УДК 351.86:338.49](477)

Олег Мельничук
аспірант кафедри глобалістики, євроінтеграції
та управління національною безпекою
НАДУ при Президентові України
ORCID iD https://orcid.org/0000-0003-3615-3730

АКТУАЛЬНІ ПИТАННЯ ПУБЛІЧНОЇ ПОЛІТИКИ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: СТАН ТА ПЕРСПЕКТИВИ ЇЇ ВПРОВАДЖЕННЯ В УКРАЇНІ

У статті проведено науково-аналітичний аналіз досліджень з публічної політики та офіційних документів розвинених країн світу щодо застосування поняття «стійкість» та «безпека критичної інфраструктури». Зосереджено увагу на переході від концепції захисту до стійкості в контексті розвитку безпеки та більш стійкого суспільства. Сформовано визначення таких термінів як «безпека критичної інфраструктури» та «стійкість критичної інфраструктури» та запропоновано розмежування області стійкості на три сфери стійкості критичної інфраструктури (КІ): суспільну, організаційну та технологічну.

Розглянуто основні завдання публічної політики щодо безпеки, захисту та забезпечення стійкого розвитку КІ держави та визначено мету і завдання публічної політики з питань захисту об'єктів КІ із розмежуванням загроз для КІ, що можуть бути застосовані в Україні. Крім того, виокремлено пріоритетні напрями забезпечення стійкості КІ, зокрема, створення установи, яка має виконувати завдання з формування та реалізації стратегічних рішень щодо стійкості системи КІ країни. Також, обґрунтовано доцільність впровадження нового підходу зі створенням безпекового партнерства між всіма зацікавленими сторонами на базі державно – приватного партнерства між бізнесом та урядом.

***Ключові слова*:** стійкість; стійкість критичної інфраструктури; організаційна стійкість; захист та безпека критичної інфраструктури; загрози критичної інфраструктури.

Oleg Melnychuk
PhD student of the Global Studies, European Integration
and State Security Management Chair of the NAPA under the President of Ukraine
ORCID iD https://orcid.org/0000–0003–3615–3730

ACTUAL PROBLEMS OF CRITICAL INFRASTRUCTURE RESILIENCE PUBLIC POLICY: CONDITION AND IMPLEMENTATION PROSPECTS FOR UKRAINE

The carry through scientific and analytical analysis of public policy researches and world developed countries official documents of the application on the concept of «resilience» and «safety of critical infrastructure». The focus is on the transition from the concept of protection to resilience in the context of developing safety and a more resilient society. Definitions of such terms as «safety of critical infrastructure» and «critical infrastructure resilience» is formulated in this article and the delimitation the sphere of resilience into three resilience areas of critical infrastructure (CI): social, organizational and technological.

The main tasks of the public policy on safety, protection and providing resilience development of the national CI are considered. The purpose and objectives of the public policy on the protection of the CI objects with the demarcation of the threats that can applied in Ukraine are determined. Besides, the priority tendency for providing CI resilience, in particular, the establishing of an institution that must forming and implementing strategic decisions on the country's CI system resilience, has been isolated. In addition, the advisability of introducing a new approach about the

organistion of a safe partnership between all stakeholders, which based on a public - private partnership between business and government, founded.

***Key words*:** resilience; resilience of critical infrastructure; organizational resilience; protection and safety of critical infrastructure; threats for critical infrastructure.

Постановка проблеми. Глобальне суспільство швидко змінюється та потребує постійного надання послуг для обслуговування своєї життєдіяльності. Національна безпека та процвітання, економіка, бізнес та громада залежать від технологій та інфраструктурних систем, які стають все більш складними та взаємопов'язаними між собою. Організації, громади та особи повинні бати обізнаними та готовими реагувати на непередбачені або несподівані ризики та події. Це пов'язано з тим, що інфраструктурі у всьому світі постійно загрожує значна кількість співзалежних антропогенних небезпек і природних явищ, які можуть привести до збою роботи життєво важливих її об'єктів.

Сучасною відповіддю новим викликам є державна система захисту, яка будується виходячи з необхідності реагування на комплекс загроз, для забезпечення стійкості суспільства, національної економіки та держави. Провідні країни світу зосереджують ресурси на захисті важливих інфраструктурних об'єктів та активно розбудовують системи із забезпечення захисту та стійкості КІ, впроваджують нормативні документи для регламентації діяльності учасників системи, готують відповідні кадри та налагоджують партнерські відносини з приватним сектором та громадою тощо.

Глобальна стратегія Європейського Союзу визнала стійкість демократичного розвитку пріоритетом та інструментом для безпечного руху вперед, попри загрози, наголошуючи що стійка держава це безпечна держава, а безпека є ключовою для процвітання та демократії. Європейська спільнота вважає нашу державу важливим партнером та допомагає Україні будувати стабільне демократичне майбутнє для своїх громадян, залишаючись непохитним прихильником незалежності, територіальної цілісності та суверенітету. Впровадження зміцнення економічних відносин, поглиблення політичних зв'язків та поваги до спільних цінностей, надихає українське суспільство продовжувати реалізацію програми реформ, що спрямована на економічне зростання і підвищення рівня життя та забезпечення стійкості суспільства. Враховуючи пов'язаність завдань публічної політики щодо безпеки та стійкості держави з безпекою та стійкість системи її КІ, необхідним є запровадження ефективних підходів до організації управління об'єктами системи КІ на державному і місцевому рівні та розробка відповідних наукових, методологічних, технологічних і інших інструментів.

Зазначені чинники характеризують актуальність наукового дослідження інструментів публічного управління системою КІ, та, у межах цього напряму, дослідження стану та можливості впровадження концепції стійкості КІ в Україні.

***Аналіз останніх досліджень і публікацій*.** Серед вітчизняних вчених, які розглядали питання стійкості, безпеки та управління захистом КІ можна віднести таких авторів: В. Абрамов, Д. Бірюков, Д. Бобро, В. Горбулін, С. Іванюта, О. Суходоля, В. Лядовська, С. Кондратов, І. Уряднікова та інші. Крім того, дослідженню проблемних питань стійкості та захисту КІ присвячені праці A. Bialas, M. Cavelty, C. Folke, P. Gattinesi, D. Gritzalis, Y. Haimes, T. Kelly, A. Lazari, J. Markucia, V. Mauer, C. Nan, C. Pursiainen, D. Rehaka, S. Rinaldi, G. Sansavini, I.Utneand, J.Vatn, A. Wenger та ін.

Разом з тим, кількість публікацій, де розглядається стійкість як система в контексті управління об'єктами КІ, у вітчизняній та закордонній літературі обмежена, тому дана тема дослідження є актуальною.

Мета статті – вивчення та аналіз наявних теоретичних засад та офіційних документів розвинених країн світу щодо застосування поняття «стійкість» та основних завдань публічної політики з питань захисту та стійкості КІ.

Виклад основного матеріалу. У будь-який історичний період існування держави та розвитку суспільства завжди існує певна множина досить різних за своєю пріоритетністю,

спрямованістю та можливістю реалізації нагальних потреб, які своєю чергою формують систему національних інтересів. Визначення цієї множини національних інтересів є ключовою передумовою політики держави щодо стабільного політичного та соціального та економічного розвитку. При цьому характерним є відносно стійкий, системний розвиток суспільства та всіх систем, які забезпечують його життєдіяльність. Зростання останнім часом кількості кібератак, негативних випадків природного та техногенного характеру, терористичних загроз, обумовлюють пріоритетність інтересів держави щодо захисту інфраструктури, життєво важливої для безпеки її громадян та суспільства. Питання вдосконалення публічної політики щодо стійкості та захисту КІ стає предметом постійного обговорення наукових установ державних та громадських організацій.

Тому є необхідність впровадження системи захисту об'єктів, діяльність яких підтримує послуги та функції, критично важливі для існування громадськості, суспільства та держави, шляхом розробки нормативних документів, а саме: концепції КІ, плану дій щодо захисту та стійкості КІ, та інших складових системи забезпечення національної безпеки.

Наразі в Україні питання застосування принципово нових методів та інструментів діяльності сектору безпеки також зумовлює прийняття Концепції розвитку сектору безпеки та оборони, проблеми забезпечення інформаційної безпеки, кібербезпеки та безпеки інформаційних ресурсів і КІ визначено пріоритетними до вирішення у сфері державної політики національної безпеки держави у Стратегії національної безпеки.Однак, в законодавстві України захист об'єктів, які згідно зі світовою практикою належать до сектору КІ, регламентується численними нормативно-правовими актами, що носять переважно відомчий характер [1].

Термін «критична інфраструктура» неодноразово використовувався в законодавстві нашої держави, проте, все ще не визначений документально. Перше посилання на КІ відбулося у 2005 році в Рекомендаціях парламентських слухань щодо розвитку інформаційного суспільства в Україні, де доручалося Службі безпеки України підготувати пропозиції щодо визначення та захисту критичних інформаційних інфраструктур.

Наступне посилання у 2007 році, в редакції 2012 року, в Стратегії національної безпеки України «Україна у світі, що змінюється», цей термін згадувався в контексті забезпечення інформаційної безпеки щодо забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами КІ, а також, зміцнення енергетичної безпеки щодо дієвого захисту КІ паливо- енергетичного комплексу від екологічного, техногенного впливів та зловмисних дій.

В чинній Стратегії національної безпеки України, що затверджена у 2015 році, вперше визначено загрози кібербезпеці, безпеці інформаційних ресурсів та безпеці КІ, пріоритети забезпечення кібербезпеки, безпеки інформаційних ресурсів та безпеки КІ, а також, спрямовано розвиток Національної гвардії України, як військового формування з правоохоронними функціями, на збільшення її спроможностей щодо забезпечення фізичного захисту об'єктів КІ.

Серед визначених пріоритетів забезпечення безпеки КІ, на нашу думку першочерговими є: комплексне вдосконалення правової основи захисту КІ, створення системи державного управління її безпекою; посилення охорони об'єктів КІ, зокрема енергетичної та транспортної; налагодження співробітництва між суб'єктами захисту КІ, розвиток державно – приватного партнерства у сфері запобігання надзвичайним ситуаціям та реагування на них.

Перш за все розкриємо підходи до розуміння співвідношення змісту понять «безпека», «захист», «стійкість», «критична інфраструктура», які використовуються науковцями та практиками у сфері національної безпеки та захисту КІ. В закордонний та

українській практиці використовується різний термінологічний опис у цій сфері, зазвичай спостерігається змістовна неузгодженість та відсутність відповідних термінів.

З огляду на відсутність визначення КІ в законодавстві нашої держави та те, що цей термін характеризується різними складовими, в залежності від національних потреб та проблем, які різняться залежно від регіону, рівня розвитку та інших специфічних чинників, пропонуємо застосування визначення цього терміну розробленого О. В. Мельничуком, посилаючись на досвід вітчизняних та закордонних фахівців з провідних країн світу. Критична інфраструктура: сукупність систем, або її елементів (об'єктів) та супровідних процесів, які в разі порушення, відмови або руйнування можуть істотно вплинути на національну безпеку та оборону, природне середовище, економіку, безпеку і здоров'я населення, або ефективне функціонування органів державної влади, місцевого самоврядування та громадських організацій [2].

Термін «критична інфраструктура» тісно пов'язаний з поняттям «захист критичної інфраструктури», оскільки саме поняття критична інфраструктура передбачає наслідки можливого її порушення, відмови або руйнування, а на їх запобігання чи зменшення і спрямовується захист КІ.

Зелена книга з питань захисту критичної інфраструктури в Україні визначає захист КІ як комплекс заходів, реалізований в нормативно – правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури [3].

Зазначене визначення на нашу думку, є неточним, тому що основне поняття в ньому містить посилання на інші пов'язані поняття, що по суті не розриває його змісту. Більш точне визначення поняття «захист КІ» надає О. М. Суходоля в матеріалах статті «Захист критичної інфраструктури: сучасні виклики та пріоритетні завдання сектору безпеки». А саме: всі види діяльності, спрямовані на забезпечення функціональності, безперервності та цілісності критичної інфраструктури з метою недопущення, пом'якшення та нейтралізації загроз, ризиків та вразливостей [4].

У розвинутих країнах світу забезпечення захисту КІ від усіх видів загроз реалізується через концепцію захисту КІ, яка прийнята в таких країнах, як Австралія, Велика Британія, Канада та інші. В більшості з них заходи захисту КІ передбачають попередню ідентифікацію об'єктів КІ, яка здійснюється спираючись на затверджені методи оцінки загроз та ризиків.

Водночас, неможливість забезпечення рівномірного високого рівня захисту для всіх об'єктів КІ від відомих видів загроз, обумовила спрямування захисту конкретних вибіркових об'єктів КІ від визначеного набору усіх прогнозованих загроз, віддаючи пріоритет тому або іншому сектору інфраструктури залежно від оцінки її критичності.

У Національній стратегії захисту критичної інфраструктури Німеччини зазначено, що вдосконалення захисту критичної інфраструктури є спільною відповідальністю Федерального уряду та урядів земель [5]. При цьому, на регіональному рівні можуть бути прийняті та виконуватися власні стратегії та програми захисту критичної інфраструктури.

Країни, що граничать з Україною, та яки входили до складу Організації Варшавського договору і Ради Економічної Взаємодопомоги, були тісно пов'язані з Радянським Союзом в політичному, військовому та економічному відношенні, однак після набуття незалежності стали членами Організації Північноатлантичного договору та членами Європейського Союзу (ЄС). Зокрема, Угорщина одна із перших п'яти колишніх комуністичних країн, що увійшла до складу членів Північноатлантичного альянсу та ЄС, рішенням уряду 2008 року ввела в дію Програму захисту національної критичної інфраструктури, згідно з якою визначено 11 секторів КІ цієї країни.

Подібна ситуація яка досі притаманна українській державі, спостерігається і у Румунії, де існує близько 15 переліків об'єктів, що відповідають терміну «критична інфраструктура», але вони зустрічаються в різних законодавчих актах.

У законодавстві Республіки Болгарія «критична інфраструктура» було визначено Законом «Про управління в умовах кризи», який діяв з березня 2005 року по травень 2009

року. Оновлене визначення терміну КІ було введено Постановою Ради Міністрів «Про порядок, спосіб та компетентні органи для визначення критичної інфраструктури та об'єктів і оцінки ризиків» в жовтні 2012 року.

Зазначимо, що після подій 11 вересня 2001 року безпека КІ в США була зосереджена в основному на захисті від загроз терористичного характеру. Однак, через неспроможність ефективно протистояти наслідкам інтенсивних та руйнівних ураганів Катріна і Ріта 2005 року, уряд США повернувся до стратегії захисту від кількох найбільш імовірних загроз, зокрема техногенних аварій та природних катастроф.

При дослідженні поняття захисту КІ простежується невід'ємний зв'язок з системою захисту національної безпеки, реалізація якого здійснюється шляхом виконання розробленої державної концепції, стратегії та відповідних планів дій. Таким чином, національні інтереси держави реалізуються через зазначені нормативно – правові документи, які мають бути спрямовані на застосування інноваційних методів та інструментів діяльності сектору безпеки.

Визначення поняття «національні інтереси» надає О. В. Мельничук в матеріалах статті «Критическая инфраструктура государства как составляющая национальной безопасности: понятийно-категориальный апарат», а саме: життєво важливі матеріальні, інтелектуальні і духовні цінності Українського народу як носія суверенітету і єдиного джерела влади в Україні, визначальні потреби суспільства і держави, реалізація яких гарантує державний суверенітет України та її прогресивний розвиток», тому можна стверджувати, що КІ включає ті матеріальні й віртуальні об'єкти, системи та супровідні процеси, від сталого функціонування яких залежать існування громадськості, суспільства та держави, а отже, національні інтереси держави [2].

Для протидії сучасним викликам, що дедалі більше впливають на глобальну та національну безпеку держави, необхідно подолати перешкоди для переходу на новий якісний рівень публічного управління державою, в основу якого покладені спільні зусилля людини, громадянина, суспільства, бізнесу і держави. В умовах глобалізації національна безпека, виробництво, економіка і фінанси кожної країни знаходяться у значній залежності від чинників, які визначають стан безпеки в інших країнах та у глобальному вимірі в цілому. Гарантоване надання життєво важливих послуг в умовах нових загроз національній безпеці в публічному суспільстві це не тільки відповідальність державних органів, але також і приватних компаній на національному та міжнародному рівні.

В цьому контексті і повинно бути визначено на законодавчому рівні мету та завдання публічної політики з питань захисту об'єктів критичної інфраструктури України, пропонуємо наступні з них:

мета публічної політики з питань захисту об'єктів КІ держави – забезпечення безперервності функціонування об'єктів КІ, з метою недопущення, пом'якшення та нейтралізації усього спектру наявних загроз і ризиків.

завдання публічної політики з питань захисту об'єктів КІ:

– прогнозування та запобігання кризових ситуацій на об'єктах КІ;

– створення єдиного центрального органу виконавчої влади, який спрямовує та координує діяльність щодо забезпечення захисту системи національної КІ;

– організація системи публічного управління об'єктами КІ, з визначенням компетенції та кола повноважень органів центральної виконавчої влади та місцевого самоврядування;

– запровадження функціонування системи виявлення, уникнення та ліквідації наслідків інцидентів на об'єктах КІ;

– розробка державних та місцевих цільових програм забезпечення захисту та стійкості об'єктів КІ;

– впровадження державно-приватного партнерства з питань захисту об'єктів КІ;

– формування системи управління ризиками, яка має стати основою для плану захисту об'єктів КІ, оцінки стану захищеності таких об'єктів;

– проведення періодичного аналізу результативності публічної політики з питань захисту об'єктів КІ.

Історично склалось, що національна безпека держави в нашій країні була об'єктом державного регулювання, тому на перехідному етапі запровадження публічної політики з питань захисту об'єктів КІ питання безпека таких об'єктів потребує окремого визначення на законодавчому рівні. На нашу думку, безпека КІ може бути визначена як стан систем, або їх елементів (об'єктів) та супровідних процесів критичної інфраструктури, при якому дія зовнішніх і внутрішніх факторів не призводить до фізичних, експлуатаційних, операційних відмов або пошкоджень їх функціонування.

Забезпечення безпеки та стійкості країни є тими основними напрямками, на які мають спрямувати свою діяльність органи влади, відповідно до Національного плану захисту критичної інфраструктури США. Зокрема, посилення захищеності національної КІ має здійснюватися шляхом: запобігання, стримування, нейтралізації або пом'якшення наслідків цілеспрямованих дій з боку терористів, спрямованих на знищення, виведення з ладу або зловмисне використання КІ, а також, посилення національної готовності, своєчасне реагування та швидке відновлення КІ в разі атаки, стихійного лиха або інших надзвичайних ситуацій. Зазначимо, що тлумачення змісту терміна «безпека», що дається в актах уряду та відповідних органів влади США, містить протистояння терористичним загрозам та природним лихам, а саме: узгоджене національне зусилля, яке гарантує, що країна захищена від нещасних випадків і стійка до терористичних атак та інших небезпек, а інтереси країни, прагнення та спосіб життя можуть процвітати [6].

Таким чином, існує певна пов'язаність завдань публічної політики щодо безпеки, захисту та забезпечення стійкого розвитку КІ держави.

Стійкість, як визначення, не було належним чином досліджено в літературі, хоча концепція «стійкості» розвивається дуже швидко. Наразі, ідея стійкості досить нечітка, а складові її визначення це все ще є предметом суперечки. Так, дослідники з різних наукових галузей економіки, екології, соціології, психології та інших, використовують термін стійкість, який широко вживається в офіційних та нормативних документах провідних країн світу, зокрема, Європейської Комісії.

Попри різні тлумачення терміну стійкості, основна тема терміна схожа. Так, стійкість системи – її здатність в найкоротші терміни відновитися до заздалегідь визначеного задовільного рівня продуктивності, після руйнівних подій чи небезпек, які відбулися [7].

C. Holling у своїй праці «Стійкість та стабільність екологічної системи» описав стійкість як міру витривалості системи та її здатність убирати зміни та порушення, при цьому підтримувати такі самі відносини між популяціями та їх варіаціями [8].

Поняття стійкості також використовують в системній інженерії. Так, Y. Haimes в статті «Про тлумачення стійкості в системах», визначає стійкість як здатність системи витримувати великі перебої в межах під ходячих параметрів деградації та відновитися протягом бажаного часу за прийнятні витрати [9].

При дослідженні оцінювання стійкості системи інженерної інфраструктури C. Nan, G. Sansavini та інші встановили, що стійкість – це здатність системи або так званої «системи систем» завдяки ефективним внутрішнім та зовнішнім зусиллям протистояти будь-якому стрімкому або повільному впливу руйнівних внутрішніх чи зовнішніх подій/сил, та здатність зменшити як величину, так і тривалість відхилення рівня продуктивності системи між початковим (або цільовим) та новим непохитним її станом [10].

Відповідно, обриви в роботі інфраструктури, які ввійшли до аналізу складу нелінійних соціально – екологічних систем, були досліджені C. Folke в науковій статті «Стійкість: поява перспективи для дослідження соціально – екологічних систем» та визначено стійкість як спосіб мислення, що представляє перспективну думку для керівництва та організацій, яка забезпечує цінний контекст для аналізу вразливості системи,

генерування науки про стійкість та міждисциплінарної співпраці з питань, що мають принципове значення для управління переходом до стійкого розвитку суспільства [11].

Зазначимо, що Університетом Флориди та Інститутом Байєра, де працював C. Holling, запроваджено дослідницьку програму «Resilience», яка згодом перетворилася у 1999 році на Альянс стійкості (Resilience Alliance). Наразі, це міжнародна багато дисциплінарна дослідницька організація, яка досліджує динаміку соціально – екологічних систем. Члени Альянсу стійкості співпрацюють у різних дисциплінах, щоб сприяти розумінню та практичному застосуванню стійкості, адаптаційного потенціалу та трансформації суспільств та екосистем з метою подолання змін та підтримки добробуту людини.

Альянс стійкості визначає «стійкість» як: здатність системи поглинати порушення, бути змінною, а потім переорганізуватися, і при цьому, зберігати ідентичність, тобто, мати ту саму основну структуру та способи функціонування. Вона містить здатність вчитися з урахуванням пошкоджень. Гнучка система поблажливо сприймає зовнішні удари. При зменшенні гнучкості, величина удару, від якого система не може відновитися, стає меншою. Стійкість зміщує увагу з приросту продуктивності на гнучкість системи та ефективність необхідного її відновлення [12].

Одночасно, поняття стійкість від англійського «Robustness» – це якість, що дозволяє системі витримувати зміни параметрів зовнішнього середовища, відмінні від розрахункових. Система організм, або проєкт може бути названо «стійким», якщо він в змозі впоратися з варіаціями (іноді непередбачуваними) в операційному середовищі з мінімальними: збитком, зміною або втратою функціональності [13].

Розглянувши варіації визначення поняття «стійкість» можна зауважити, що стійкість системи складається з двох основних вимірюваних частин:

I – статична стійкість, яка показує здатність системи повернутися до потрібного рівня функціональності після катастрофи, тобто різниця між початковим (або цільовим) та фактичним (після події) її станом;

II – динамічна стійкість, що показує, як швидко відбувається відновлення та кількість зусиль, ресурсів, необхідних для відбудови функціонування до заздалегідь визначеного бажаного рівня продуктивності системи.

Таким чином, під стійкістю КІ будемо розуміти здатність інфраструктури функціонувати у стандартному режимі та адаптуватися до умов, що постійно змінюються, в тому числі до технічних збоїв, аварій, зловмисних дій, небезпечних природних явищ та лих, а також, відновитися протягом мінімального часу за прийнятні витрати.

Зазначимо, що в розвинених країнах світу термін «стійкість» часто вживається в нормативних та офіційних документах, спрямованих на реалізацію завдань публічної політики щодо безпеки, захисту та забезпечення стійкого розвитку суспільства.

Перехід від концепції захисту до стійкості відбувався поступово, так, спершу була започаткована Європейська програма захисту КІ, при цьому, концепція стійкості не зазначалась в офіційних документах. Водночас, «Зелена книга про Європейську програму захисту КІ», визнає, що не всі інфраструктури можуть бути захищені від усіх загроз. Рішення щодо захисту КІ полягало в визначенні пріоритетних заходів захисту та зосередженні уваги на обраних об’єктах що охороняють [14]. Аналогічно, Директива Ради Європи від 08 грудня 2008 року № 144 характеризується тим самим підходом, тобто, відсутністю будь – яких посилань на стійкість [15].

Концепція стійкості була популяризована в науково-аналітичному аналізі та дослідженнях з публічної політики в середині 2000-х років, а попередньо, використовувалася екологами з початку 1970-х років. Згодом, термін «стійкість» увійшов в наукову сферу досліджень КІ, замінивши зосередженість на захисті [7-11].

Зміна уваги стала помітною на рівні органів публічної політики та уряду США, так, Директива президента США 2013 року визначає основні поняття та завдання політики щодо забезпечення безпеки та стійкості КІ:

Стійкість КІ – спроможність підготуватись та адаптуватися до змінних умов, а також протистояти загрозам порушень функціонування та швидко відновлюватися від порушень. Стійкість включає спроможність протистояти загрозам та відновлюватися від цілеспрямованих атак, аварій, природних загроз та інцидентів;

Забезпечення безпеки КІ – зменшення ризику критичної інфраструктури від втручання, атак або ефектів, спричинених природними катастрофами або людською діяльністю, шляхом реалізації заходів із фізичного захисту або кіберзахисту [16].

Очевидним є зміщення акцентів зі змісту діяльності органів державної влади США щодо безпеки на діяльність із недопущення пошкодження функціонування умовного об'єкта переважно внаслідок зловмисних дій, з фокусуванням на створенні додаткового захисту від загроз. Термін же «стійкість» зосереджується на підготовці до запобігання та реагування на загрози, адаптації до нових умов функціонування та відновлення стандартного режиму роботи. При цьому, стійкість у США розглядається як цінність, якість та бажана характеристика суспільства та держави.

Схожа тенденція спостерігається в офіційних документах Європейського Союзу, так, в Робочому документі штатної Європейської Комісії з питань перегляду Європейської програми захисту КІ у 2012 році концепція стійкості вже грає, хоч і невелику, але певну роль. Однак стійкість, як концепція що альтернативна захисту, не розглядалася Європейською Комісією до проведення тестування стійкості КІ, результати якого зазначені у Звіті Європейського Союзу 2014 року [17; 18].

А вже у липні 2016 року главами держав та урядів країн Організації Північноатлантичного договору на Варшавському саміті було визначено сім базових вимог до держав-членів Північноатлантичного альянсу щодо забезпечення національної стійкості, а саме щодо: енергозабезпечення; транспортної системи; систем комунікацій; водозабезпечення та постачання продовольства; безперервність урядування та надання найважливіших державних послуг; ефективного подолання неконтрольованого переміщення людей; надання допомоги потерпілим від стихійних лих, що отримали ушкодження.

Глобальна стратегія Європейського Союзу, прийнята в червні 2016 року «Спільне бачення, спільна дія: Сильніша Європа», визнала «стійкість демократичного розвитку» пріоритетом та інструментом забезпечення спроможності ЄС орієнтуватись та рухатися вперед, створюючи зовнішній авторитет та вплив ЄС, нівелюючи загрози. «Стійка держава – це безпечна держава, а безпека є ключовою для процвітання та демократії. Стійкість – це більш розширене поняття, яке охоплює всіх людей та все суспільство. Гнучке суспільство з демократією, довірою до інститутів та сталим розвитком лежить в основі стійкої держави» [19].

Виконуючи цілі сталого розвитку, ЄС визначив спільний підхід до своєї гуманітарної політики, розвитку, торгівлі, інвестицій, інфраструктури, освіти, охорони здоров'я та наукових досліджень. Згідно з зазначеною Стратегією, фонди розвитку ЄС повинні каталізувати стратегічні інвестиції через державно – приватне партнерство, сприяючи сталому зростанню, створенню робочих місць, а також навичок та передачі технологій. Соціальна стійкість буде зміцнюватися шляхом поглиблення відносин з громадянським суспільством, зокрема, в його зусиллях із залучення до відповідальності урядів. ЄС прагне посилити енергетичну та екологічну стійкість і розвивати суспільну стійкість шляхом поглиблення роботи з питань освіти, культури та молоді, співіснуванню і повазі.

Першочерговим завданням для спільноти ЄС є інтегрування максимальних зусиль для роботи над внутрішніми та зовнішніми аспектами європейської енергетичної безпеки. Відповідно до цілей Енергетичного союзу, ЄС прагне диверсифікувати свої джерела енергії, маршрути та постачальників, особливо в газовій галузі, зміцнювати відносини у всьому світі з надійними країнами, що виробляють енергію, а також надає підтримку створенню стійкої інфраструктури в державах союзу.

Поряд з цим ЄС підтримує швидке відновлення держав-членів у разі нападів шляхом посилених зусиль щодо безпеки постачання, захисту КІ та нівелювання наслідків кібервійни. Для цього ЄС зосереджує свою увагу на кібербезпеці, допомозі державам – членам захищатися від кіберзагроз, зберігаючи відкритий, вільний та безпечний кіберпростір. Це обумовлює посилення технологічних можливостей, спрямованих на пом'якшення загроз та стійкості КІ, мереж та служб щодо зменшення кіберзлочинності, шляхом сприяння розвитку інноваційних систем та інформаційно-комунікаційних технологій. Саме вони зможуть гарантувати доступність та цілісність даних, забезпечуючи при цьому безпеку в цифровому просторі, за допомогою відповідної політики щодо місця зберігання даних та сертифікації цифрових продуктів та послуг.

Погоджуючись з експертами ЄС, зазначимо, що європейська безпека залежить від спільної якісної оцінки внутрішніх і зовнішніх загроз та викликів. Для покращення моніторингу та контролю потоків, які мають наслідки для безпеки потрібні інвестиції в розвідку та спостереження, включаючи системи пілотування літальних апаратів, супутниковий зв'язок. Щодо протидії тероризму, доцільно унормувати законодавство щодо вибухових речовин та вогнепальної зброї. Важливим також є інвестування в цифрові можливості для захисту даних, мереж та КІ в цифровому просторі. Для підвищення стійкості суспільства необхідно розвивати можливості в надійних цифрових послугах та в кібертехнологіях.

Загальне розуміння поняття «стійкість», надано в Міжнародній стратегії Об'єднаних Націй, а саме: здатність системи, громади чи суспільства піддаватися небезпекам та протистояти, поглинати втручання та своєчасно, ефективно відновлюватися від наслідків небезпеки, у тому числі шляхом збереження та відновлення основних структур та функцій (UNISDR) [20].

У зазначеному визначенні дієслово «протистояти» означає, що включені захисні заходи, тобто, стійкість може бути зрозуміла як концепція, що охоплює захист КІ. Отже, вона в основному охоплює всі цикли традиційного управління кризами. Стійкість зосереджується на профілактиці, пом'якшенні та готовності до кризи, а також на реагування під час кризи. Та найголовніше, що стійкість також передбачає відновлення після кризи.

Беручи до уваги зазначене визначення та організації і установи, які відповідають за вжиття відповідних заходів до, під час або після шкідливої та небажаної події, що впливає на функціонування КІ, можемо розмежовувати область стійкості на три сфери стійкості КІ: суспільну, організаційну та технологічну.

У суспільній стійкості важливими суб'єктами є органи влади та місцевого самоврядування, територіальні громади, органи самоорганізації населення і окремі фізичні особи. Саме в таких умовах стійкість КІ часто перегукується з цивільним захистом та запобіганням виникнення надзвичайних ситуацій.

В організаційній стійкості суб'єкти включають підприємства та організації різної форми власності, які мають найбільший вплив на взаємозв'язки між об'єктами КІ.

У технологічній стійкості суб'єктами є відповідні оператори об'єктів КІ, а також, зацікавлені сторони відповідальні за оптимальне управління матеріальними, інформаційними, фінансовими потоками і безпеку.

Зауважимо, що в Нордичних країнах, Скандинавського регіону Європейського Союзу концепція стійкості також перейшла від академічної дискусії до офіційних політичних документів.

Агентством з надзвичайних ситуацій Королівства Данія з 2006 по 2010 рік підготовлено Доповіді про національну вразливість [21], що зосереджувалися на вразливості, як на зворотному понятті від концепції стійкості. Аналізуючи зазначені документи, можна сказати, що вразливість, та її протилежність, стійкість, виражає загальну здатність системи функціонувати та досягати своїх цілей, стикаючись із загрозами. Система є вразливою, коли їй не вистачає або не має спроможності планувати, запобігати, реагувати або відновлюватися

після реалізованої загрози, а оцінка вразливості проводиться шляхом порівняння загроз з наявними можливостями, враховуючи бажаний ступінь захисту. У такому підході поняття вразливості та стійкості фактично ідентифікують одне і те ж визначення, тоді як стійкість сама по собі не обговорюється окремо. При цьому, термін стійкість опосередковано охоплюється тим, що в цих документах використовуються такі слова, як стійкість, вразливість та відновлення, які можна розглядати як ключові слова чи елементи в концепції стійкості. Національний профіль ризику, розроблений Агентством з надзвичайних ситуацій Королівства Данія 2013 року, зокрема, зазначає, що суспільство повинно бути міцним і готовим до аварій та катастроф, а в Національному профілі ризику 2017 року розглядаються всі елементи стійкості на базі застосування моделі типового циклу управління кризами, з його до, під час та післякризовими фазами, однак, основний акцент, робиться на захисті, тобто на етапах запобігання, готовності та реагування [22; 23]. Також, розподілено ризики на типи подій та тенденції. Так, серед ризиків для суспільства, що можуть відбутися, зазначено захворювання, пов'язані з водою та харчовими продуктами, погодні умови в зоні приполярного океанічного клімату. Тенденції включають напруженість у політиці безпеки, стійкість до антибіотиків, нерегулярну міграцію.

Аналогічно, Міністерством внутрішніх справ Фінляндії підготовлено доповідь з внутрішньої безпеки «Національна оцінка ризиків 2015 року», в якій концепція стійкості має досить помітне значення [24]. Фінський мовний еквівалент, який, можна виразити як «протистояння кризі», досить чітко підкреслює, що, з огляду на неможливість запобігання кожній кризі, потрібно нарощувати стійкість для постійного швидкого відновлення від матеріалізованої кризи. Концепція стійкості до кризових ситуацій навіть включена до урядового Звіту з питань зовнішньої політики та політики безпеки за 2016 рік [25], що відображає її зв'язок із традиційною концепцією загальної оборони.

У Королівстві Норвегія концепція стійкості також є досить новою, особливо коли мова йде про КІ, навіть якщо вона неявно була представлена раніше в інших документах. Міністерство юстиції та громадської безпеки, соціального захисту після великого теракту в Осло у 2011 році оприлюднило звіт до парламенту Королівства Норвегія про громадську безпеку, в якому згадується про КІ, однак в ньому не міститься концепція стійкості. Королівський указ 2012 року також підкреслює, що відомства повинні оцінювати ризики, вразливість та стійкість КІ у власному секторі на основі національного аналізу ризиків Норвезької дирекції цивільного захисту [26; 27]. Крім того, в резолюції зазначається, що різним відомствам слід розглянути можливість проведення запобіжних заходів, пов'язаних з захистом і посиленням стійкості КІ та важливих функцій суспільства. При цьому, оцінка ризиків повинна включати здатність підтримувати або відновлювати важливі суспільні функції в умовах, які створює небажана подія. Таким чином, ключові елементи стійкості КІ зазначені в цьому документі, але без використання самої концепції стійкості.

Загальною метою Норвезької дирекції цивільного захисту є захист країни та громадян від катастроф, нещасних випадків та інших інцидентів. Дирекції бере участь у міжнародних групах з координації кризи й регулює цивільну оборону, кібербезпеку та відповідає за дослідження, аналіз, запобігання, управління кризами, цивільне і військове співробітництво, навчання, проводить оцінку та нагляд.

У офіційних звітах про оцінку ризиків, пов'язаних з кліматом, та їх значенням для норвезької економіки 2018 року зазначено, що на зовнішні потрясіння краще реагує гнучка система. Стійкі суспільства характеризуються тим, що здатні адаптуватися до мінливих умов під час і після надзвичайного стресу і напруги. Властивості, що характеризують стійкі суспільства – це стійкість та здатність швидко реагувати на зміни. Стійкість системи передбачає її здатність витримувати удар та підтримувати свою структуру і функції. Ці потрясіння часто мають своє походження у зовнішніх джерелах та можуть бути поза сферою впливу постраждалих, але вразливість може бути знижена завдяки заходам, що покращують її здатність реагувати на події [28].

Королівство Швеція, безумовно, було однією з перших країн, яка застосовувала суспільний підхід щодо розвитку безпеки та більш стійкого суспільства, а не простий захист. Так, у 2011 році за замовленням уряду Шведське агентство з надзвичайних ситуацій (MSB) опублікувало Національну стратегію захисту соціально важливої діяльності, визначивши стійкість як «спроможність суспільства протистояти та відновлюватись після збою» [29]. У 2013 році MSB опублікував Звіт щодо захисту соціально важливих видів діяльності під заголовком «Стійкість – концепція різних значень поняття та сфери використання» [30]. Звіт містить ряд визначень поняття стійкість та інформацію про те, як цей термін використовується у різних секторах.

У 2015 році в Лундському університеті, MSB створив науково-дослідний «Центр досліджень критичної інфраструктури» (CenKIP), на базі кафедри управління ризиками та соціального захисту, для здійснення практичних досліджень стійкості та захисту КІ. Останнім документом Центру є дослідження на тему «Підступні вразливості та загрози – виклик для роботи щодо захисту суспільно важливих видів діяльності» що представлений в березні 2020 року. Поняття стійкість використовується в контексті розбудови міцних міст, що мають бути стійкими до різних видів катастроф [31].

Зауважимо, що уряд Великій Британії пишається прогресом, досягнутим для покращення планування і збільшення інвестицій щодо прискорення реалізації проєктів покращення інфраструктури держави. Впровадження першого в історії Національного плану розвитку інфраструктури, заклало основи для зрушення інфраструктури, більш продуктивної економіки та кращого суспільства, так заплановано виділити на 2020 – 21 роки, в рамках проєкту «Трубопровід» на суму 483 мільярди фунтів стерлінгів [32]. У цьому Плані йдеться про необхідність забезпечення стійкості та безпеки об’єктів КІ, а визначення їх переліку, тобто ідентифікація розглядається як спосіб пріоритетності ресурсів. Важливим є питання балансу між посиленням захисту та ціною таких заходів, при цьому основна відповідальність за стійкість КІ покладається на власників та операторів об’єктів КІ, але уряд, регулювальні органи та промислові компанії повинні працювати разом, щоб забезпечити інвестиції в інфраструктуру з урахуванням потреб у безпеці та стабільності.

Одночасно зазначимо, що Австралійський Союз визнає важливість КІ та зосереджує свою політику на стійкості найважливіших послуг для повсякденного життя громадян. Основоположним документом за цим напрямом була Стратегія стійкості КІ уряду Австралії (AGCIRS) 2010 року [33]. В ній враховано залежності між об’єктами КІ різних секторів та визначено стійкість у контексті КІ, як координоване планування в секторах та мережах, оперативне, гнучке та своєчасне відновлення, заходи та розвиток організаційної культури, яка має можливість забезпечувати: мінімальний рівень обслуговування під час перебоїв, надзвичайних ситуацій та катастроф, та швидке повернення до початкового стану. Більш гнучка КІ має допомогти забезпечити постійне безперервне надання основних послуг та підтримати національну безпеку, економічне процвітання та соціальний добробут. Визначивши міжгалузеві взаємозалежності урядом Австралії спрямовано дільність, згідно AGCIRS на наступні стратегічні аспекти:

– здійснювати ефективне партнерство між бізнесом та урядом щодо управляння КІ власниками та операторами;

– розробити та просувати організаційну стійкість знань та загальне розуміння організаційної стійкості;

– допомогти власникам та операторам КІ виявити, проаналізувати та керувати операціями враховуючи міжсекторні залежності;

– надавати своєчасну, якісну політичну консультацію з питань стійкості КІ;

– впровадити Стратегію кібербезпеки уряду Австралії для підтримки надійного, стійкого робочого електронного середовища, в тому числі для власників та операторів КІ;

– підтримка державних та територіальних програм стійкості КІ.

Таким чином в цій країні започатковано новий стратегічний напрямок – організаційна стійкість. Під організаційною стійкістю треба розуміти здатність бізнесу розвиватися та адаптуватися до розвитку глобального ринку, протидії будь – якому короткочасному потрясінню та підготувати себе для реагування на довгострокові виклики.

Стійкість та життєздатність організацій потребує постійного моніторингу фактичного її стану. При цьому, цей підхід допомагає організаціям управляти непередбаченими або несподіваними ризиками та формує можливості не лише ефективно реагувати, але й адаптуватися, вчитися з урахуванням інцидентів та набирати конкурентоспроможної переваги. Тому, організації з сильною культурою стійкості довше зберігатимуть оперативні можливості, попри негаразди, та швидше, ніж конкуренти будуть адаптуватися та повертатися до звичайної діяльності. В розумінні держави, стійка громада краще протистоїть кризовим подіям та реагує на них і, навіть, може бути в найкращому становищі після події.

Існують різні концепції стійкості, хоча вони, як правило, розглядають стійкість як здатність складних систем вижити, адаптуватися, відновлюватися та розвиватися в умовах бурхливих змін. Традиційні стратегії управління ризиками повинні розвиватися одночасно зі швидко мінливим середовищем.

Саме в Австралійському Союзі підхід до стійкості КІ враховує зазначені вимоги відповідно до прагнень підвищити спроможність організацій і громад вижити, відновитися та адаптуватися до всіх видів небезпек, що виникають. Так, частиною AGCIRS є Програма моделювання та аналізу КІ (КІРМА), яка використовує велику кількість масивів даних та інформації для моделювання поведінки системи КІ та її взаємозв'язків щодо: зменшення ризику, відновлення від великих перебоїв і катастроф; досвіду від інцидентів. Цю програму можуть використовувати урядові установи Австралії, уряди території, власники, оператори КІ як набір інструментів для моделювання та аналізу з метою запобігання, підготовки та реагування на природні або спричинені людиною пошкодження КІ, або відновлювання. КІРМА також підтримує роботу мережі довіреної інформації для обміну інформацією (TISN) для стійкості КІ. TISN – це мережева платформа для обміну інформацією між урядовими установами, власниками та операторами КІ [34].

Таким чином, на базі державно – приватного партнерства між бізнесом та урядом Австралії реалізовано AGCIRS та створено чинні механізми моделювання поведінки системи КІ та її взаємозв'язків, ідентифікації ризиків КІРМА та обміну інформацією щодо стійкості КІ – TISN, завдяки яким організації, що належать до системи КІ, можуть керувати як передбачуваними, так і непередбаченими, несподіваними ризиками для своїх критичних інфраструктурних активів, ланцюгів постачання та мереж.

Схожий інноваційний інструмент захисту КІ нещодавно був представлений на Генеральній асамблеї Європейського союзу у Відні, це Мережа дослідження підготовки та стійкості критичної інфраструктури (CIPRNet), що фінансується ЄС з метою сприяння підтримці європейської безпеки через посилення захисту її інфраструктури. Вона створює базу знань щодо захисту КІ та проводить дослідження і розробки для широкого кола зацікавлених сторін, включаючи операторів КІ, політиків та суспільства, для цього інтегруються ресурси партнерів CIPRNet з понад 60 науково-дослідних проєктів Європейського союзу.

Ключовою технологією нових можливостей є система підтримки прийняття рішень (DSS), яка включає аналіз наслідків, прогнозування загроз, візуалізацію загроз, а також доступ та збирання даних. Окрім надання доступу до даних у реальному часі, цей робочий потік пропонує симулятор подій для систем тестування, зокрема, коли користувач може приймати сценарії штучної загрози, отримані дані можна використовувати для проєктування, порівняння та затвердження зусиль щодо пом'якшення наслідків.

CIPRNet одночасно дозволяє здійснювати моделювання системи КІ, враховуючи взаємодії та залежності між елементами системами, а також, моделювання та аналіз заходів захисту КІ. Цей метод потребує об'єднання широкого спектра досвіду, знань та даних з

різних об'єктів інфраструктури. Для подолання технічної перешкоди щодо поєднання даних із різних джерел зазначений проєкт розробив програмне забезпечення для сумісності, яке виконує завдання моделювання та аналізу.

Крім того, CIPRNet розвиває спільну компетенцію шляхом об'єднання різних європейських науково-дослідних заходів в один Віртуальний центр компетентності та експертизи захисту критичної інфраструктури (VCCC). Він надає підтримку при управлінні КІ як на регіональному, національному, так і на транскордонному рівні, в тому числі під час надзвичайних ситуацій, що дозволяє ефективно співпрацювати та сприяє встановленню технічних стандартів [35].

Аналіз застосування поняття «стійкість» свідчить про використання цього терміна для виокремлення двох інструментів формалізації діяльності системи забезпечення національної безпеки, а саме як:

– вимоги до діяльності, що має враховувати різні типи загроз та спроможність реагувати протягом усього діапазону можливого розвитку ситуації щодо передбачення, підготовки, запобігання, реагування та відновлення;

– цільовий стан, який, серед іншого, передбачає формування нових спроможностей системи та показує стратегічний напрям діяльності.

Враховуючи зазначений розподіл використання терміна «стійкість» розглянемо основні світові типи загроз що існують, адже багато країн спрямовують ряд заходів щодо стійкості КІ на захисті від усіх видів загроз, використовуючи підхід до всіх ризиків.

Під поняттям загроза ми будемо розуміти будь-яку дію з потенційною можливістю завдати шкоди інтересам держави або суспільству. Загроза може бути природною, тобто незалежною від діяльності людини, або викликана суб'єктом, наділеним волею і наміром та представленим окремою особою, групою, організацією або державою. Як правило, законодавством провідних держав загрози КІ розподілено на три основні типи, а саме:

– шкідливі дії: саботаж, війна та дії, які спричиняють шкоду суспільству, окремих осіб або груп, таких як злочинці та терористи;

– природні небезпеки: екстремальні погодні умови, лісові та степові пожежі, сейсмічні події, урагани, торнадо, цунамі, епідемії та пандемії, космічні явища;

– технічні аварії: збої системи, викиди шкідливих речовин, пожежі, аварії різних видів, людські помилки тощо.

Кожна з зазначених загроз при виникненні може спричинити негативні наслідки, які стануть ініціаторами інших типів загроз для системи КІ, тобто обумовлює так званий каскадний ефект. Події, які відбуваються внаслідок реалізації загрози безпосередньо один за одним з коротким часовим проміжком, як, наприклад, другий вибух, що відбувається трохи пізніше першого, або кілька аварійних ситуацій, що мають місце практично одночасно в різних місцях, при певних умов, також можуть викликати каскадний ефект.

Аналізуючи можливість здійснення шкідливих дій на об'єктах КІ, тобто загрози, які виходять від тероризму або злочинних діянь за кожною складовою цього типу загрози необхідно дослідити характеристику потенційних злочинців, їх можливих або характерних методів дій, їх цілей і мотивів, а також ступінь кримінальної активності. Це дозволить визначити, які ризики необхідно враховувати за певним типом загрози. Наскільки потенційні злочинці можуть заподіяти серйозної шкоди, і в яких місцях це можливо, має бути предметом оцінки ризиків з урахуванням виявлених вразливих місць безпосередньо за місцем розташування об'єктів КІ.

Без сумніву, події в АР Крим та Східній Україні мають суттєвий вплив на загрози національній системі КІ. Слід очікувати, що високий рівень терористичних, диверсійних та кримінальних загроз системи КІ в Донбаському регіоні збережеться в довгостроковій перспективі. Збройні дії в Донецькій та Луганській областях, сприяють високому рівню зносу основних фондів, що створює загрозу аварій на об'єктах КІ, зокрема, електроенергетики та інженерних мереж, вугільних шахт, хімічних фабрик, металургійних

заводів і призводять до серйозних проблем з екологічною та антропогенною безпекою. Що стосується наявних типів загроз КІ в інших регіонах України, їх характер визначається середовищем загальнонаціональної безпеки.

Аналізуючи можливість виникнення природних небезпек, як загрозу стійкості об'єктів КІ необхідно враховувати, що шкода, яку завдають стихійні лиха, виникає здебільшого в наслідок таких екстремальних атмосферних явищ як паводки, повені, затоплення, сніг, лід, бурі, посухи тощо. Особлива небезпека в випадку паводків виникає в результаті дії води, яка підмиває дороги, мости, дамби, та предметів що плаває в ній. Паводкові води можуть спричинити забруднення питної води та виникнення тим самим значного ризику для здоров'я людини, через витік шкідливих речовин і відходів, які потрапляють та переносяться нею.

Навіть віддалені райони, в яких розташовані об'єкти КІ можуть бути схильні до затоплення внаслідок підйому рівня ґрунтових вод. Щодо таких природних явищ як бурі та урагани, то крім безпосереднього збитку в результаті тиску вітру і подальших сильних поривів, вони можуть викликати додаткові загрози, які спричиняють уламки та сміття, що переносяться у швидко обертає мій воронці. Градини крім шкоди для сільськогосподарських культур та матеріального збитку також можуть призводити до значних травм у людини. Загроза, що виходить від землетрусів, неминуче зростає по мірі зростання їх інтенсивності та може заподіяти значної шкоди будівлям і об'єктам КІ. При певних умовах необхідно враховувати та вторинний збиток від землетрусів, наприклад, у вигляді пожеж.

Суцільні пожежі можуть виникати природним шляхом в наслідок удару блискавки, самозаймання або навмисного чи ненавмисного підпалу в поєднанні з тривалою посухою. Загрозі піддаються, в основному, лісові масиви, сільськогосподарські угіддя та торфовища.

У зв'язку з глобальним товарообігом і туризмом, промисловим вирощуванням тварин, а також повенями та засухами, існує загроза епідемії, як масового географічного поширення будь-якої інфекційної хвороби у людей або тварин. Підвищена небезпека виникає при пандемії – епідемії, яка охоплює населення ряду країн або навіть всього світу.

Аналізуючи можливість виникнення технічних аварій, тобто пожеж, викидів шкідливих речовин, вибухів та інших інцидентів внутрішнього і зовнішнього фізичного впливу, як загрозу стійкості об'єктів КІ необхідно враховувати, що високий рівень старіння українських основних фондів створює загрозу аварій в на об'єктах підвищеної небезпеки, об'єктах електроенергетики та інженерних мережах.

Пожежа на об'єктах КІ може виникнути в результаті людських прорахунків і технічних збоїв, включаючи підпал, внаслідок удару блискавки, виділення небезпечних речовин або вибухів. Залежно від їх масштабу пожежі можуть бути дрібні, середні та великі, які можуть спричинити вивільнення небезпечних речовин. До небезпечних речовин відносяться будь-які хімічні, біологічні, радіологічні або ядерні речовини, що можуть мати шкідливий вплив на довкілля або людину, чи приводити до вибухів і пожеж. Небезпечні речовини за своїми властивостями дуже різні: від дратівливих, легкозаймистих, до вибухонебезпечних і токсичних, що представляють загрозу для довкілля та завдають значний збиток. За допомогою реєстру небезпечних речовин можна забезпечити ідентифікацію небезпечних речовин, які використовуються на підприємстві.

Наслідком людських прорахунків, технічних збоїв, включаючи умисні дії можуть бути вибухи, під час яких відбувається раптове об'ємне розширення газів внаслідок виділення енергії з можливим виділенням тепла, що приводить до виникнення ударної хвилі. Внутрішній і зовнішній фізичний вплив може бути результатом нещасних випадків і аварій. Саме цей ризик характерній більшості об'єктам інфраструктури, класифікованим як потенційно небезпечні. Поряд з руйнуванням об'єктів КІ нещасні випадки та аварії можуть також призводити до пожеж та вибухів, і вивільнення небезпечних речовин, а також до інших відповідних проявів.

Зазначимо, що в Україні, за даними Державної служби України з надзвичайних ситуацій, на 955 об'єктах інфраструктури, зазначених в Державному реєстрі надзвичайно небезпечних об'єктів, можуть виникнути аварії, які спричинять надзвичайні ситуації на національному та регіональному рівнях, що можуть загрожувати системі КІ, зокрема, щодо функціонування паливо-енергетичного комплексу, мостів та доріг, муніципальної інфраструктури тощо.

Визначення небезпечних ризиків, які притаманні всім країнам світу, традиційно, є предметом обговорення на Всесвітньому економічному форумі (ВЕФ), який відбувся 22 січня 2019 року у швейцарському Давосі. Головними глобальними ризиками протягом останніх десятиліть були ризики, що носили виключно економічний характер. Однак, зброя масового знищення та екстремальні погодні явища вже третій рік поспіль належать до основних світових загроз. У оприлюдненій Доповіді про глобальні ризики 2019 року всі ризики поділені на дві категорії: за ступенем імовірності та ступенем впливу події, якщо вона відбудеться.

Серед найбільш імовірних ризиків 2019 року, на думку експертів ВЕФ, перші три позиції посідають екологічні проблеми: екстремальні погодні явища, неготовність до кліматичних змін і стихійні лиха. Далі за ступенем імовірності йде шахрайство та крадіжка даних, кібератаки, штучні екологічні проблеми, масова міграція, втрата біорізноманіття, криза водопостачання та економічна бульбашка.

Половину небезпечних щодо можливого впливу ризиків також складають екологічні проблеми, й усі вони є в групі ймовірних на 2019 рік. Але перше місце в цьому рейтингу все одно посідає зброя масового знищення. Крім того, небезпечними назвали штучні екологічні проблеми та поширення інфекційних захворювань [36].

В Україні класифікація надзвичайних ситуацій за характером походження подій, що можуть зумовити виникнення надзвичайних ситуацій закріплена статтею 5 Кодексу цивільного захисту України. А саме, визначено такі види надзвичайних ситуацій: 1) техногенного характеру; 2) природного характеру; 3) соціальні; 4) воєнні [37].

На наш погляд, враховуючи події в АР Крим та Східній Україні, які мають суттєвий вплив на загрози національній системі КІ, класифікація, яка зазначена в Кодексі цивільного захисту України може бути прийнята для розмежування загроз КІ. Вона має такі три складові, що за своєю суттю відповідають основним типам загроз КІ в цьому безпековому напрямі у світі. При цьому, загрози для КІ України, що мають військовий характер, є актуальними та будуть потребувати уваги ще довгий час.

Термін «стійкість» входить у практику використання українським законодавством, зокрема, Концепція створення державної системи захисту критичної інфраструктури України зазначає, що «створення державної системи захисту критичної інфраструктури спрямоване на забезпечення стійкості критичної інфраструктури до загроз усіх видів, включаючи загрози природного і техногенного характеру, загрози, спричинені протиправними діями, та інші загрози» [38]. Зміни, які відбуваються в напрямі забезпечення національної стійкості у світі, в тому числі, й у термінологічному плані, накладають свій відбиток і на процес реалізації концепції захисту критичної інфраструктури в Україні. Передові країни, що забезпечують життєдіяльність суспільства, базуючись на принципах демократії та верховенства права, навіть стали визначати стійкість як пріоритетний напрям розвитку політики у сфері національної безпеки.

В Україні недосконаліть заходів із комплексного управління захистом КІ спричиняє необхідність вдосконалювати нормативні, організаційні та технологічні інструменти за для забезпечення безпеки та стійкості КІ. Світовий досвід провідних країн світу свідчить про ефективність організації захисту та стійкості об'єктів КІ саме через забезпечення його нормативно – правового супроводження та реалізації заходів єдиним державним органом, що спрощує організаційну діяльність та підвищує рівень управлінської підзвітності та відповідальності. Так, в США було створено єдиний орган виконавчої влади Міністерство

внутрішньої безпеки, на який покладено функції координації захисту КІ США. У Великій Британії урядовим органом з питань безпеки національної інфраструктури є Центр захисту національної інфраструктури, роль якого полягає у захисті та зменшені вразливості національної інфраструктури від тероризму та інших загроз. В Іспанії створено Національний Центр з захисту КІ, який є державною структурою, що відповідає за інформаційну безпеку та кібербезпеку, а також за поширення інформації щодо кіберзагроз та кіберінцидентів, та забезпечує координацію і співпрацю між різними секторами економіки з державними та приватними інституціями. В Республіці Польща за координацію та виконання завдань щодо функціонування системи захисту КІ відповідає Урядовий центр з питань безпеки. В Норвегії створено дирекцію цивільного захисту, яка регулює цивільну оборону та кібербезпеку, спрямовує діяльність щодо захисту від катастроф, нещасних випадків та інших інцидентів, в тому числі, на об'єктах КІ, відповідає за дослідження, аналіз, запобігання, управління кризами, проводить оцінку та нагляд. Віртуальний центр компетентності та експертизи захисту КІ, це новий інноваційний проєкт ЄС, що дозволяє при виникненні надзвичайних ситуацій, ефективно співпрацювати та надавати підтримку при управлінні КІ на регіональному, національному та транскордонному рівні.

Враховуючи вищезазначене, вважаємо, що Україна може перейняти успішний світовий досвід та створити та підтримати функціонування державної установи, яка буде здійснювати координацію дії всіх відомств в разі небезпеки, дестабілізації роботи об'єктів КІ, виконуватиме завдання з організації та впровадження стратегічних рішень щодо стійкості системи КІ в країни. Крім того, така установа має виконувати функції аналітичного та прогностичного характеру щодо комплексної оцінки загроз КІ. Така оцінка може здійснюватися з врахуванням впливу загроз на рівень національної безпеки, та буде корисним інструментом при проведенні моніторингу щодо запобігання кризовим ситуаціям, які пов'язані із функціонуванням системи КІ. Також, новостворена державна установа має бути самостійною, тобто, не входити до організаційної структури будь-якого з відомств, що залучені до вирішення завдань захисту КІ.

Вважаємо, що стійкість КІ не просто оновлення термінів в чинному законодавстві, а впровадження нового підходу зі створенням безпекового партнерства між всіма зацікавленими сторонами. Тут потрібно враховувати співвідношення контролю за об'єктами КІ з боку держави та приватного сектору. Зокрема, у США до 85 % всієї КІ перебуває у приватній власності, а в Україні 100 % нафтопереробляння та понад 75 % теплової енергетики, знаходяться у приватних руках. Однак зазначимо, що саме держава має відповідати за розроблення та впровадження стандартизованого методологічного підходу до оцінювання загроз і ризиків КІ, узагальнення всієї інформації та розроблення стратегічних рішень щодо стійкості системи КІ.

Більшість провідних країн світу цьому питанню приділяють значну увагу, одна з них Канада у Національній стратегії захисту КІ якої зазначається, що відповідальність за забезпечення захисту КІ країни мають нести усі державні органи, приватний сектор, а також канадці як члени канадського суспільства. Особлива увага зосереджується на суспільстві яке повинно бути готовим протистояти надзвичайним ситуаціям щонайменше упродовж перших 72 годин з моменту настання тієї чи іншої події. При цьому робота, по розробленню пріоритетів та основних заходів зі зменшення загроз, спрямованих на КІ у кожному із секторів, ведеться урядом Канади в рамках державно-приватного партнерства (ДПП) з усіма зацікавленими суб'єктами процесу. Для цього уряд надає операторам і власникам об'єктів та систем КІ точну інформацію щодо загроз і ризиків та забезпечує їх та місцеві органи влади планами реагування на надзвичайні ситуації.

Стосовно Європейської програми захисту КІ, то відповідальність за захист її об'єктів КІ покладається на їх власників, операторів та уряд відповідної держави-члену ЄС. При цьому, підтримка публічного сектору у розбудові інституційного потенціалу ДПП та контроль за галузевим і національним розвитком ринку ДПП здійснюється Європейським

експертним центром з питань ДПП (ЕРЕС). Він був створений за підтримки Європейського інвестиційного банку у 2008 році для підтримки держав-членів та інших членів та кандидатів ЄС у роботі за напрямом ДПП [39].

Проєкти ДПП в Європі спрямовані на розвиток публічного та приватного секторів шляхом надання товарів та послуг, які мають поставлятися державним сектором з застосуванням пом'якшення жорстких бюджетних обмежень на державні витрати. Тобто, ДПП це домовленість між державним органом та приватним партнером, про виконання проєкту та послуги для публічної інфраструктури за довгостроковим контрактом. Відповідно до цього договору, приватний партнер несе значні ризики та обов'язки управління. Державна влада здійснює платежі на основі ефективності приватного партнера за надання послуги або надає приватному партнеру право на отримання частини доходу від надання послуги. Приватні фінанси зазвичай беруть участь у ДПП. При правильній підготовці проєкти ДПП можуть принести значні переваги як державному сектору, так і користувачам проєкту та можуть бути розроблені для досягнення широкого спектра цілей у різних секторах, таких як транспорт, соціальне житло та охорона здоров'я, і можуть бути структуровані за різних підходів.

ДПП за своєю суттю та результатами не відрізняються від традиційних проєктів закупівель, але вони демонструють деякі відмінності в управлінні. Основна відмінність – це розподіл ризику між державним та приватним партнером. Приватний партнер часто несе відповідальність за ризики, пов'язані з проєктуванням, будівництвом, фінансуванням, експлуатацією та обслуговуванням інфраструктури, тоді як державний партнер зазвичай бере на себе регуляторні та політичні ризики.

Більшість ДПП в ЄС реалізується в галузях дорожнього транспорту та інформаційно-комунікаційних технологій, випереджаючи охорону здоров'я та освіту. Основні гранти фінансуються ЄС у співпраці з Європейським інвестиційним банком незалежно від того, чи мають вони обґрунтований аналіз та чи відповідають встановленим правовим рамкам загальні підходи, що використані в проєктах, оскільки очікується, що проєкти ДПП будуть реалізовані. Багато проєктів довгострокові, з тривалістю виконання від 5 до 7 років, що призводить до здороження закупівлі, затримкам із виплатами та збільшення часу їх реалізації, особливо це стосується проєктів будівництва. Зауважимо, що на думку європейських експертів ЕРЕС, кошти витрачені на проєкти будівництва автомагістралі у Греції, були використані неефективно з точки зору досягнення потенційної вигоди. В основному це було пов'язано з фінансовою кризою та неякісною підготовкою проєктів державним партнером, згідно з якими було передчасно укладено недостатньо ефективні договори концесії з приватними партнерами. Крім того, розподіл ризиків між державними та приватними партнерами був невідповідним, неузгодженим та неефективним, а високі показники оплати праці приватного партнера не завжди показували ризики, які вони несуть.

Всупереч зазначеному, у Європі існує тенденція до більш інтенсивного використання державних коштів з приватними фінансами через ДПП. Здебільш, продовж періоду з 1990 по 2016 роки ДПП було зосереджено у Великобританії, Франції, Греції, Іспанії, Португалії та Німеччині, які реалізували проєкти, що становлять 90 % всього ринку. Стратегія «Європа 2020» підкреслює важливість ДПП, наголошуючи, що використання фінансових коштів шляхом поєднання приватних і державних фінансів та створення інноваційних інструментів для фінансування необхідних інвестицій є одним із ключових аспектів, які Європа повинна дотримуватися для досягнення своїх цілей до 2020 року.

Успішне виконання проєктів ДПП дозволило державним органам реалізувати великі об'єкти інфраструктури за допомогою єдиної Процедури закупівлі, однак, замовники, які мали слабкі переговорні позиції виявилися недостатньо конкурентоспроможними для участі.

Згідно із дослідженими літературними джерелами зазначимо, що проєкти ДПП забезпечують досягнення потенційної вигоди у порівнянні з традиційними методами закупівель, особливо відносно інфраструктурних об'єктів, зокрема такими перевагами є:

– реалізація запланованої програми капітальних інвестицій регіону, оскільки ДПП можуть забезпечити важливе додаткове фінансування для доповнення традиційних бюджетних коштів;

– можливість підвищення ефективності в реалізації проєкту шляхом швидшого виконання окремих проєктів;

– підвищення рівня обслуговування, в порівнянні з традиційними проєктами, через замовлення всього процесу разом;

– об'єднання державних та приватних експертиз найбільш ефективним чином для проведення поглибленої оцінки проєкту та досягнення оптимізації обсягу проєкту.

Досвід різних держав світу, розглянутий вище, дозволяє зазначити, що ключовими інструментами забезпечення національної безпеки та стійкості суспільства є успішна розробка та впровадження державної концепції, стратегії та відповідних планів дій, зокрема плану забезпечення стійкості КІ. Більшість розвинутих країн продовжують спрямовувати зусилля на впровадження та реалізацію комплексних програм за цим напрямом осторонь інших пріоритетів та мають конкретні поліпшення рівня безпеки та стійкості.

Висновки. Для поліпшення якості нашого життя та забезпечення безперебійної роботи інфраструктури, доцільно впровадити концептуальний підхід до підвищення безпеки та стійкості системи КІ, тобто реагування на непередбачені, несподівані ризики та події тощо. Оскільки саме КІ забезпечує життєво важливі для населення, суспільства та держави послуги та функції, без яких неможливі їх безпечне існування та добробуту, а також належний рівень національної безпеки.

Наразі ми можемо спостерігати поступовий перехід від концепції захисту до стійкості в контексті розвитку безпеки та більш стійкого суспільства, яке розглядається як цінність, якість і бажана характеристика. Відбувається формування такого стратегічного напрямку як організаційна стійкість, що допомагає організаціям управляти непередбаченими або несподіваними ризиками та формує можливості не лише ефективно реагувати, але й адаптуватися, вчитися з урахуванням інцидентів та набирати конкурентоспроможної переваги.

Низка аналітичних матеріалів та офіційних документів з даної тематики надали підґрунтя для формування визначення таких термінів як «безпека КІ» та «стійкість КІ», а також, можливість розмежування області стійкості на три сфери стійкості КІ: суспільну, організаційну та технологічну. Крім того, в статті запропоновані мета та завдання публічної політики з питань захисту об'єктів КІ та розмежування загроз КІ, з враховуванням завдань публічної політики щодо безпеки, захисту та забезпечення стійкого розвитку КІ держави, які можуть бути використані при розробці нормативно-правових актів.

На нашу думку, серед пріоритетних напрямів забезпечення стійкості КІ є створення установи, яка виконуватиме завдання з формування та реалізації стратегічних рішень щодо стійкості системи КІ країни, а також, впровадження нового підходу зі створенням безпекового партнерства між всіма зацікавленими сторонами. При цьому, достатня увага має бути приділена впровадженню інноваційних проєктів моделювання системи стійкості КІ та аналізу комплексної оцінки загроз об'єктів КІ на базі державно-приватного партнерства між бізнесом та урядом.

Література.

1. Мельничук О. В. Управління критичною інфраструктурою держави: базові методи та критерії ідентифікації об'єктів. *Державне управління та місцеве самоврядування*: зб. наук. праць. Дніпро: ДРІДУ НАДУ, 2019. Вип. 3(42). С. 13–27.

2. Мельничук О. Критическая инфраструктура государства как составляющая национальной безопасности: понятийно-категориальный апарат. Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy ISSN 1896-8333, e-ISSN 2449-9013. № 30(1)/2019. p. 249–265.

3. Зелена книга з питань захисту критичної інфраструктури в Україні: зб. матеріалів міжнар. експерт. нарад / упоряд.: Д. С. Бірюков, С. І. Кондратов; за заг. ред. О. М. Суходолі. Київ: НІСД, 2015. 176 с.

4. Суходоля О. М. Захист критичної інфраструктури: сучасні виклики та пріоритетні завдання сектору безпеки. *Науковий часопис Академії національної безпеки*. 2017. Вип. 1–2(13–14). С. 50–80.

5. Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS–Strategie) BMI, 2009. URL: http://www.kritis.bund.de (дата звернення: 16.03.2020).

6. Quadrennial Homeland Security Review, 2010, 2014. URL: https://www.dhs.gov/quadrennial-homeland-security-review (дата звернення: 19.03.2020).

7. Keogh M., Cody C. , Resilience in Regulated Utilities / research document of the National Association of Regulatory Utility Commissioners, 2013. URL:https://pubs.naruc.org/pub/536F07E4-2354-D714-5153-7A80198A436D (дата звернення: 22.03.2020).

8. Holling C. Resilience and stability of ecological systems, Annual review of ecology and systematics, pp. 1–23, 1973.

9. Haimes Y., On the Definition of Resilience in Systems, Risk Analysis. 2009. Vol. 29. №4. Pp. 498–501.

10. Nan C., Sansavini G. A quantitative method for assessing resilience of interdependent infrastructures, Reliability Engineering and System Safety. Elsevier, 2017. Vol. 157(C). P. 35–53.

11. Folke C., Resilience: the emergence of a perspective for soKIal – ecological systems analyses. *Global Environmental Change.* 2006. 16(3). P. 253–267.

12. Resilience Analysis and Practice, The Resilience Alliance. *Research organization.* URL: http://www.resalliance.org/index.php/resilience (дата звернення: 24.03.2020).

13. Стійкість систем / матеріал з Вікіпедії – вільної енциклопедії / URL: https://uk.wikipedia.org/wiki/Стійкість_систем (дата звернення: 25.03.2020).

14. EC, Green Paper on a European Programme for Critical Infrastructure Protection, Commission of The European Communities, Brussels, 2005 (17 November 2005, (Com)(2005) 576 Final).

15. The European Council. On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Council Directive 2008/114/EC of 8 December 2008.

16. Presidential Policy Directive – Critical Infrastructure Security and Resilience. (2013). URL: https://www.dhs.gov/sites/default/files/publications/PPD–21–Critical–Infrastructure–andResilience–508.pdf (дата звернення: 16.03.2020).

17. European Commission Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPKIP), Brussels, 22 June 2012, SWD(2012) 190 final, 2012.

18. Pursiainen C., Gattinesi P., Towards Testing Critical Infrastructure Resilience, Publications Office of the European Union, JRC SKIentific and Policy Reports, Luxembourg, 2014.

19. European External Relations Service (EEAS) Building, 9A Rond Point Schuman, 1046 Brussels, Belgium URL: https://eeas.europa.eu/topics/eu–global–strategy_en (дата звернення: 26.03.2020).

20. UNISDR (n.d.) Terminology on Disaster Risk Reduction, United Nations International Strategy for Disaster Reduction, Switzerland, Geneva, [Online] Available at URL: http://www.unisdr.org/we/inform/terminology (дата звернення: 23.03.2020).

21. DEMA, National Sårbarhedsrapport, Beredskabsstyrelsen, Denmark, Birkerød, 2006, 2010.

22. DEMA, National Risk Profile (NRP), The Danish Emergency Management Agency, Denmark, Birkerød, 2013.

23. DEMA Nationalt Risikobillede, Beredskabsstyrelsen, Denmark, Birkerød, 2017.

24. Ministry of the Interior, Finland National Risk Assessment 2015, Internal security, Ministry of The Interior Publication 4/2016, Finland, Helsinki, 2016.

25. Valtioneuvoston kanslia, Valtioneuvoston ulko – ja turvallisuuspoliittinen selonteko, Valtioneuvoston kanslian julkaisusarja 7/2016, Finland, Helsinki, 2016.

26. Ministry of Justice and Public Safety, Samfunnssikkerhet, Report to the Storting 29 (2011–2012), Norway, Oslo, 2012.

27. DSB, Instruks for departementenes arbeid med samfunnssikkerhet og beredskap, Justis – og beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentral krisehåndtering (Royal Decree of 15 June 2012), Norwegian Directorate for KIvil Protection, Norway, Oslo, 2012.

28. OffiKIal Norwegian Reports NOU 2018: 17 Summary. Climate risk and the Norwegian economy. Summary of a report from a Commission appointed by Royal Decree on 6 October 2017 to assess climate–related risk factors and their significance for the Norwegian economy. URL:https://www.regjeringen.no/contentassets/c5119502a03145278c33b72d9060fbc9/en–gb/pdfs/nou201820180017000engpdfs.pdf (дата звернення: 28.01.2020).

29. MSB, Ett fungerande samhälle i en föränderlig värld: Nationell strategi för skydd av samhällsviktig verksamhet, Swedish KIvil ContingenKIes Agency, Sweden, Karlstad, 2011.

30. MSB, Handlingsplan för skydd av samhällsviktig verksamhet, Swedish KIvil ContingenKIes Agency, Sweden, Karlstad, 2013.

31. CenCIP. Besöksadress: Avdelningen för Riskhantering och Samhällssäkerhet V-byggnaden, John Ericssons Väg 1, Lund, Sweden, Box 118, 221 00 Lund. URL: https://www.cencip.lu.se (дата звернення: 16.04.2020).

32. National Infrastructure Delivery Plan 2016 – 2021. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/520086/2904569_nidp_deliveryplan.pdf (дата звернення: 06.04.2020).

33. Australian Government (2010) Critical infrastructure resilience strategy. ISBN: 978–1–921725–25–8. URL: http://www.emergency.qld.gov.au/publications/pdf/Critical_Infrastructure_Resilience_Strategy.pdf (дата звернення: 20.01.2020).

34. The Trusted Information Sharing Network for Critical Infrastructure Resilience. URL: https://www.tisn.gov.au/ (дата звернення: 20.04.2020).

35. Critical Infrastructures Preparedness and Resilience Research Network. URL: https://ciprnet.eu/home/ (дата звернення: 22.04.2020).

36. Глобальні ризики 2019 року: зброя масового знищення та екстремальна погода Аналітичний портал «Слово і Діло» URL: https://www.slovoidilo.ua/2019/01/23/infografika/svit/hlobalni–ryzyky–2019–roku–zbroya–masovoho–znyshhennya–ta–ekstremalna–pohoda (дата звернення: 11.04.2020)

37. Кодекс цивільного захисту України. URL: https://zakon.rada.gov.ua/laws/show/5403–17 (дата звернення: 13.04.2020).

38. Про рішення Ради національної безпеки і оборони України від 04 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України»: Указ Президента України від 14.03.2016 р. № 92/2016. URL: http://zakon3.rada.gov.ua/laws/show/92/2016 (дата звернення: 10.04.2020).

39. The European public-private partnership Expertise Centre. URL: https://www.eib.org/epec/ (дата звернення: 16.04.2020).

40. Рекомендації парламентських слухань щодо розвитку інформаційного суспільства в Україні, схвалено Постановою Верховної Ради України «Про Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні» від 01.12.2005 р. № 3175–IV.

41. Стратегія національної безпеки України «Україна у світі, що змінюється», затверджено Указом Президента України «Про Стратегію національної безпеки України» від 12.02.2007 № 105 в редакції Указу Президента України від 08.06.2012 р. № 389/2012.

42. Стратегія національної безпеки України: затверджено Указом Президента України «Про рішення Ради національної безпеки і оборони України від 06.05.2015 року «Про Стратегію національної безпеки України» від 26.05.2015 № 287/2015.

References.

1. Melnychuk O. V. Upravlinnia krytychnoiu infrastrukturoiu derzhavy: bazovi metody ta kryterii identyfikatsii obiektiv. Derzhavne upravlinnia ta mistseve samovriaduvannia: zb. nauk. prats. Dnipro: DRIDU NADU, 2019. Vyp. 3(42). S. 13–27.

2. Melnychuk O. Krytycheskaia ynfrastruktura hosudarstva kak sostavliaiushchaia natsyonalnoi bezopasnosty: poniatyino-katehoryalnыi aparat. Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy ISSN 1896-8333, e-ISSN 2449-9013. № 30(1)/2019. p. 249–265.

3. Zelena knyha z pytan zakhystu krytychnoi infrastruktury v Ukraini: zb. materialiv mizhnar. ekspert. narad / uporiad.: D. S. Biriukov, S. I. Kondratov; za zah. red. O. M. Sukhodoli. Kyiv: NISD, 2015. 176 s.

4. Sukhodolia O. M. Zakhyst krytychnoi infrastruktury: suchasni vyklyky ta priorytetni zavdannia sektoru bezpeky. Naukovyi chasopys Akademii natsionalnoi bezpeky. 2017. Vyp. 1–2(13–14). S. 50–80.

5. Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS–Strategie) BMI, 2009. URL: http://www.kritis.bund.de (data zvernennia: 16.03.2020).

6. Quadrennial Homeland Security Review, 2010, 2014. URL: https://www.dhs.gov/quadrennial-homeland-security-review (data zvernennia: 19.03.2020).

7. Keogh M., Cody C. , Resilience in Regulated Utilities / research document of the National Association of Regulatory Utility Commissioners, 2013. URL:https://pubs.naruc.org/pub/536F07E4-2354-D714-5153-7A80198A436D (data zvernennia: 22.03.2020).

8. Holling C. Resilience and stability of ecological systems, Annual review of ecology and systematics, pp. 1–23, 1973.

9. Haimes Y., On the Definition of Resilience in Systems, Risk Analysis. 2009. Vol. 29. №4. Pp. 498–501.

10. Nan C., Sansavini G. A quantitative method for assessing resilience of interdependent infrastructures, Reliability Engineering and System Safety. Elsevier, 2017. Vol. 157(C). P. 35–53.

11. Folke C., Resilience: the emergence of a perspective for soKIal – ecological systems analyses. Global Environmental Change. 2006. 16(3). R. 253–267.

12. Resilience Analysis and Practice, The Resilience Alliance. Research organization. URL: http://www.resalliance.org/index.php/resilience (data zvernennia: 24.03.2020).

13. Stiikist system / material z Vikipedii – vilnoi entsyklopedii / URL: https://uk.wikipedia.org/wiki/Stiikist_system (data zvernennia: 25.03.2020).

14. EC, Green Paper on a European Programme for Critical Infrastructure Protection, Commission of The European Communities, Brussels, 2005 (17 November 2005, (Com)(2005) 576 Final).

15. The European Counsil. On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Counsil Directive 2008/114/EC of 8 December 2008.

16. Presidential Policy Directive – Critical Infrastructure Security and Resilience. (2013). URL: https://www.dhs.gov/sites/default/files/publications/PPD–21–Critical–Infrastructure–andResilience–508.pdf (data zvernennia: 16.03.2020).

17. European Commission Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPKIP), Brussels, 22 June 2012, SWD(2012) 190 final, 2012.

18. Pursiainen C., Gattinesi P., Towards Testing Critical Infrastructure Resilience, Publications Office of the European Union, JRC SKIentific and Policy Reports, Luxembourg, 2014.

19. European External Relations Service (EEAS) Building, 9A Rond Point Schuman, 1046 Brussels, Belgium URL: https://eeas.europa.eu/topics/eu–global–strategy_en (data zvernennia: 26.03.2020).

20. UNISDR (n.d.) Terminology on Disaster Risk Reduction, United Nations International Strategy for Disaster Reduction, Switzerland, Geneva, [Online] Available at URL: http://www.unisdr.org/we/inform/terminology (data zvernennia: 23.03.2020).

21. DEMA, National Sårbarhedsrapport, Beredskabsstyrelsen, Denmark, Birkerød, 2006, 2010.

22. DEMA, National Risk Profile (NRP), The Danish Emergency Management Agency, Denmark, Birkerød, 2013.

23. DEMA Nationalt Risikobillede, Beredskabsstyrelsen, Denmark, Birkerød, 2017.

24. Ministry of the Interior, Finland National Risk Assessment 2015, Internal security, Ministry of The Interior Publication 4/2016, Finland, Helsinki, 2016.

25. Valtioneuvoston kanslia, Valtioneuvoston ulko – ja turvallisuuspoliittinen selonteko, Valtioneuvoston kanslian julkaisusarja 7/2016, Finland, Helsinki, 2016.

26. Ministry of Justice and Public Safety, Samfunnssikkerhet, Report to the Storting 29 (2011–2012), Norway, Oslo, 2012.

27. DSB, Instruks for departementenes arbeid med samfunnssikkerhet og beredskap, Justis – og beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentral krisehåndtering (Royal Decree of 15 June 2012), Norwegian Directorate for KIvil Protection, Norway, Oslo, 2012.

28. OffiKIal Norwegian Reports NOU 2018: 17 Summary. Climate risk and the Norwegian economy. Summary of a report from a Commission appointed by Royal Decree on 6 October 2017 to assess climate–related risk factors and their significance for the Norwegian economy. URL:https://www.regjeringen.no/contentassets/c5119502a03145278c33b72d9060fbc9/en–gb/pdfs/nou201820180017000engpdfs.pdf (data zvernennia: 28.01.2020).

29. MSB, Ett fungerande samhälle i en föränderlig värld: Nationell strategi för skydd av samhällsviktig verksamhet, Swedish KIvil ContingenKIes Agency, Sweden, Karlstad, 2011.

30. MSB, Handlingsplan för skydd av samhällsviktig verksamhet, Swedish KIvil ContingenKIes Agency, Sweden, Karlstad, 2013.

31. CenCIP. Besöksadress: Avdelningen för Riskhantering och Samhällssäkerhet V-byggnaden, John Ericssons Väg 1, Lund, Sweden, Box 118, 221 00 Lund. URL: https://www.cencip.lu.se (data zvernennia: 16.04.2020).

32. National Infrastructure Delivery Plan 2016 – 2021. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/520086/2904569_nidp_deliveryplan.pdf (data zvernennia: 06.04.2020).

33. Australian Government (2010) Critical infrastructure resilience strategy. ISBN: 978–1–921725–25–8. URL: http://www.emergency.qld.gov.au/publications/pdf/Critical_Infrastructure_Resilience_Strategy.pdf (data zvernennia: 20.01.2020).

34. The Trusted Information Sharing Network for Critical Infrastructure Resilience. URL: https://www.tisn.gov.au/ (data zvernennia: 20.04.2020).

35. Critical Infrastructures Preparedness and Resilience Research Network. URL: https://ciprnet.eu/home/ (data zvernennia: 22.04.2020).

36. Hlobalni ryzyky 2019 roku: zbroia masovoho znyshchennia ta ekstremalna pohoda Analitychnyi portal «Slovo i Dilo» URL: https://www.slovoidilo.ua/2019/01/23/infografika/svit/hlobalni–ryzyky–2019–roku–zbroya–masovoho–znyshhennya–ta–ekstremalna–pohoda (data zvernennia: 11.04.2020)

37. Kodeks tsyvilnoho zakhystu Ukrainy. URL: https://zakon.rada.gov.ua/laws/show/5403–17 (data zvernennia: 13.04.2020).

38. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 04 bereznia 2016 roku «Pro Kontseptsiiu rozvytku sektoru bezpeky i oborony Ukrainy»: Ukaz Prezydenta Ukrainy vid 14.03.2016 r. № 92/2016. URL: http://zakon3.rada.gov.ua/laws/show/92/2016 (data zvernennia: 10.04.2020).

39. The European public-private partnership Expertise Centre. URL: https://www.eib.org/epec/ (data zvernennia: 16.04.2020).

40. Rekomendatsii parlamentskykh slukhan shchodo rozvytku informatsiinoho suspilstva v Ukraini, skhvaleno Postanovoiu Verkhovnoi Rady Ukrainy «Pro Rekomendatsii parlamentskykh slukhan z pytan rozvytku informatsiinoho suspilstva v Ukraini» vid 01.12.2005 r. № 3175–IV.

41. Stratehiia natsionalnoi bezpeky Ukrainy «Ukraina u sviti, shcho zminiuietsia», zatverdzheno Ukazom Prezydenta Ukrainy «Pro Stratehiiu natsionalnoi bezpeky Ukrainy» vid 12.02.2007 № 105 v redaktsii Ukazu Prezydenta Ukrainy vid 08.06.2012 r. № 389/2012.

42. Stratehiia natsionalnoi bezpeky Ukrainy: zatverdzheno Ukazom Prezydenta Ukrainy «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 06.05.2015 roku «Pro Stratehiiu natsionalnoi bezpeky Ukrainy» vid 26.05.2015 № 287/2015.