.ua/ua/news/novosti-rynka/10893.html

20 Майже 22 тис. об'єктів критичної інфраструктури зруйновано внаслідок ворожих атак – ДСНС. Армія INFORM. URL:

https://armyinform.com.ua/2022/06/29/majzhe-22-tys-obyektiv-krytychnoyi-infrastruktury-zrujnovano-vnaslidok-vorozhyh-atak-dsns/

21 Магомедов А. О. «Ризики та загрози для об'єктів критичної інфраструктури та шляхи їх подолання». Інвестиції: практика та досвід № 15/2024.

22 Костянтин Кононенко, Віктор Павленко, Петро Крикун «Як удосконалити захист об'єктів критичної інфраструктури в Україні». Інформаційне агентство Оборонно–промисловий кур'єр. URL: https://https://opk.com.ua

23 Храпкіна В.В., Трушкіна Н.В. Механізми забезпечення стійкості критичної інфраструктури: європейський досвід. URL: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/956affad-5103-4f4b-b19f-cbbe18e4c839/content.

24 Мельник Д.С.. Побудова моделі загроз національній критичній інфраструктурі України як основа забезпечення її безпеки та стійкості. *Вісник ХНУВС*. 2024. № 1(104).

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

26 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. Випуск 3 (13). С. 142-148.

27 Про місцеве самоврядування в Україні: Закон України від 21.05.1997 р. №280/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/280/97-вр.

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

29 Степаненко Ярослав. Цифровізація та важливість безпеки мережі ОТ. Інформаційна агенція ЛІГА Бізнес Інформ. URL: https://https://blog.liga.net/user/yastepanenko/article/tsifrovizatsiya-ta-vajlivist-bezpeki-mereji-ot.

30 Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури: Розпорядження Кабінету Міністрів України № 825-р. від 19 вересня 2023 р. URL: https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text

31 Деякі питання паспортизації об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України № 818 від 04.08.2023 р. URL:https://ips.ligazakon.net/document/TM072049

32 Звіт про прямі збитки інфраструктури від руйнувань внаслідок військової агресії Росії проти України станом на початок 2024 року. URL:https://kse.ua/wp-content/uploads/2024/04/01.01.24_Damages_Report.pdf

33 Кизим М. О., Хаустова В. Є., Трушкіна Н. В. Сутність поняття «критична інфраструктура» з позицій національної безпеки України. БІЗНЕСІНФОРМ. 2022. № 12. URL: https://www.business-inform.net/export_pdf/business-inform-2022-12_0-pages-58_78.pdf

34 Томашук Я. Об'єкти критичної інфраструктури: детальний аналіз та відповіді на поширені питання. URL: https://smarttender.biz/blog/view/ob-yekti-kritichnoyi-infrastrukturi-detalniy-analiz-ta-vidpovidi-na-poshireni-pitannya/

35 Критична інфраструктура забезпечена альтернативними джерелами живлення: Тернопільська ОВА. URL: https://suspilne.media/ternopil/917103-kriticna-infrastruktura-zabezpecena-alternativnimi-dzerelami-zivlenna-ternopilska-ova/

36 За рік війни РФ завдала збитків інфраструктурі України майже на $144 млрд. – KSE. URL: https://forbes.ua/news/za-rik-viyni-rf-zavdala-zbitkiv-infrastrukturi-ukraini-mayzhe-na-144-mlrd-kse-22032023-12556

37 Магомедов А. О. Ризики та загрози для об'єктів критичної інфраструктури та шляхи їх подолання. *Інвестиції: практика та досвід.* 2024. № 15. С. 216–221.

38 Національний банк посилить роботу щодо захисту критичної інфраструктури фінансового сектору. URL: https://bank.gov.ua/ua/news/all/natsionalniy-bank-posilit-robotu-schodo-zahistu-kritichnoyi-infrastrukturi-finansovogo-sektoru

39 Гора, І. В., Батюк, О. В. Окремі питання захисту об’єктів критичної інфраструктури: зарубіжний досвід. *Соціально–правові студії*. 2021. № (1), 11.

40 Директива Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту. URL: https://zakon.rada.gov.ua/laws/show/984_002-08#Text.

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

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

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

44 ФранчукВ.І., ПригуновП.Я., Мельник С.І.. Безпека об’єктів критичної інфраструктури в Україні: організаційно – нормативні проблеми та підходи. *Соціально–правові студії*, 2021. Випуск 3 (13). С. 142-148.

45 Інтерв’ю голови Держспецзв’язку від 15.11.2023 «Бути об’єктом критичної інфраструктури – це і великі переваги, і чіткі зобов’язання. URL: https://interfax.com.ua/news/interview/947864.html

46 Ростислав Вонс. Ізраїль та США створять технологію для захисту критичної інфраструктури від кібератак. Онлайн-медіа «Інформаційне агентство «Главком». URL: https://glavcom.ua/techno/hitech/izrajil-ta-ssha-stvorjat-tekhnolohiju-dlja-zakhistu-kritichnoji-infrastrukturi-vid-kiberatak-950387.html#google_vignette

47 Харченко А. М.. Забезпечення безпеки та стійкості критичної інфраструктури. Інструменти і практики публічного управління в контексті децентралізації : Матеріали IV Міжнародної науково-практичної конференції, 22–23 червня 2023 року. – Житомир: Поліський національний університет, 2023.