DOI https://doi.org/10.51647/kelm.2022.7.15

CECHY POLITYKI PAŃSTWOWEJ OCHRONY INFRASTRUKTURY KRYTYCZNEJ W UKRAINIE I KIERUNKI JEJ POPRAWY W WARUNKACH WOJNY

Yaroslav Strakhnitskyi
aspirant Katedry Administracji Publicznej i Administrowania
Winnickiego Państwowego Uniwersytetu Pedagogicznego im. Mychajła Kociubynskiego (Winnica, Ukraina)
ORCID ID: 0000-0002-3066-0961
strahnitskiy@gmail.com

Adnotacja. W przepisach artykułu naukowego autor analizuje regulacyjne ramy prawne i prace naukowców dotyczące nowoczesnych aspektów polityki państwa w zakresie ochrony infrastruktury krytycznej w Ukrainie i kierunku jej poprawy w warunkach wojny. W wyniku analizy aktów prawnych podsumowano poziomy zarządzania, odpowiedzialne organy i ogólny skład podmiotów krajowego systemu ochrony infrastruktury krytycznej. W praktycznym wdrożeniu architektury bezpieczeństwa narodowego zidentyfikowano quadrokompleks autonomicznych państwowych systemów ochrony. Należy zauważyć, że krajowe ramy regulacyjne i prawne w obecnej formie nie mogą być wiarygodną podstawą do opracowania i wdrożenia planów i procedur koordynacji działań, interakcji i wymiany informacji między istniejącymi w Ukrainie systemami ochrony, bezpieczeństwa i reagowania kryzysowego. Zidentyfikowane luki instytucjonalne w działalności podmiotów bezpieczeństwa infrastruktury krytycznej proponuje się wyeliminować na podstawie wdrożenia niektórych elementów zagranicznej praktyki ochrony obiektów infrastruktury krytycznej. Szczególną uwagę zwraca się na ideę zrównoważonego rozwoju infrastruktury krytycznej.

Słowa kluczowe: infrastruktura krytyczna, polityka publiczna, systemy ochrony, systemy reagowania kryzysowego, odporność infrastruktury krytycznej.

Yaroslav Strakhnitskyi
Postgraduate student of the Department of Public Administration
Vinnytsia Mykhailo Kotsiubynsky State Pedagogical University
(Vinnytsia, Ukraine)
ORCID ID: 0000-0002-3066-0961
strahnitskiy@gmail.com

Abstract. In the provisions of the scientific article, the author conducts an analysis of the regulatory legal framework and the works of scientists regarding modern aspects of the state policy of protection of critical infrastructure in Ukraine and directions for its improvement in wartime conditions. As a result of the analysis of regulatory legal acts, management levels, responsible bodies and the general composition of subjects of the national critical infrastructure protection system were summarized. In the practical implementation of the national security architecture, a quadrocomplex of autonomous state protection systems has been identified. It is noted that the national legal framework in its current form cannot be a reliable basis for the development and implementation of plans and procedures for the coordination of actions, interaction and information exchange between the protection, security and crisis response systems existing in Ukraine. Identified institutional gaps in the activities of critical infrastructure security entities are proposed to be eliminated based on the implementation of certain elements of foreign practice of protecting critical infrastructure objects. Special attention is paid to the idea of ensuring the stability of critical infrastructure.

Key words: critical infrastructure, state policy, protection systems, crisis response systems, critical infrastructure sustainability.

ОСОБЛИВОСТІ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ ТА НАПРЯМИ ЇЇ УДОСКОНАЛЕННЯ В УМОВАХ ВІЙНИ

Ярослав Страхніцький
аспірант кафедри публічного управління та адміністрування
Вінницького державного педагогічного університету
імені Михайла Коцюбинського (Вінниця, Україна)
ORCID ID: 0000-0002-3066-0961
strahnitskiy@gmail.com

Анотація. У положеннях наукової статті автор проводить аналіз нормативно правової бази та праць науковців щодо сучасних аспектів державної політики захисту критичної інфраструктури в Україні та напрями її удосконалення в умовах війни. У результаті аналізу нормативно-правових актів узагальнено рівні управління, відповідальні органи та загальний склад суб'єктів національної системи захисту критичної інфраструктури. У практичній реалізації архітектури національної безпеки ідентифіковано квадрокомплекс автономних державних систем захисту.

Відзначається, що національна нормативно-правова база в її теперішньому вигляді не може бути надійною основою для розробки і реалізації планів і процедур координації дій, взаємодії та обміну інформацією між існуючими в Україні системами захисту, безпеки та кризового реагування. Виявлені інституційні прогалини у діяльності суб'єктів безпеки критичної інфраструктури запропоновано усунути на основі імплементації окремих елементів закордонної практики захисту об'єктів критичної інфраструктури. Особлива увага приділено ідеї забезпечення стійкості критичної інфраструктури.

Ключові слова: критична інфраструктура, державна політика, системи захисту, системи кризового реагування, стійкість критичної інфраструктури.

Вступ. Сучасні глобальні військові загрози тягнуть за собою комплекс наслідків і потребують координації дій усіх національних систем безпеки та кризового реагування. Масштабні терористичні дії російської федерації на території України спричиняють деструктивний вплив на повсякденне життя населення, функціонування суспільних і державних інститутів та національної економіки. Нівелюючи міжнародні закони та звичаї ведення війни, країна агресор систематично ставить під удар цивільну інфраструктуру та об'єкти життєзабезпечення населення. У такій ситуації на перший план виходять питання державної політики із забезпечення безперервності функціонування критичної інфраструктури. Важливість даного сегменту у тому, що він є основою забезпечення сталості життєдіяльності мирного населення.

Як відомо, запорукою злагодженого забезпечення національної безпеки є наукова обґрунтованість державної політики. Сьогодні державна політика у сфері захисту критичної інфраструктури перебуває у режимі тестування в реальному часі на предмет цілісності та ефективності в умовах реальних військових загроз. Зазначимо, що структурні підрозділи національної системи безпеки та кризового реагування в Україні, побудовані на основі відомчих підходів. Відповідальні за безпеку критичної інфраструктури секторальні органи діють виключно в межах своїх «наборів загроз» та мають власні уніфіковані алгоритми реагування і термінологію. Дана ситуація створює певні проблеми у вигляді неузгодженості процедур і механізмів та відсутність чіткого розподілу відповідальності за дії у разі виникнення загроз. Серед основних інструментів усунення зазначених проблем та забезпечення адекватного реагування на безпекові виклики для України варто відзначити наукове обґрунтування напрямків удосконалення державних систем координації сфери забезпечення захисту та стійкості критичної інфраструктури в умовах війни. Проведенню відповідних досліджень із зазначеного спектру проблем у світовій науковій літературі присвятили свої праці вчені Бурбела Т.М., Кондратов С.І., Зубко Г.Ю., Суходоля О.М., Петрашко І.Р., які можуть стати не тільки предметом наукових дискусій, а й бути використаними у напрямку усунення виявлених проблем.

Мета статті – визначити особливості державної політики захисту критичної інфраструктури в Україні та розглянути перспективні напрями її удосконалення в умовах війни. Формування науково обґрунтованих засад координації структурно-функціонального суб'єктного складу відповідального за реалізацію державної політики у сфері захисту критичної інфраструктури.

Основна частина. Згідно Закону «Про критичну інфраструктуру» Державна політика у сфері захисту критичної інфраструктури передбачає формування комплексу заходів, спрямованих на забезпечення безпеки критичної інфраструктури, які розподілено на блоки: організаційний, нормативно-правовий, інженерно-технічний, ресурсний, інформаційно-аналітичний, методологічний (Закон України «Про критичну інфраструктуру» №1882-IX)**.** Зауважимо, що у практичній реалізації архітектури національної безпеки можемо ідентифікувати квадрокомплекс автономних державних систем захисту:

1. Єдина державна система цивільного захисту (ЄДСЦЗ);
2. Єдина система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків (ЄСЗРПТА);
3. Державна система фізичного захисту (ДСФЗ);
4. Національна система кібербезпеки (НСК)

Вітчизняні вчені акцентують увагу на тому, що наявна інституційна структура безпеки критичної інфраструктури в її теперішньому вигляді не може бути надійною основою для розробки і реалізації планів і процедур координації дій, взаємодії та обміну інформацією між існуючими в Україні системами захисту, безпеки та кризового реагування (Кондратов, Суходоля, 2020: 20). Розробка дієвих планів і процедур координації дій, взаємодії та обміну інформацією потребує, щонайменше, прийняття спільної термінології, визначення співвідношень між режимами, рівнями та умовами функціонування систем, узгодження принципів управління комплексною кризою, яка пов'язана з дією кількох небезпечних факторів, що має бути враховане при розробці та коригуванні документів оперативного і тактичного рівнів.

На сучасному етапі реформування сектору безпеки і оборони держави слід вважати доцільним створення єдиної державної системи захисту критичної інфраструктури на основі існуючих національних систем захисту, безпеки та кризового реагування за умов досягнення якісно нового рівня координації дій та взаємодії між ними (Петрашко, 2020:31).

Основоположним нормативним актом у сфері державної політики захисту критичної інфраструктури на даний час є Закон Україним «Про критичну інфраструктуру». Проаналізуємо основні його положення. Закон визначає рівні управління національною системою захисту критичної інфраструктури, серед яких встановлено:

1) Загальнодержавний рівень. Управління здійснюється Кабінетом Міністрів України, уповноваженим органом у сфері захисту критичної інфраструктури України, органами державної влади відповідно

до розподілу повноважень, іншими центральними органами виконавчої влади та державними органами та Національним банком України.

2) Регіональний та галузевий рівні. Управління здійснюється центральними та місцевими органами виконавчої влади, визначеними в установленому законом порядку відповідальними за забезпечення формування та реалізацію державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури та відповідальними за функціонування окремих державних систем захисту та реагування.

3) Місцевий рівень. Управління здійснюється місцевими органами виконавчої влади (військово-цивільними адміністраціями в умовах військового стану), органами місцевого самоврядування в межах повноважень.

4) Об'єктовий рівень. Управління здійснюється безпосередньо операторами критичної інфраструктури.

Аналізуючи суб'єктний склад відповідальний за формування та реалізацію державної політики у сфері захисту критичної інфраструктури, ідентифікуємо наступні відповідальні органи (Закон України «Про критичну інфраструктуру» №1882-IX):

1. Кабінет Міністрів України – відповідає за провадження державної політики у сфері захисту критичної інфраструктури України, організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи захисту критичної інфраструктури, визначає уповноважений орган з питань захисту критичної інфраструктури України, затверджує Регламент обміну інформацією, спрямовує, координує та контролює діяльність уповноваженого органу у сфері захисту критичної інфраструктури, затверджує Положення про Уповноважений орган у сфері захисту критичної інфраструктури.

2. Функціональні органи у сфері захисту критичної інфраструктури – відповідають за функціонування окремих державних систем захисту та реагування. Беруть участь у реагуванні на кризові ситуації, пов'язані із забезпеченням безпеки та стійкості критичної інфраструктури, готують пропозиції щодо включення об'єктів інфраструктури до Реєстру, формують перелік об'єктів критичної інфраструктури, що належать до сфери їх управління, надають власникам та операторам інфраструктури консультації щодо ризиків і загроз критичній інфраструктурі та заходів щодо їх нейтралізації, організовують проведення оцінки загроз та ризиків критичній інфраструктурі у відповідних сферах, беруть участь у проведенні оцінки загроз та ризиків критичній інфраструктурі на загальнодержавному рівні, формують пропозиції щодо національних та секторальних проектних ризиків і загроз, забезпечують організацію взаємодії та обміну інформацією з іншими суб'єктами національної системи захисту критичної інфраструктури, здійснюють моніторинг рівня безпеки об'єктів критичної інфраструктури у відповідних сферах.

3. Секторальні органи у сфері захисту критичної інфраструктури – відповідальні за формування та реалізацію державної політики у ввірених їм секторах критичної інфраструктури. Відповідають за створеня у межах штатної чисельності у своєму складі структурних підрозділів з питань захисту критичної інфраструктури, збирають, узагальнюють та здійснюють попередній аналіз даних щодо критичної інфраструктури та її функціонування, спільно з операторами критичної інфраструктури здійснюють категоризацію об'єктів критичної інфраструктури своїх секторів, формують секторальні переліки об'єктів та подають інформацію до Реєстру, розробляють та затверджують: вимоги до захисту критичних об'єктів відповідно до категорій, проектні загрози критичній інфраструктурі секторального рівня; плани взаємодії функціональних органів, плани взаємодії та підтримання життєво важливих функцій у випадку порушення функціонування об'єктів критичної інфраструктури; розробляють та впроваджують норми і регламенти захисту критичної інфраструктури у відповідних секторах критичної інфраструктури; затверджують проектні загрози критичній інфраструктурі об'єктового рівня у відповідних секторах; погоджують паспорти безпеки об'єктів критичної інфраструктури, надані операторами у відповідних секторах; здійснюють перевірку та оцінку захищеності об'єктів критичної інфраструктури; займаються підготовкою пропозицій до проектних ризиків та загроз критичній інфраструктурі національного рівня та щорічної оцінки ризиків і загроз критичній інфраструктурі національного рівня; організовують систему підготовки персоналу, навчання та тренувань щодо забезпечення стійкості та захисту секторів критичної інфраструктури, готують щорічний звіт щодо забезпечення захисту критичної інфраструктури у відповідному секторі, беруть участь у реагуванні на кризові ситуації, пов'язані з безпекою, захистом та стійкістю об'єктів критичної інфраструктури, а також у створенні умов для належного виконання правоохоронними, розвідувальними та контррозвідувальними органами своїх завдань щодо захисту критичної інфраструктури; попереджають про загрози операторів критичної інфраструктури та надають інформаційну, консультативну, експертну, методичну допомогу операторам критичної інфраструктури, користувачам їх послуг (населенню) задля попередження, реагування, мінімізації можливого впливу загроз; надають операторам об'єктів критичної інфраструктури рекомендації з питань захисту критичної інфраструктури та обов'язкові до виконання вимоги щодо усунення причин і умов, які порушують стійкість критичної інфраструктури; виконують збір, аналіз та узагальнення даних щодо об'єктів критичної інфраструктури та загроз їх функціонуванню; здійснюють заходи із функціонування відповідних систем обміну інформацією, моніторингу рівня безпеки об'єктів критичної інфраструктури; організовують функціонування системи обміну інформацією та взаємодії у відповідних секторах критичної інфраструктури між суб'єктами національної системи захисту критичної інфраструктури; готують пропозиції до стратегічних документів щодо забезпечення стійкості та захисту критичної інфраструктури, щороку подають інформацію уповноваженому органу у сфері захисту критичної інфраструктури України.

4. Уповноважений орган у сфері захисту критичної інфраструктури України – відповідає за формування і реалізацію державної політики у сфері захисту критичної інфраструктури, координацію діяльності суб'єктів національної системи захисту критичної інфраструктури, узагальнює пропозиції суб'єктів національної системи захисту критичної інфраструктури, формує та веде Реєстр об'єктів критичної інфраструктури, організовує здійснення оцінки захищеності об'єктів критичної інфраструктури та оцінює загальний стан їх захищеності, проводить оцінку загроз критичній інфраструктурі на національному рівні та оцінку загроз національній безпеці внаслідок реалізації загроз критичній інфраструктурі із залученням секторальних та функціональних органів, готує щорічну оцінку ризиків і загроз критичній інфраструктурі національного рівня та погоджує проектні ризики й загрози секторального рівня, готує рекомендації щодо визначення вимог до забезпечення захисту та стійкості секторів критичної інфраструктури, готує рекомендації щодо визначення вимог до забезпечення захисту та стійкості секторів критичної інфраструктури, надає пропозиції Кабінету Міністрів України щодо розробки Національного плану захисту та забезпечення стійкості критичної інфраструктури, порядку розроблення, форми та змісту паспорта безпеки та порядку розроблення, форми та змісту планів заходів щодо захисту критичної інфраструктури національного рівня, розробляє та затверджує Проектні загрози критичній інфраструктурі національного рівня, що становлять інформацію з обмеженим доступом, готує висновки та рекомендації власнику/оператору критичної інфраструктури щодо зміни права власності, цільового призначення чи режиму функціонування об'єкта критичної інфраструктури, забезпечує функціонування системи обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури, створює бази даних щодо загроз і вразливостей критичній інфраструктурі, забезпечує координацію секторальних органів, підготовку пропозицій до проектів стратегічних документів щодо забезпечення безпеки та стійкості, здійснення захисту критичної інфраструктури (Стратегії національної безпеки України, Стратегії кібербезпеки України та Стратегії громадської безпеки та цивільного захисту України), бере участь у розробленні нової галузі знань, програм навчання, підвищення кваліфікації, робочих і навчальних програм з питань забезпечення стійкості та захисту критичної інфраструктури, здійснює міжнародне співробітництво, забезпечує дотримання і виконання зобов'язань, взятих відповідно до міжнародних договорів України з питань захисту критичної інфраструктури, налагоджує і підтримує зв'язки з міжнародними організаціями, іноземними державами, їх правоохоронними органами і спеціальними службами.

Загальний склад суб'єктів національної системи захисту критичної інфраструктури окрім зазначених вище інститутів включає також: Апарат Ради національної безпеки і оборони України, Центральну виборчу комісію, Національний банк України, Національну комісію з цінних паперів та фондового ринку, Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації, Національну комісію, що здійснює державне регулювання у сферах енергетики та комунальних послуг, Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, Фонд державного майна України, інші центральні органи виконавчої влади із спеціальним статусом, центральні органи виконавчої влади, які забезпечують формування та реалізацію державну політику у сфері цивільного захисту, секторальні та функціональні органи, інші міністерства та центральні органи виконавчої влади, Службу безпеки України, правоохоронні та розвідувальні органи, суб'єкти оперативно-розшукової та контррозвідувальної діяльності, Збройні Сили України, інші військові формування, утворені відповідно до законів України, місцеві органи виконавчої влади (військово-цивільні адміністрації), органи місцевого самоврядування, підприємства, установи та організації незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки та стійкості критичної інфраструктури.

Перелік суб'єктів державної політики у сфері безпеки критичної інфраструктури не обмежується державними інститутами, а включає в себе органи місцевого самоврядування, суб'єктів господарювання, об'єднання громадян, окремих осіб, які надають послуги, пов'язані з національними інформаційними ресурсами. У такий спосіб розглянутий Закон містить найбільш вичерпний і систематизований перелік суб'єктів. Слушною вважаємо пропозицію Зубка Г. Ю. щодо вдосконалення нормативно-правової бази у досліджуваній сфері, зокрема у напрямку визначення, фіксації та чіткої узгодженості у нормативних актах переліку повноважень і завдань кожного суб'єкта, а також затвердження відповідних положень (Зубко, 2020: 170). Без цього реалізація державної політики у сфері захисту критичної інфраструктури залишиться безсистемною і фрагментарною.

Віднесення об'єктів до критичної інфраструктури здійснюється в порядку, встановленому Кабінетом Міністрів України згідно з положеннями Постанови № 1109 (Постанова Кабінету Міністрів України № 1109). Віднесення об'єктів до критичної інфраструктури здійснюється **за сукупністю критеріїв,** що визначають їх соціальну, політичну, економічну, екологічну значущість для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку, зокрема для реалізації життєво важливих функцій та надання життєво важливих послуг, свідчать про існування загроз для них, можливість виникнення кризових ситуацій через несанкціоноване втручання в їх функціонування, припинення функціонування, людський фактор чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму. Рівень критичності визначається як відносна міра важливості об'єктів критичної інфраструктури, якою враховується вплив раптового припинення функціонування або функціонального збою на безпеку постачання, забезпечення суспільства важливими товарами і послугами (Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України № 23).

Закон України «Про критичну інфраструктуру» передбачає, що в Україні має бути створений реєстр об'єктів критичної інфраструктури, тобто автоматизована система, що містить перелік найбільш важливої для життєдіяльності суспільства та держави критичної інфраструктури (Закон України «Про критичну інфраструктуру» №1882). Норми вищевказаного Закону та Постанови передбачають, що Реєстр формується та ведеться уповноваженим органом у сфері захисту критичної інфраструктури України на основі пропозицій суб'єктів національної системи захисту критичної інфраструктури.

Після включення об'єкта до Реєстру секторальні органи у сфері захисту критичної інфраструктури повідомляють про це оператора об'єкта критичної інфраструктури для забезпечення паспортизації та захисту об'єкта критичної інфраструктури відповідно до вимог цього Закону.

Інформація про об'єкти критичної інфраструктури, що міститься в Реєстрі, є відкритою, загальнодоступною та безоплатною, крім інформації з обмеженим доступом. Варто зауважити, що війна внесла певні корективи. Частина інформації щодо критичної інфраструктури стала закритою. Так, зокрема, НКРЕКП внесла зміни до своєї постанови від 26.03.2022 № 349 «Щодо захисту інформації, яка в умовах воєнного стану може бути віднесена до інформації з обмеженим доступом, у тому числі щодо об'єктів критичної інфраструктури» (Постанова НКРЕКП «Щодо захисту інформації, яка в умовах воєнного стану може бути віднесена до інформації з обмеженим доступом, у тому числі щодо об'єктів критичної інфраструктури» №349). Вказаною постановою визначено, що під час дії воєнного стану в Україні та до останнього дня місяця, наступного за місяцем припинення або скасування воєнного стану, на вебсайтах ліцензіатів повинен бути закритий доступ. Частково була закрита й інформація з боку інших секторів (закладів освіти і охорони здоров'я, кадастру, системи життєзабезпечення та захисту населення). Така ситуація зрозуміла і повністю відповідає особливостям регулювання у воєнний час.

Постанова № 1109 визначає перелік секторів (підсекторів), основних послуг критичної інфраструктури, останнім до цього списку було внесено агропромисловий комплекс, як основу продовольчого забезпечення держави. Станом на кінець 2022 р. в Україні налічується 25 секторів критичної інфраструктури: Паливно-енергетичний сектор, Цифрові технології, Захист інформації, Системи життєзабезпечення, Харчова промисловість та агропромисловий комплекс, Державний матеріальний резерв, Охорона здоров'я, Ринки капіталу та організовані товарні ринки, Фінансовий сектор (відповідає Мінфін), Фінансовий сектор (відповідає НБУ), Транспорт і пошта, Промисловість (хімічна, металургійна, оборонна, космічна, авіаційна, суднобудівна), Сектор громадської безпеки, Цивільний захист населення і територій, Міграція (імміграція та еміграція), Охорона навколишнього природного середовища, Сектор оборони, Національна безпека, Правосуддя, Тримання під вартою, Наукові дослідження та розробки, Вибори та референдуми, Соціальний захист, Інформаційні послуги, Державна влада та місцеве самоврядування (Постанова Кабінету Міністрів України № 1109).

Набір зазначених ключових блоків державної політики детермінує наявність системного підходу із кризового реагування. На національному рівні ініційовано створення державної системи захисту критичної інфраструктури (ДСЗКІ) – сукупності об'єктів, які є стратегічно важливими для економіки і безпеки держави, суспільства, населення та порушення функціонування яких може завдати шкоди життєво важливим національним інтересам України (Розпорядження Кабінету Міністрів України «Про схвалення Концепції створення державної системи захисту критичної інфраструктури» № 1009-р). До даної системи учені Бурбела Т. М. та Кондратов С. І. (Бурбела, Кондратов, 2020:15) відносять наявність наступних складових:

– нормативно-правових актів щодо забезпечення готовності до кризового реагування на глобальні загрози;

– національного плану реагування на кризові ситуації, викликані глобальними кризами або масштабними загрозами комплексного характеру;

– урядового органу, відповідального за координацію дій усіх залучених сторін при реагувані на глобальні загрози або комплексні загрози національного рівня;

– національної мережі ситуаційних та інформаційно-аналітичних центрів для підтримки процесу прийняття рішень у сфері безпеки;

– національного плану підготовки персоналу та населення для реагування на кризові ситуації;

– державної системи захисту критичної інфраструкури від усіх видів фізичних загроз;

– розвинуте державно-приватне партнерство у сфері захисту критичної інфраструктури та його повноцінне нормативно-правове забезпечення.

Даний перелік вважаємо за необхідне доповнити:

– державною структурою, відповідальною за інформування та обробку інформації про інциденти (кризи), пов'язані з критичною інфраструктурою та державною програмою міжвідомчого співробітництва у сфері захисту та стійкості критичної інфраструктури.

Звернемо увагу, що у питаннях захисту об'єктів критичної інфраструктури розвинених країн прослідковується актуалізація предикату стійкості критичної інфраструктури. Це її здатність бути готовою та адаптуватися до умов, що змінюються, а також протистояти змінам і швидко відновлюватися після порушень функціонування. При цьому, питанням забезпечення стійкості приділяється дедалі більше уваги у порівнянні з питаннями захисту. Таке зміщення акценту проблематики обумовлене тим, що в умовах війни, жодна створена система захисту не може у повній мірі забезпечити захист від усіх загроз і небезпек, що є особливо актуальним у сучасних умовах в Україні (Кондратов, Суходоля: 2020:18).

Нагадаємо, що функції уповноваженого органу у сфері захисту критичної інфраструктури України покладено на Державну службу спеціального зв'язку та захисту інформації України (Держспецзв'язку). Це вчергове підтверджує обширність суб'єктного складу та навність нескоординованих режимів функціонування, планів і процедур реагування на різні набори загроз і ризиків у сфері захисту критичної інфраструктури. До того ж визначені у положеннях і планах механізми і процедури взаємодії між зазначеним уповноваженим органом у сфері захисту критичної інфраструктури та існуючими національними системами безпеки і кризового реагування є недостатньо відпрацьованими та апробованими для випадків масштабних кризових ситуацій, оскільки в країні до цього часу практика міжвідомчих навчань і тренувань на рівнях, вищих ніж об'єктовий, була розвинута слабко. У напрямку вирішення даної проблеми варто розглянути ідею формування державної системи захисту критичної інфраструктури, схвалену Концепцією створення державної системи захисту критичної інфраструктури (Розпорядження Кабінету Міністрів України «Про схвалення Концепції створення державної системи захисту критичної інфраструктури» №1009-р). Згадана вище Концепція передбачає захист від комплексних загроз, тому вважаємо доцільним посилити увагу до превентивних заходів забезпечення стійкості критичної інфраструктури та доповнити ними розширену державну систему безпеки та стійкості критичної інфраструктури (ДСБСКІ). Тобто організаційно-правова структура ДСБСКІ матиме на меті протидію усім видам загроз та ризиків і стане вагомим елементом сучасної національної системи кризового реагування, а також виконувати координаційну роль.

Виявлені інституційні прогалини у координації діяльності суб'єктів безпеки критичної інфраструктури, детермінують ініціювання відповідних управлінських рішень у подальній реалізації державної політики. Аналізуючи закордонний досвід у даному напрямку, звернемо увагу на Агенство з кібербезеки та стійкості критичної інфраструктури (CISA) у США, яке діє у якості уповноваженого органу у сфері захисту критичної інфраструктури (The Cybersecurity and Infrastructure Security Agency, 2022). У його складі функціонує Міжвідомчий комітет безпеки, який співпрацює з компаніями, громадами та державними партнерами на всіх рівнях, щоб забезпечити навчання та інші інструменти та ресурси, пов'язані з безпекою критичної інфраструктури. Зусилля зосереджені на підвищенні обізнаності серед широкої спільноти про необхідність безпеки та стійкості критичної інфраструктури та активізації їхніх поточних зусиль. CISA відіграє життєво важливу роль у обміні інформацією з партнерами як з державного, так і з приватного секторів, що має важливе значення для безпеки та стійкості нації. Урядовий і приватний сектори створили партнерські відносини в структурі галузевої координаційної ради, щоб виконати спільну відповідальність щодо запобігання та зменшення ризиків збоїв у роботі критичної інфраструктури. CISA також проводить навчання з низки тем, пов'язаних із безпекою критичної інфраструктури. Експерти з предметних питань проводять навчання за допомогою різноманітних засобів, включаючи незалежні навчальні курси, віртуальне навчання під керівництвом інструктора та особисте навчання в аудиторії.

Вдалим у плані реалізації державної політики у сфері захисту критичної інфраструктури вважаємо також досвід Німеччини, де безпека об'єктів критичної інфраструктури є спільним завданням, яке виконують уряд, приватні компанії та оператори, а також громадянське суспільство. Керівними принципами державної політики захисту критичної інфраструктури можемо виділити довірливу співпрацю держави з бізнесом і промисловістю на всіх рівнях та вимоги, придатність і пропорційність вжитих заходів і використання ресурсів для підвищення рівня захисту (National Strategy for Critical Infrastructure Protection in Germany, 2009:23). Щоб спільні дії були успішними, необхідні стратегічні вказівки, які описують основну філософію, дії та практику в усіх важливих питаннях політики безпеки щодо захисту критичної інфраструктури з посиланням на всі відповідні ризики. На цій основі можна буде розробити підцілі, які, у свою чергу, будуть конкретизовані в програмах, планах чи концепціях та реалізовуватимуться в них. Зусилля держави у цій сфері мають бути спрямовані на забезпечення та підвищення рівня захисту за допомогою відповідних заходів, склад яких можемо узагальнити у відповідний квадро-комплекс (рис. 1).

Ключові позиції, на яких варто акцентувати увагу у забезпеченні стійкості критичної інфраструктури це:

– превентивні заходи – виявлення заздалегідь існуючих та очікуваних ризиків та здійснення профілактичних дій, що дозволить уникнути серйозних збоїв у роботі важливих інфраструктурних;

– імплементація – реалізація комплексу рішень ефективного управління в надзвичайних ситуаціях і кризових ситуаціях у результаті чого наслідки серйозних збоїв будуть максимально зведені до мінімуму.

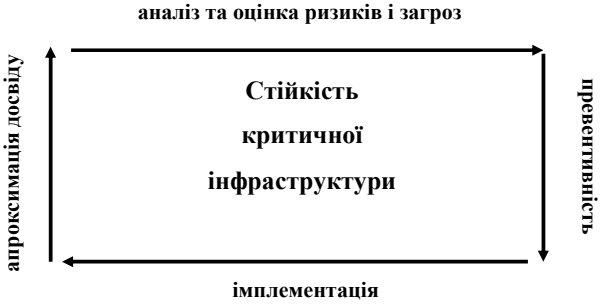

Рис. 1. Квадро-комплекс забезпечення стійкості критичної інфраструктури

– апроксимація досвіду – «засвоєння уроків» щодо посилення захисту об'єктів критичної інфраструктури на базі отриманого досвіду та постійного аналізу загроз та ризиків технологічних та інших інцидентів, які сталися в країні або за її межами. Ці висновки повинні бути переведені в стандарти захисту, які повинні бути розроблені та затверджені спільно з відповідними операторами та міжнародними партнерами.

Послідовна реалізація зазначеного комплексу у формі циклу управління загрозами та ризиками для критичної інфраструктури запропонує необхідну гарантію послідовної захисної системи тривалої ефективності, яка підвищить компетенцію в галузі безпеки об'єктів критичної інфраструктури.

Висновки. За результатами проведених досліджень варто зазначити що існує ряд проблем у сфері захисту критичної інфраструктури. Варто наголосити, що наявна інституційна структура безпеки критичної інфраструктури в її теперішньому вигляді не може бути надійною основою для розробки і реалізації планів і процедур координації дій, взаємодії та обміну інформацією між існуючими в Україні системами захисту, безпеки та кризового реагування. Це спричинено насмперед обширністю суб'єктного складу та навністю нескоординованих режимів функціонування, планів і процедур реагування на різні набори загроз і ризиків у сфері захисту критичної інфраструктури в Україні. Доцільно запропонувати удосконалення державної політики у напрямах: превентивність заходів із попередження ризиків та загроз об'єктам критичної інфраструктури та мінімізація їх наслідків, налагодження партнерства між урядом та операторами інфраструктури на принципах співробітництва, довіри та розділеної відповідальності, розвиток державно-приватного партнерства у сфері забезпечення безпеки критичної інфраструктури і запобігання виникненню надзвичайних ситуацій, розвиток міжнародного співробітництва у сфері захисту критичної інфраструктури.

Список використаних джерел:

1. Бурбела Т.М., Кондратов С.І. Деякі проблеми реагування на поширення COVID-19 у контексті забезпечення безпеки та стійкості критичної інфраструктури. URL: https://niss.gov.ua/sites/default/files/2020-04/krytychna-infrastructura-pry-covid-19-1.pdf
2. Закон України «Про критичну інфраструктуру» від 16.11.2021 р., №1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20/ed20211116#Text
3. Зубко Г.Ю. Система суб'єктів реалізації державної інфраструктурної політики України. Правові новели. 2020. № 11. С. 166–178.
4. Кондратов С. І. Проблеми забезпечення взаємодії при реагуванні на інциденти та кризи комплексного характеру на об`єктах критичної інфраструктури. Аналітична записка URL: https://niss.gov.ua/sites/default/files/2018-09/Kondratov-81403.pdf
5. Кондратов С.І., Суходоля О.М. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки: аналіт. доп. / за ред. Суходолі. Київ : НІСД, 2020. 28 с.
6. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури» від 15.01.2021 № 23. URL: https://zakon.rada.gov.ua/rada/show/v0023519-21#Text
7. Офіційний веб-сайт Національного інституту стратегічних досліджень (НІСД). URL: https://niss.gov.ua/
8. Петрашко І. Р. Аналіз регуляторного впливу проекту Закону України «Про критичну інфраструктуру та її захист». URL: https://www.drs.gov.ua/wp-content/uploads/2020/07/5854-ob.pdf
9. Постанова КМУ «Деякі питання об'єктів критичної інфраструктури» від 9 жовтня 2020 р. № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020п#Text
10. Постанова НКРЕКП «Щодо захисту інформації, яка в умовах воєнного стану може бути віднесена до інформації з обмеженим доступом, у тому числі щодо об'єктів критичної інфраструктури» від 20.04.2022 № 384. URL: https://www.nerc.gov.ua/
11. Розпорядження КМУ «Про схвалення Концепції створення державної системи захисту критичної інфраструктури» від 06.12.2017 р. № 1009-р. URL: https://zakon.rada.gov.ua/laws/show/1009-2017п#Text
12. National Strategy for Critical Infrastructure Protection in Germany. URL: http://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?blob=publicationFile&v=1
13. The Cybersecurity and Infrastructure Security Agency. URL: https://www.cisa.gov

References:

1. Burbela T. M., Kondratov S. I. (2020), Deiaki problemy reahuvannia na poshyrennia COVID-19 u konteksti zabezpechennia bezpeky ta stiikosti krytychnoi infrastruktury [Some problems of responding to the spread of COVID-19 in the context of ensuring the safety and stability of critical infrastructure], URL: https://niss.gov.ua/sites/default/files/2020-04/krytychna-infrastructura-pry-covid-19-1.pdf [in Ukrainian].
2. VRU, Law of Ukraine (2021), Pro krytychnu infrastrukturu [Law of Ukraine «About critical infrastructure»], URL: https://zakon.rada.gov.ua/laws/show/1882 [in Ukrainian].
3. Zubko G.Yu.(2020), Systema subiektiv realizatsii derzhavnoi infrastrukturnoi polityky Ukrainy [System of entities implementing the state infrastructure policy of Ukraine], Pravovi novely, [Legal novels], vol. 11. pp. 166–178. [in Ukrainian].
4. Kondratov S. I. (2018), Problemy zabezpechennia vzaiemodii pry reahuvanni na intsydenty ta kryzy kompleksnoho kharakteru na ob`iektakh krytychnoi infrastruktury [Problems of ensuring cooperation in responding to incidents and crises of a complex nature at critical infrastructure facilities]: analytical note, URL: https://niss.gov.ua/sites/default/files/2018-09/Kondratov-81403.pdf [in Ukrainian].

5. Kondratov S. I., Sukhodolya O. M. (2020), Derzhavna systema zakhystu krytychnoi infrastruktury v systemi zabezpechennia natsionalnoi bezpeky [State system of critical infrastructure protection in the national security system]: analytical note, Kyiv: NISD,. 28 p. [in Ukrainian].
6. ASSSCIPU (2021), Pro zatverdzhennia Metodychnykh rekomendatsii shchodo katehoryzatsii obiektiv krytychnoi infrastruktury [On Approval of Methodological Recommendations for Categorization of Critical Infrastructure Objects], The order of the Administration of the State Service for Special Communications and Information Protection of Ukraine, dated 15.01.2021. № 23, URL: https://zakon.rada.gov.ua/rada/show/v0023519-21#Text [in Ukrainian].
7. Ofitsiinyi veb-sait National Institute for Strategic Studies (NISD). URL: https://niss.gov.ua/ [in Ukrainian].
8. Petrashko I. R. (2020), Analiz rehuliatornoho vplyvu proektu Zakonu Ukrainy «Pro krytychnu infrastrukturu ta yii zakhyst [Analysis of the regulatory impact of the draft Law of Ukraine "On critical infrastructure and its protection"], URL: https://www.drs.gov.ua/wp-content/uploads/2020/07/5854-ob.pdf. [in Ukrainian].
9. KMU (2020), *Deiaki pytannia obiektiv krytychnoi infrastruktury* [Some critical infrastructure issues], The order of the Cabinet of Ministers of Ukraine, dated 09.10.2020. № 1109, URL: https://zakon.rada.gov.ua/laws/show/1109-2020 [in Ukrainian].
10. NCRECP (2022), Shchodo zakhystu informatsii, yaka v umovakh voiennoho stanu mozhe buty vidnesena do informatsii z obmezhenym dostupom, u tomu chysli shchodo obiektiv krytychnoi infrastruktury [Regarding the protection of information that in the conditions of martial law may be classified as information with limited access, including regarding critical infrastructure objects], The order of the National Commission, which carries out state regulation in the spheres of energy and communal services, dated 20.04.2022 № 384. URL: https://www.nerc.gov.ua/. [in Ukrainian].
11. KMU (2020), Pro skhvalennia Kontseptsii stvorennia derzhavnoi systemy zakhystu krytychnoi infrastruktury [On the approval of the Concept of creating a state system for the protection of critical infrastructure], Decree of the Cabinet of Ministers of Ukraine, dated 06.12.2017. № 1009-p., URL: https://zakon.rada.gov.ua/laws/show/1009-2017п#Text [in Ukrainian].
12. National Strategy for Critical Infrastructure Protection in Germany. URL: http://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?blob=publicationFile&v=1 [in English].
13. The Cybersecurity and Infrastructure Security Agency. URL: https://www.cisa.gov [in English].