DOI 10.52363/2414-5866-2024-1-43
УДК 351.863 + 338.246.87

Кічата Н.М., *асистент, НАУ, м. Київ,*
ORCID:0000-0002-6991-3970,
Третьяков О.В., *д.т.н., професор, НАУ, м. Київ*
ORCID:0000-0002-0457-9553

Kichata N., *assistantof the Department of Civil and Industrial Safety, National Aviation University, Kyiv,*
Tretyakov O., *Doctor of Technical Sciences, Professor, Professor of the Department of Civil and Industrial Safety, National Aviation University, Kyiv*

ШЛЯХИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

WAYS TO IMPROVE THE EFFICIENCY OF STATE POLICYIMPLEMENTATION IN THE SPHERE OF CRITICAL INFRASTRUCTURE PROTECTION

У статті наведено обгрунтування теоретичних принципів державного управління в сфері захисту критичної інфраструктури в Україні. Проаналізовано функції та завдання, спрямовані на забезпечення безпеки та підвищення стійкості об'єктів критичної інфраструктури. Проведено аналіз потенційних загроз та небезпек, які можуть вплинути на критичну інфраструктуру, визначено відмінності між ними. Наведено способи вдосконалення державних механізмів забезпечення безпеки та підвищення ефективності захисту критичної інфраструктури. Розроблено рекомендації щодо захисту та підвищення стійкості об'єктів критичної інфраструктури. Розроблені пропозиції можуть бути успішно використані для подальшої розробки концептуальних засад удосконалення захисту критичної інфраструктури в Україні.

Ключові слова: *критична інфраструктура, об'єкти, держава, загроза, небезпека, стійкість, захист.*

The article provides substantiation of theoretical principles of public administration in the sphere of critical infrastructure protection in Ukraine. The functions and tasks aimed at ensuring the safety and increasing the stability of critical infrastructure objects were analyzed. The analysis of potential threats and dangers that can affect the

ISSN 2414-5858 (Print)
ISSN 2414-5866 (Online)

critical infrastructure was carried out, and the differences between them were determined. Methods of improving the state mechanisms for ensuring safety and increasing the efficiency of protecting critical infrastructure are provided. Recommendations for the protection and resiliency of critical infrastructure objects have been developed. The developed proposals can be successfully used for further development of conceptual foundations for improving the protection of critical infrastructure in Ukraine.

***Key words**: critical infrastructure, state, threat, danger, resilience, protection.*

Постановка проблеми. Побудова сучасної системи захисту критичної інфраструктури (КІ) – це складний та багатоаспектний процес, який вимагає поєднання правових, технічних, організаційних підходів, з урахуванням міжнародного досвіду, для забезпечення безпеки та стійкості цих важливих об’єктів.

Підвищення ефективності реалізації державної політики в сфері захисту критичної інфраструктури є край важливим завданням для забезпечення безпеки, стабільності та розвитку суспільства.

Пріоритетність у актуалізації непорушності основних принципів і фундаментальних засад забезпечення національної безпеки має надзвичайно важливе значення для будь-якої суверенної держави світу. Нині, в умовах військової агресії, для України це питання номер один у сфері державного управління.

Критична інфраструктура України – це системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких може призвести до значних негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки [1].

Прикладами критичної інфраструктури можуть бути: енергетична інфраструктура (електростанції, газопроводи, нафтопроводи, електричні мережі), транспортна інфраструктура (аеропорти, мости, тунелі, залізничні системи, морські та річкові порти), інформаційно-комунікаційна інфраструктура (мережі зв’язку, інтернет-інфраструктури, дата-центри), водопостачання і каналізація, системи охорони здоров’я (лікарні, аптечні склади, системи телемедицини), фінансова і банківська інфраструктура, харчова інфраструктура (сховища продуктів, продуктові мережі) та інші сектори, що можуть бути важливими для національної безпеки та економіки, такі як оборона, вугільна промисловість тощо.

Один з основних аспектів конкретизації та визначення необхідних заходів для захисту об’єктів критичної інфраструктури – це постійна співпраця між державою і інфраструктурними організаціями. У такій ситуації держава виступає гарантом внутрішньої безпеки та виконує роль посередника в інформаційно-комунікаційних процесах. З іншого боку, інфраструктурні організації, які, як правило, володіють найбільш повною інформацією щодо конкретної кризової ситуації і мають найбільшу компетентність

у вирішенні цих проблем (як технічно, так і професійно), здатні вживати ефективні заходи для їхнього захисту. З цього погляду, відповідні структури, які керують управлінням кризовими ситуаціями, повинні приймати конкретні заходи для усунення наслідків конкретної ситуації. Крім того, експерти та науковці підкреслюють необхідність створення системи контролю, такої як «система ризик-менеджменту, яка дозволить вчасно виявляти тенденції і факти, що становлять загрозу для подальшого існування суспільства» [2].

Захист критичної інфраструктури передбачає розробку та впровадження стратегій та заходів з метою забезпечення її стійкості, відновлення та захисту від можливих загроз. Це включає в себе заходи кібербезпеки, плани реагування на надзвичайні ситуації, контингентні плани, технічні засоби захисту та інші заходи, спрямовані на запобігання та реагування на ризики та небезпеки, що можуть вплинути на критичну інфраструктуру.

Головною метою розробки концепції основних заходів для захисту об'єктів критичної інфраструктури є забезпечення безпеки людей шляхом зменшення ризику вразливості критичних компонентів інфраструктури перед військовими атаками, природними катастрофами, техногенними аваріями або помилками людей, а також зниження рівня вразливості до актів тероризму. Ця концепція має включати в себе стандартизовані будівельні, організаційні, кадрові та технічні заходи безпеки, які допоможуть забезпечити захист [1, 3].

Організаційну структуру, функціонування та майбутній розвиток системи захисту критичної інфраструктури визначає держава. Тому саме предметом дослідження є нормативне та адміністративне забезпечення державного управління критичною інфраструктурою. Об'єктом дослідження є система державного управління безпекою та забезпеченням життєво важливої інфраструктури для населення і територій.

Аналіз останніх досліджень і публікацій. Система захисту критичної інфраструктури в контексті національної безпеки України показує, що вона має значний обсяг теоретичних досліджень українських та закордонних вчених. Автори, які зробили вагомий внесок у цю область: М.Б. Домарацький, Я. О. Страхніцький, Д. Г. Бобро, Ю. А. Абрамов, С. С. Теленик, В. А. Андронов, Ю.М. Бєлоусов, Б. Е. Братка, П. Б. Волянський, А. Б. Качинський, В. В. Коврегін, В. А. Ліпкан, О. А. Мельниченко, Д. О. Полковниченко, В. О. Пономаренко, А. В. Ромін, В. П. Садковий, В. Ю. Стрельцов, Г. П. Ситник, М. В. Сунгуровський та інших.

У той же час, деяким аспектам цієї важливої проблематики, зокрема питанням розробки ефективних стратегій розвитку державного управління для критично важливих об'єктів, практично приділено не достатньо уваги. Ці проблеми залишаються недостатньо дослідженими, як з практичної, так і з теоретичної точки зору. Особливо сьогодні, в сучасних умовах війни і

загроз національній безпеці України, досягнення стабільного соціально-економічного розвитку вимагає забезпечення економічної стійкості кожного регіону та стійкості соціально-економічних систем на більш низьких рівнях, таких як галузі, підприємства та фінансові установи.

Створення системи управління національним процесом захисту критичних об'єктів тісно пов'язане з розробкою основних стратегічних напрямів регіональної політики, яку здійснюють органи місцевого самоврядування в Україні для забезпечення критично важливих об'єктів в надзвичайних ситуаціях та у випадках терористичних актів. Розробка такої регіональної політики включає в себе багаторівневий процес, який повинен враховувати різні природні явища та інші фактори, що можуть мати вплив на загальну систему управління цим процесом. Це підкреслює В. Могильниченко у своїх дослідженнях [4].

Відповідальність за захист критичної інфраструктури залишається за національними органами влади, як детально викладено у роботі О. Мельничука [5].

Сучасна критична інфраструктура держави представляє собою складний комплекс різноманітних компонентів, які мають різні характеристики. Вона включає в себе різні організаційні структури, різні моделі управління, функції та системи, які існують як у фізичному, так і у віртуальному просторі. Управління критичною інфраструктурою включає участь державних структур на всіх рівнях з різними областями відповідальності та повноваженнями, а також власників і операторів об'єктів і систем, що входять до критичної інфраструктури. У зв'язку з процесами глобалізації, національна безпека, виробництво, економіка і фінанси кожної країни стають залежними від чинників, що визначають стан безпеки в інших країнах і на глобальному рівні.

Постановка завдання. Мета роботи полягає в розкритті сутності державного управління забезпеченням безпеки об'єктів критичної інфраструктури та проведені оцінки можливих небезпек і загроз критичній інфраструктурі України, задля підвищення ефективності захисту об'єктів критичної інфраструктури.

Виклад основного матеріалу. Сучасна українська держава стикається з найскладнішим випробуванням з точки зору безпеки за всю свою історію незалежності. Гостра соціально-політична криза, військові дії, посилення екстремізму та тероризму, економічний спад, масштабна гуманітарна криза, руйнування та пошкодження численних підприємств і інфраструктурних об'єктів – це всі нові реалії, з якими сьогодні стикається Україна. В цих умовах головним пріоритетом є забезпечення безпеки громадян, суспільства і державних інституцій.

Критична інфраструктура є ключовою для функціонування суспільства та економіки, і вона сильно залежить від держави у багатьох аспектах.

Наприклад те, що держава відіграє важливу роль у регулюванні та захисті критичної інфраструктури. Вона встановлює стандарти безпеки, приймає правила та політику, яких повинні дотримуватися операторами критичної інфраструктури для запобігання кіберзагрозам, терористичним атакам та іншим загрозам.

Державні інвестиції та фінансування можуть бути вирішальними для розвитку та модернізації критичної інфраструктури. Держава може надавати фінансову підтримку для проєктів, спрямованих на покращення безпеки, надійності та стійкості систем.

Держава забезпечує систему нагляду та контролю за критичною інфраструктурою, щоб вчасно реагувати на потенційні загрози.

Держава відіграє ключову роль у кризовому управлінні та реагуванні на інциденти, що можуть вплинути на критичну інфраструктуру. Вона розробляє та впроваджує плани відновлення та роботи систем після інцидентів.

З огляду на зростання кіберзагроз, держава відіграє ключову роль у забезпеченні цифрової безпеки критичної інфраструктури. Вона повинна сприяти впровадженню передових технологій, стандартів та практик кібербезпеки.

У світі великої глобалізації держави співпрацюють для забезпечення міжнародної безпеки критичної інфраструктури. Це може включати обмін інформацією про кіберзагрози, спільні проєкти та стандарти безпеки.

Саме держава може і повинна визначати стратегії стійкості та запасів для забезпечення продовження роботи критичної інфраструктури під час кризових ситуацій або екстремальних обставин, які ми бачимо на сьогодні.

Забезпечення безпеки і захисту критичної інфраструктури є однією з ключових функцій держави, оскільки недостатність або втрата функціонування таких систем може призвести до серйозних наслідків для економіки, суспільства та національної безпеки.

В Україні захист об’єктів, які, відповідно до міжнародної практики, вважаються «критичною інфраструктурою» регулюється різними нормативно-правовими актами, які, переважно, стосуються внутрішнього використання. Така ситуація виникла логічно, оскільки кожне окреме відомство було спроможним визначити конкретні загрози для своїх підпорядкованих об’єктів і володіло власним набором інструментів та ресурсів для забезпечення їх безпеки.

Як вказано в Законі України «Про критичну інфраструктуру» [6] серед завдань, пов’язаних із формуванням та впровадженням державної політики захисту критичної інфраструктури України та створення відповідної державної системи, можна виділити такі аспекти: забезпечення безпеки, стійкості та недоторканності критичної інфраструктури України, запо-

бігання кризовим ситуаціям, які можуть призвести до порушень в роботі критичної інфраструктури, утворення та організація державної системи захисту критичної інфраструктури, розроблення нормативно-правової бази з питань безпеки об'єктів, розроблення та реалізація державних цільових програм, розроблення комплексу заходів, аналіз сучасних викликів та загроз, які можуть вплинути на стійкість критичної інфраструктури, а також оцінка рівня її захищеності.

Нормативно-правове регулювання у сфері захисту критичної інфраструктури включає в себе різноманітні закони, стандарти та положення, які мають на меті забезпечення безпеки та надійності критичних об'єктів. Зазвичай це регулювання орієнтоване на важливі сектори, такі як енергетика, транспорт, інформаційні технології, комунікації та інші, які є визначальними для економічного функціонування та безпеки країни.

Сектор критичної інфраструктури охоплює всі об'єкти, що відносяться до певної галузі економіки або мають спільну функціональну спрямованість в межах цього сектору. Відповідно до Постанови Кабінету Міністрів України від 16 грудня 2022 р, № 1384, уповноважені органи визначають об'єкти критичної інфраструктури в своїх секторах (підсекторах) критичної інфраструктури, використовуючи перелік секторів (підсекторів) і основних послуг цієї інфраструктури [7].

Секторальні органи вказують на різні галузеві міністерства та відомства, які відповідають за різні аспекти управління та регулювання в сфері захисту КІ.

Одні сектори можуть бути взаємозалежними, і порушення в одному секторі може мати наслідки для інших. Така взаємодія може включати обмін інформацією, розробку спільних стратегій захисту, планування екстрених ситуацій, а також координацію дій у разі кризових подій.

Забезпечення ефективної взаємодії між секторами в регіонах допомагає зменшити ризики та підвищити стійкість перед потенційними загрозами, такими як військові дії, техногенні аварії, кібератаки та інші небезпеки. У цьому контексті розвиток механізмів співпраці та обміну інформацією між різними секторами та регіональними органами стає ключовим елементом забезпечення стійкості та безпеки національної критичної інфраструктури України.

Державна політика у сфері захисту критичної інфраструктури базується на наступних принципах: гарантування надійності та стабільності критичної інфраструктури; визначення правових вимог до основних принципів, стратегічних напрямків, підходів до захисту критичної інфраструктури; визначення суб'єктів, які складають національну систему захисту критичної інфраструктури, їхніх повноважень та відповідальності; створення умов і впровадження заходів, спрямованих на ефективне управління та контроль над ризиками безпеки, зниження ризику реалізації можливих

загроз, а також на ліквідацію наслідків загроз та інших подій; розроблення системи раннього виявлення загроз критичній інфраструктурі; запровадження механізмів державно-приватного партнерства та співпраці між суб'єктами господарювання та населенням у питаннях забезпечення безпеки та стійкості критичної інфраструктури; підтримка міжнародного співробітництва в галузі захисту критичної інфраструктури; створення умов для швидкого відновлення надання життєво важливих функцій та послуг у випадку реалізації загроз і порушень функціонування критичної інфраструктури [8].

Основні повноваження державної політики включають в себе:

– розроблення стратегічних напрямків у галузі захисту критичної інфраструктури;

– законодавчу діяльність;

– міжнародне співробітництво;

– організацію системи захисту;

– створення програм і проектів,

– визначення стандартів і вимог з питань безпеки об'єктів критичної інфраструктури на всіх етапах їх життєвого циклу та аналіз ризиків і загроз для критичної інфраструктури.

Ці повноваження визначаються законами та нормативними актами України і забезпечують розвиток та функціонування системи захисту критичної інфраструктури в країні.

Державна політика України у сфері захисту критичної інфраструктури включає в себе ряд функцій та завдань, спрямованих на забезпечення безпеки та стійкості критичних об'єктів.

Законодавча функція: розробка та прийняття законів, нормативних актів та правил, що регулюють захист критичної інфраструктури. Це включає в себе створення нормативно-правової бази для ідентифікації критичних об'єктів, встановлення вимог до їх захисту, а також регулювання обов'язкових стандартів безпеки. В Україні за законодавчу функцію у сфері захисту критичної інфраструктури відповідає Верховна Рада України, яка має повноваження приймати закони та нормативно-правові акти, що регулюють цю сферу.

Координаційна функція: організація співпраці та координація діяльності між різними органами влади, агентствами та структурами, що забезпечують захист критичної інфраструктури. Мета полягає в уніфікації дій та об'єднанні зусиль для забезпечення ефективного захисту. У сфері захисту критичної інфраструктури в Україні координаційну функцію виконує Державна служба з надзвичайних ситуацій України (ДСНС України).

Аналітична функція: збір, аналіз та оцінка інформації про потенційні загрози та ризиків для критичної інфраструктури. Ця функція передбачає постійний моніторинг ситуації та розробку прогнозів для виявлення

нових загроз. Аналітичну функцію в сфері захисту критичної інфраструктури в Україні зазвичай виконує низка державних та недержавних організацій та інститутів. До найбільш важливих організацій, які можуть здійснювати аналітичну діяльність у цій сфері, належать: ДСНС України, Міністерство цифрової трансформації України, Державна служба стандартизації, метрології та сертифікації України, громадські організації та експерти.

Фінансова функція: виділення фінансових ресурсів для здійснення заходів захисту критичної інфраструктури. Це включає в себе виділення бюджетних коштів, фінансування проєктів та програм, спрямованих на зміцнення безпеки об'єктів. У сфері захисту критичної інфраструктури в Україні фінансову функцію виконують декілька ключових структур та організацій: державний бюджет України, ДСНС України, Міністерство цифрової трансформації України, донорські організації та міжнародні проєкти.

Освітньо-інформаційна функція: інформування громадськості, підприємств та інших зацікавлених сторін про загрози та заходи захисту критичної інфраструктури. Освітні кампанії та інформаційні заходи допомагають підвищити обізнаність та готовність суспільства до дій у надзвичайних ситуаціях. Освітньо-інформаційна функція у сфері захисту критичної інфраструктури в Україні виконується спільними зусиллями державних та цивільних структур: Міністерством цифрової трансформації України, ДСНС України, Міністерством освіти і науки України, Міністерством внутрішніх справ України, Міністерством оборони України, громадськими організаціями.

Технічна функція: забезпечення наявності та доступності сучасних технічних засобів та технологій для захисту критичної інфраструктури. Це включає в себе розробку та впровадження систем контролю, виявлення та реагування на загрози. Технічна функція у сфері захисту критичної інфраструктури в Україні виконується різними структурами та відомствами залежно від конкретного сектору та виду інфраструктури: Міністерство цифрової трансформації України, ДСНС України, Міністерство енергетики та захисту довкілля України, Міністерство внутрішніх справ України, Міністерство оборони України, Міністерство транспорту, Міністерство охорони здоров'я та ін., які забезпечують технічний захист і безпеку відповідних об'єктів.

Кризовий менеджмент: розробка та впровадження планів кризового управління, які передбачають дії у надзвичайних ситуаціях та реагування на аварії чи катастрофи. ДСНС України грає ключову роль у координації та управлінні надзвичайними ситуаціями на об'єктах критичної інфраструктури в державі.

Міжнародна співпраця: співпраця з іншими країнами та міжнародними організаціями у сфері захисту критичної інфраструктури для обміну

інформацією, досвідом, навчанням, участю в міжнародних проєктах та програмах, а також спільними заходами для підвищення рівня стійкості та захищеності об'єктів критичної інфраструктури від потенційних загроз. Міжнародна співпраця в цій сфері відбувається на різних рівнях, і ДСНС є однією з ключових установ, що забезпечують координацію та реалізацію цієї співпраці в Україні.

Державна політика в сфері захисту критичної інфраструктури має на меті забезпечити стабільність та безпеку суспільства, захист важливих об'єктів і ресурсів, а також готовність до дій в надзвичайних ситуаціях техногенного, природного та військового характеру.

Визначення загроз є важливим етапом у процесі захисту критичної інфраструктури і включає в себе різні аспекти. Спочатку потрібно визначити всі можливі загрози, які можуть вплинути на критичну інфраструктуру. Ця ідентифікація включає в себе аналіз можливих джерел загроз, таких як природні явища (повені, землетруси, урагани), техногенні аварії (поломки обладнання, витоки небезпечних речовин, тощо), акти тероризму, кібератаки, людський фактор та інші.Після чого обов'язково потрібно проаналізувати вразливості критичної інфраструктури, що можуть бути використані загрозами для спричинення шкоди або перешкоди нормальному функціонуванню. Визначити можливі наслідки або збитки, які можуть виникнути внаслідок реалізації загроз.

Всі загрози потрібно згрупувати і класифікувати за різними критеріями, такими як тип загрози (природні, техногенні, терористичні), можливість реалізації загрози, потенційні наслідки тощо. Необхідно визначити та встановити пріоритет для кожної загрози залежно від її важливості та можливості виникнення. Розробити стратегії та плани заходів для запобігання, реагування та відновлення внаслідок реалізації загроз. І також здійснювати постійний моніторинг загроз, надавати оцінку їх актуальності та оновлення заходів із захисту відповідно до змін у загрозах або вразливості.

Цей процес є постійним і динамічним, оскільки загрози можуть змінюватися з часом, і заходи із захисту повинні бути адаптовані до нових умов. Визначення загроз є важливою передумовою для розробки ефективної стратегії та планування заходів із захисту критичної інфраструктури.

Небезпека відрізняється від загрози тим, що загроза має спрямований характер і призначена для цільового об'єкта, системи або території, в той час як небезпека є більш загальним імпульсом, або наслідком реалізації загрози. Багато методів аналізу стійкості регіонів орієнтовані на узагальнену небезпеку або сценарії, які є основою для проведення аналізу (наприклад, дослідження впливу втрати електроенергії на критично важливу галузь проводиться через загрозу втрати електроенергії). Однак аналіз, спрямований на наслідки, зазвичай фокусується на конкретній за-

грозі (наприклад, кібератака на системи промислового управління об’єктом або систему критичної інфраструктури) або небезпеці (наприклад, ураган, який впливає на порт).

Потенційний вплив загроз і небезпек на сферу критичної інфраструктури може бути різноманітним і включати в себе: матеріальні збитки, загрозу життю та здоров’ю людей, перешкоди в нормальному функціонуванні, економічні втрати, заворушення суспільного порядку, вплив на природне середовище, втрати інформації та даних, загрози для національної безпеки.

Щоб врахувати загрози та небезпеки при аналізі регіональної стійкості, важливо розуміти характер цих загроз та як вони можуть вплинути на відповідну інфраструктуру. Отже, аналіз загроз і небезпеки нерозривно пов’язаний з аналізом вразливості. Існують різні рівні аналізу загроз і небезпек, які можна застосовувати в залежності від обсягу оцінки та бажаного рівня складності.

Перший рівень аналізу – це загальна оцінка вразливості інфраструктури щодо можливих загроз або небезпек. Основна мета полягає в тому, щоб з’ясувати, чи існує потенціал для впливу цих загроз на інфраструктурні системи. На цьому етапі не проводиться докладний аналіз конкретного впливу, але досліджується можливість такого впливу. Наприклад, цей рівень аналізу може включати визначення ступеня залежності інфраструктурних систем від підключених до Інтернету систем управління, що свідчить про загальну вразливість до кіберзагроз та можливих перебоїв.

Другий рівень аналізу фокусується на більш детальному розгляді конкретної загрози або небезпеки і вразливості інфраструктури до неї. На цьому рівні проводиться також аналіз потенційних наслідків для інфраструктури і для інших залежних об’єктів. Для цього потрібне більш глибоке технічне розуміння конкретної загрози або небезпеки, а також самої інфраструктури. Наприклад, на цьому рівні може проводитися аналіз конкретних кіберзагроз і технічної вразливості використовуваних систем або моделювання впливу паводків на об’єкти інфраструктури.

Оцінка потенційного впливу загроз і небезпек є важливим кроком у розробці стратегій та планів захисту критичної інфраструктури. Вона дозволяє визначити пріоритети та необхідність заходів для запобігання, реагування та мінімізації наслідків загроз і небезпек.

Оцінка загроз критичній інфраструктурі може бути проведена за допомогою різних методів та підходів [9, 10].

1. Експертний метод: вимагає участі експертів, які мають глибокі знання у сфері критичної інфраструктури та потенційних загроз. Експерти оцінюють ймовірність та наслідки різних загроз на основі свого досвіду та знань.

2. Аналітичний метод: використовує аналітичні інструменти, такі

як статистика, математичні моделі, імітаційне моделювання тощо, для оцінки загроз. Наприклад, можна аналізувати історичні дані щодо інцидентів у сфері критичної інфраструктури та робити прогнози на цій основі.

3. Моделювання загроз: використовується створення математичних моделей, які дозволяють аналізувати можливі наслідки різних загроз. Це може включати моделювання поведінки природних катастроф, кібератак, терористичних актів.

4. SWOT-аналіз: використовує аналіз SWOT (Strengths, Weaknesses, Opportunities, Threats), щоб визначити внутрішні і зовнішні фактори, які впливають на критичну інфраструктуру. Загрози визначаються як зовнішні негативні фактори.

5. Мультикритеріальний аналіз: використовується для визначення вагомості різних загроз та їх впливу на критичну інфраструктуру. Зазвичай використовуються числові показники для оцінки загроз.

6. Оцінка імовірності та наслідків: для кожної загрози визначається ймовірність її виникнення та можливі наслідки для критичної інфраструктури. Ці параметри потім комбінуються для визначення рівня загрози.

7. Аналіз вразливості: визначає, наскільки вразлива критична інфраструктура на різні види загроз. Це включає в себе оцінку заходів, призначених для захисту інфраструктури.

Вибір конкретного методу або комбінації методів залежить від конкретних умов і завдань оцінки загроз для критичної інфраструктури.

Серед усіх загроз різного походження для безпеки критичної інфраструктури найбільш важливими визначено такі [11]:

- природні: повені, екстремальні погодні явища, лісові пожежі, землетруси, епідемії та пандемії, епізоотії;

- техногенні: промислові аварії, ядерні/радіологічні аварії, аварії на транспорті, втрата критично важливої інфраструктури, кібератаки, терористичні атаки.

Особливої уваги потребують взаємозв’язки та взаємозалежності між загрозами природного походження, коли виникнення одних небезпечних явищ призводить до формування нових через механізм «каскадних ефектів» [3]. Наприклад, така загроза як небезпечні погодні явища пов’язана з наступними загрозами: повені, зсуви, пожежі, забруднення, втрата критичної інфраструктури, транспортні аварії; забруднення з пандеміями.

Сьогодні по всій Україні спостерігаємо зростання ризиків виникнення надзвичайних ситуацій техногенного походження через руйнування багатьох промислових і житлових споруд внаслідок військових дій. Терористичний характер воєнних дій з боку росії, полягає у спрямованому та навмисному пошкодженні критично важливих громадських інфраструк-

турних об’єктів держави. Ця стратегія включає в себе руйнування водосховищ, гідроелектростанцій, розподільчих станцій, систем електропостачання, газопостачання, підприємств, будівель, залізничних і дорожніх мереж, засобів зв’язку, об’єктів життєдіяльності населення, а також загрози використання ядерних вибухових пристроїв, хімічних, біологічних, токсичних та інших небезпечних речовин, які становлять серйозну загрозу для населення і довкілля.

Варто відмітити зростання кібернетичних загроз для об’єктів критичної інфраструктури держави, обумовлених хакерськими атаками, що можуть призвести до відмов важливої інформаційної інфраструктури. Хакерські атаки були націлені на об’єкти критичної інформаційної інфраструктури енергогенеруючих і енергопостачальних компаній, об’єктів транспорту, ряду банківських установ, телекомунікаційних компаній. Повідомлення про ураження інформаційних систем комерційних компаній надходили, зокрема, від мережі Auchan, поштової служби DHL, комерційних банків і телеком-операторів (Київстар). Зараженими вірусом виявились численні державні ресурси включаючи системи міністерства інфраструктури, Державної фіскальної служби, електророзподільчі мережі компанії Укренерго.

Дослідження у сфері запобігання та протидії загрозам різного походження підтверджують необхідність впровадження ризик-орієнтованого підходу у державну систему захисту населення від надзвичайних ситуацій природного та техногенного характеру. Це необхідно для ефективного передбачення та зменшення ризику виникнення різних катастроф для об’єктів критичної інфраструктури [12].

З метою аналізу загроз на об’єкті КІ, необхідно ідентифікувати і детально вивчити всі можливі ризики, враховуючи загрози, визначені у відповідних нормативних актах (зазвичай це робиться державними органами з питань безпеки та правопорядку). Крім цього, важливо враховувати індивідуальні особливості та характер небезпек, які можуть виникати на конкретному об’єкті критичної інфраструктури.

Для запобігання негативним наслідкам загроз та небезпек створюється система раннього виявлення та попередження їх. Крім того, внесені зміни до політики підприємства щодо фінансування в сфері безпеки. Для досягнення цієї мети розробляються проєкти, які надають перевагу належному захисту об’єкта критичної інфраструктури в умовах конкуренції.

В Україні сьогодні різні міністерства і відомства виконують оцінку загроз у своїх відповідних галузях використовуючи власні методи та критерії. Проблемою є відсутність можливості порівняти та об’єднати отримані результати, оскільки вони часто несумісні між собою. Також існує недостатня координація та співпраця між різними відомствами у цій об-

ласті, і недостатнє врахування результатів наукових досліджень у практичній діяльності.

Наявні методи оцінювання загроз на основі історичного досвіду мають свої недоліки, оскільки вони не враховують нові виклики та ситуації, які раніше не мали аналогів. Це призводить до зниження надійності та точності прогнозів, оскільки вони обмежені попереднім досвідом.

Все важливішою стає необхідність розробки стандартних і універсальних процедур та інструкцій для ефективного реагування на типові загрози. Визначення таких загроз, створення сценаріїв кризових ситуацій та створення відповідних баз даних стають основними завданнями, які передбачає національна система оцінювання ризиків і загроз.

Окресливши специфіку державного управління забезпеченням безпеки критичної інфраструктури в Україні та здійснивши оцінку ризиків критичній інфраструктурі від потенційного впливу загроз і небезпек бачимо, що потребується вдосконалення державних механізмів забезпечення безпеки та підвищення ефективності захисту критичної інфраструктури.

Необхідно розробляти конкретні заходи захисту для кожного об’єкта критичної інфраструктури. Це включає в себе заходи щодо кіберзахисту, фізичного забезпечення, резервування та відновлення, а також плани екстреного реагування. Впроваджувати технічні заходи безпеки, наприклад, встановлювати сучасні системи захисту кожного типового об’єкту КІ, шифрувати дані, забезпечувати резервні джерела енергії або альтернативні тощо.

Одним із шляхів подальшого удосконалення механізму координації співпраці та взаємодії між суб’єктами управління безпекою КІє інтеграція передових технологій, таких як штучний інтелект, для автоматизації процесів виявлення та реагування на загрози. Використання технологічних рішень може допомогти забезпечити більш швидке та точне реагування на інциденти.

Обов’язковою складовою є розроблення алгоритму дій при появі відповідних загроз для типових об’єктів КІ. Наразі в Україні існують або формуються кілька систем, які призначені для нагляду та захисту об’єктів та інфраструктури, пов’язаної з інформацією. Для ефективного розроблення планів взаємодії та координації дій серед цих систем необхідно узгодження та прийняття спільної термінології, визначення взаємозв’язків між різними режимами, рівнями та умовами функціонування систем, а також узгодження принципів управління у складних кризових ситуаціях.

Дуже важливим кроком є співпраця з приватним сектором: багато об’єктів критичної інфраструктури перебувають у приватній власності. Ефективна політика захисту КІ вимагає партнерства і співпраці між державними органами та приватним сектором для спільного забезпечення захисту.

Цільовим заходом є забезпечення організації підготовки кадрів щодо захисту КІ. Для цього потрібно встановити співпрацю з університетами та іншими освітніми установами для впровадження спеціалізованих програм та курсів з безпеки критичної інфраструктури, розробити спеціалізовані навчальні курси та програми, які охопили б усі аспекти безпеки, кібербезпеки, управління кризами та відновлення після них, а також основи захисту інфраструктури.

Для оцінки ефективності політики захисту КІ важливо мати систему моніторингу та аналітики для постійного відстеження потенційних загроз та реагування на них. Наприклад, використовувати систему спостереження для виявлення змін у рівні безпеки, які можуть вказувати на можливі загрози або прогностичну модель для передбачення можливих загроз у геополітичному, екологічному або соціальному контексті, аналізувати вразливості інфраструктури для ідентифікації початку загроз. Також для оцінки можливих небезпек та їх потенційного впливу на критичну інфраструктуру можна застосувати методи моделювання. Моделювання включає процес створення моделі критичної інфраструктури, яка охоплює її ключові складові, системи чи комплексів. Ці моделі повинні як можна точніше відтворювати основні характеристики і складові частини інфраструктури, описувати основні процеси їх функціонування, а також уявлення загроз та їх впливу на інфраструктуру.

Важливою задачею являється введення штатного режиму роботи в сферізахисту КІ, тобто проводити аналіз потенційних загроз, планувати умови роботи інформаційних систем та визначати заходи реагування відповідно до визначених загроз та їх впливу на різних рівнях важливості. Застосовувати заходи, які спрямовані на уникнення потенційних загроз або зменшення наслідків від них.

Вміти реагувати своєчасно на подію або загрозу з метою відновлення роботи інформаційних систем до попередніх параметрів та надання життєво важливих функцій.

Важливим кроком для підвищення готовності та сприяння ефективному захисту критичної інфраструктури є включення громадськості у процес реалізації політики захисту КІ та публічна освіта щодо цих питань, інформування.

Завершальним етапом є відновлення режимів функціонування КІ з урахуванням досвіду для покращення процесу відновлення у майбутньому. Загальна ефективність політики захисту КІ залежить від інтеграції всіх цих аспектів та постійного вдосконалення стратегій та заходів захисту. Реагування на нові загрози та зміни в інфраструктурному середовищі також є важливою частиною ефективної політики захисту КІ.

Висновки. На сьогодні в Україні сучасну модель державної політики у сфері захисту КІ в умовах військового стану не вивчено достатньо

глибоко. Для ефективного створення стратегічних напрямків щодо реалізації державної політики у сфері захисту КІ необхідно ознайомитись, зрозуміти глибину та складність реальних проблем, що виникають в країні під час активних воєнних дій і терористичних актів, які впливають на об'єкти критичної інфраструктури в реальному часі. Ці знання необхідно враховувати при корегуванні в майбутньому державної політики щодо захисту об'єктів критичної інфраструктури.

Серед одних з найсуттєвіших проблем можна виділити недолік механізмів реагування на кризові ситуації та нормативно-правової бази, яка б уточнювала відповідальність та повноваження відповідних державних установ у цій області. Треба врахувати, що можливості ухвалення законодавчих рішень були обмежені через відсутність чи недосконаліть потрібних рішень.

Відсутність чіткого законодавчого порядку і рішень щодо введення воєнного стану призвела до відсутності чітких та однозначних правил узгодження між державою та суб'єктами підприємницької діяльності, обмеживши можливість залучення ресурсів підприємств для забезпечення стійкості роботи критичної інфраструктури. Також виникли труднощі у координації дій держави та підприємств з метою захисту та оборони важливих об'єктів критичної інфраструктури.

Уряд держави повинен проаналізувати наступні важливі аспекти сучасної ситуації країни: 1) розглянути спектр поточних і передбачуваних критичних загроз і ризиків; 2) оцінити стан та структуру економіки країни; 3) дослідити суспільно-політичну обстановку в країні; 4) проаналізувати загальну інституційну практику державного управління; 5) переглянути основи конституційного ладу країни.

Усвідомлюючи ситуацію сьогодення, дослідження українського правового поля в галузі захисту інформації на об'єктах критичної інфраструктури вказує на недостатність національних та спеціалізованих нормативних вимог стосовно гарантування безпеки інформації об'єктів критичної інфраструктури в Україні.

Оцінюючи стратегії державної політики стосовно захисту КІ під час воєнного конфлікту, можна зауважити, що головним чинником залишається регулювання позицій нормативного правового підходу до інституційних аспектів цього питання.

Список використаних джерел:

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

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

3. Мельниченко О. А. Надзвичайні ситуації техногенного характеру: сутність та засоби державного управління. Вісник Національного університету цивільного захисту України. Державне управління. Київ, 2014. №2. С. 149–156.

4. Захист населення і територій від надзвичайних ситуацій. Техногенна та природна небезпека / за заг. ред. В. В. Могильниченка. Київ: КІМ, 2007. 636 с.

5. Мельничук О. Управління критичною інфраструктурою держави: базові методи та критерії ідентифікації об'єктів // Державне управління та місце всамоврядування: збірник наук. праць. Дніпро, 2019, Вип. 3 (42). С.13-27.

6. Про критичну інфраструктуру: Закон України від 16.11.2021р. №1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text(дата звернення: 15.12.2023).

7. Деякі питання об'єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 р. № 943. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text(дата звернення: 15.12.2023).

8. Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України: Рішення Ради національної безпеки і оборони України від 01.03.2014. / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/n0001525-14 (дата звернення: 15.12.2023).

9. Корченко А.О. Метод оцінки рівня критичності для систем управління кризовими ситуаціями / за ред.: А.О. Корченко, В.А. Козачок, А.І. Гізун // Захист інформації. 2015. Т. 17, № 1. С. 86–98. URL: http://nbuv.gov.ua/UJRN/Zi_2015_17_1_14 (дата звернення: 15.12.2023).

10. Risk assessment methodologies for critical infrastructure protection. Part I: a state of theart / G. Giannopoulos, R. Filippini, M. Schimmer. Luxembourg: Joint Research Centre of Institute for the Protection and Security of the Citizen, 2012. 70 p.

11. Risk assessment methodologies for critical infrastructure protection. Part II:a new approach. Luxembourg: Joint Research Centre of Institute for the Protection and Security of the Citizen, 2015. 28 p.

12. Іванюта С. П., Качинський А. Б. Екологічна та природно-техногенна безпека України: регіональний вимір загроз і ризиків: монографія. Київ: НІСД, 2012. 308 с.

13. Комаров М. Ю. Методика побудови системи управління інформаційною безпекою на об'єктах критичної інфраструктури / М. Ю. Комаров, С. Ф. Гончар // Моделювання та інформаційні технології. 2017. Вип. 81. С. 12-19.

14. Цюрупа М. Зміна парадигм воєнно-політичного мислення у доктринах та стратегіях воєнної безпеки України XX–XXI ст.: українознавчий альманах. 2021. Вип. 28. С. 120–126.

дата надходження статті: 07.05.2024
дата прийняття статті: 17.05.2024
дата публікації: 28.06.2024