

НАЦІОНАЛЬНИЙ ІНСТИТУТ СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ

Центр безпекових досліджень
Center for Security Studies

<https://doi.org/10.53679/NISS-analytrep.2024.04>

О. М. Суходоля

**СТІЙКІСТЬ
КРИТИЧНОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ
ТА ЖИТТЄДІЯЛЬНОСТІ ГРОМАД**

Аналітична доповідь

Київ 2024

Електронну версію видання розміщено на: <http://www.niss.gov.ua>
*За повного або часткового відтворення матеріалів цієї публікації
посилання на видання є обов'язковим*

Автор:

О. М. Суходоля, завідувач відділу критичної інфраструктури, енергетичної та екологічної безпеки центру безпекових досліджень Національного інституту стратегічних досліджень, доктор наук з державного управління, професор

Суходоля О. М.

C91 Стійкість критичної енергетичної інфраструктури та життєдіяльності громад : аналіт. доп. – Київ : НІСД, 2024. – 160 с. – <https://doi.org/10.53679/NISS-analytrep.2024.04>

В аналітичній доповіді уміщено огляд методологічних підходів щодо визначення мети, завдань і змісту діяльності із забезпечення безпеки та стійкості критичної інфраструктури, яка підтримує життєдіяльність громад. Представлено концептуальну модель формалізації вимог до діяльності у сфері стійкості, окреслено структуру заходів забезпечення стійкості за етапами циклу кризового реагування. Запропоновано розроблені методологію визначення завдань суб'єктів кризового реагування, необхідних і можливих рівнів стійкості функціонування критичної інфраструктури та надання життєво важливих функцій і послуг. Запропоновано принципи планування стійкості, орієнтовні типову структуру та зміст плану стійкості життєдіяльності громад.

Розраховано на експертів, науковців, менеджерів, які працюють у сфері національної безпеки, суб'єктів владних повноважень, представників громадських організацій, а також усіх, хто цікавиться проблематикою стійкості функціонування критичної інфраструктури, забезпечення життєво важливих функцій та надання послуг. Дослідження буде корисним для формування цільових параметрів стійкості різних сфер управління, формалізації інструментів планування стійкості, розроблення практичного інструментарію регулювання діяльності всіх суб'єктів, залучених до забезпечення стійкості життєдіяльності суспільства.

Sukhodolia, O. M.

C91 Resilience of critical energy infrastructure and communities : report. – Kyiv : NISS, 2024. – 160 p. – <https://doi.org/10.53679/NISS-analytrep.2024.04>

The analytical report includes an overview of methodological approaches to determining the goals, tasks and content of stakeholders' actions to ensure the security and resilience of critical infrastructure that enables a stable functioning of community. A conceptual model of formalization of requirements for activities in the field of resilience is presented, and the structure of measures to ensure resilience of critical infrastructure according to the stages of the crisis response cycle is outlined. The methodology for defining the tasks of crisis response subjects, the required levels of the functioning of critical infrastructure and the provision of vital functions and services are proposed. The principles of resilience planning as well as the structure and content of the community resilience plan are proposed.

The publication is intended for experts, scientists, managers who work in the field of national security, as well as everyone who is interested in critical infrastructure protection and resilience, provision of vital functions and services. The report will be useful for development of resilience metric and target setting in various spheres of management. The study will support the formalization of the resilience planning process, the development of a practical toolkit for regulating the activities of all subjects involved in ensuring the resilience of critical infrastructure and society's vital functions and services.

УДК 681.5.7+338.49:32.019.5:620.9

ЗМІСТ

ВСТУП	5
Розділ 1. СТІЙКІСТЬ КРИТИЧНОЇ ІНФРАСТРУКТУРИ У СИСТЕМІ НАЦІОНАЛЬНОЇ СТІЙКОСТІ.....	8
1.1. Огляд політики та законодавства окремих країн з питань безпеки та стійкості критичної інфраструктури.....	8
1.2. Забезпечення стійкості надання життєво важливих функцій / послуг: досвід США у сфері енергозабезпечення.....	22
1.3. Розвиток законодавства України з питань стійкості функціонування критичної інфраструктури: стан та виклики.....	29
1.4. Узагальнення світового досвіду та узгодження підходів до планування заходів безпеки та стійкості і критичної інфраструктури.....	35
Розділ 2. БЕЗПЕКА ТА СТІЙКІСТЬ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ФОРМАЛІЗАЦІЯ МОДЕЛІ ТА ВСТАНОВЛЕННЯ ВИМОГ	48
2.1. Безпека критичної інфраструктури як складова частина планів стійкості.....	48
2.2. Формалізація вимог щодо стійкості надання життєво важливих функцій / послуг та функціонування критичної інфраструктури	54
2.3. Узагальнення практики реагування на порушення функціонування критичної енергетичної інфраструктури.....	60
Розділ 3. ЗАСАДИ РОЗРОБЛЕННЯ ПЛАНУ СТІЙКОСТІ ФУНКЦІОНУВАННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА НАДАННЯ ЖИТТЄВО ВАЖЛИВИХ ФУНКЦІЙ НА РІВНІ ТЕРИТОРІАЛЬНИХ ГРОМАД	62
3.1. Організація планування стійкості життєдіяльності громад.....	62
3.2. Зміст етапів підготовки плану стійкості	65
Розділ 4. РОЗРОБЛЕННЯ ПЛАНУ СТІЙКОСТІ	102
4.1. Загальні засади планування стійкості функціонування критичної інфраструктури та надання життєво важливої функції / послуги	102
4.2. Базові вимоги до розроблення плану стійкості	103
4.3. Зміст плану стійкості за етапами циклу кризового реагування.....	104
4.4. Орієнтовний зміст і структура плану стійкості.....	109
ВИСНОВКИ	111
ДОДАТКИ	113
Додаток 1. Групи загроз / небезпек, що увійшли до Стратегічної національної оцінки ризику США	113

<i>Додаток 2. Порівняльний аналіз прикладів реагування на загрози й ризику кризової ситуації за етапами циклу кризового реагування</i>	115
<i>Додаток 3. Взаємозалежності життєво важливих функцій та особливості їх надання</i>	120
<i>Додаток 4. Огляд загроз для енергетичного сектору</i>	127
<i>Додаток 5. Загальний алгоритм оцінювання впливу загроз</i>	130
<i>Додаток 6. Потенціал відновлюваних джерел енергії України</i>	138
<i>Додаток 7. Приклади реалізації проєктів енергозабезпечення територіальних громад України на основі використання місцевих ресурсів</i>	141
<i>Додаток 8. Огляд заходів реагування на порушення функції електропостачання через руйнування РФ енергетичної інфраструктури України в осінньо-зимові періоди 2022–2024 рр.</i>	150

ВСТУП

Забезпечення стійкості життєдіяльності країни чи функціонування окремих систем, які її підтримують, сьогодні стало актуальним напрямом наукових досліджень у сфері національної безпеки, пріоритетом створення й удосконалення методології стратегічного планування розвитку та запровадження сучасних механізмів державного управління.

У багатьох країнах завдання забезпечення національної стійкості, захисту критичної інфраструктури (КІ) та забезпечення життєво важливих функцій (ЖВФ) і надання послуг суспільству визначено низкою законодавчих актів, документів концептуального та стратегічного характеру.

В Україні у 2021 р. також було прийнято акти законодавства, які перемістили завдання розбудови стійкості життєдіяльності країни з поля науково-теоретичної дискусії у площину практичних дій.

Концепція забезпечення національної стійкості України, затверджена рішенням Ради національної безпеки і оборони (РНБО), визначила мету, основні принципи, напрями, механізми й строки запровадження та функціонування національної системи стійкості. Ця система спрямована на формування спроможності країни забезпечити стійкість функціонування важливих сфер життєдіяльності суспільства та держави.

Закон України «Про критичну інфраструктуру» визначає пріоритети політики у сфері безпеки та стійкості критичної інфраструктури, яка забезпечує життєво важливі для країни функції та послуги, а також завдання суб'єктам управління в цій сфері, а саме:

- секторальним органам з питань захисту КІ – щодо розроблення планів взаємодії та підтримання ЖВФ на випадок порушення функціонування об'єктів критичної інфраструктури;

- місцевим органам виконавчої влади – щодо розроблення та затвердження місцевих програм забезпечення безпеки та стійкості КІ, програм підвищення стійкості територіальних громад до кризових ситуацій, спричинених припиненням або погіршенням надання важливих для їхньої життєдіяльності життєво важливих функцій.

Такі завдання є серйозним викликом для суб'єктів управління через ускладнення аналізу та регулювання діяльності в зазначеній сфері. Крім іманентної динаміки зовнішнього середовища функціонування визначеної сфери управління (системи, галузі економіки, громади тощо), потенційна змінність її внутрішньої будови та переліку ЖВФ потребує постійного аналізування зовнішнього та внутрішнього середовища життєдіяльності

визначеної сфери управління. Нерідко суб'єктам управління простіше визначити конкретний статичний об'єкт і реалізовувати звичну процедуру його захисту (наприклад, застосувати фізичну охорону мосту через річку), ніж забезпечувати стійкість функції, реалізацію якої забезпечує такий об'єкт (зокрема, транспортне сполучення між берегами, що може здійснюватися за допомогою різних інфраструктурних об'єктів та різними способами).

Саме ця обставина зумовлює вимогу трансформації підходів щодо діяльності суб'єктів, залучених до забезпечення стійкості визначеної сфери управління. При акцентуванні уваги на стійкості надання визначеної послуги / функції суб'єкт управління має значно розширити сфери аналізу, аби мати можливість залучати ширший набір ресурсів і механізмів управління та забезпечити розвиток власних спроможностей відповідно до рівня завдань. Водночас варто розуміти, що суб'єкти управління повинні намагатися досягти чіткого усвідомлення мети та змісту управлінських дій з питань забезпечення стійкості їхньої сфери управління, яке поки що не сформоване. Спостерігаються лише перші спроби окреслити розуміння змісту практичних дій та способів їх формалізації, а практична діяльність інституцій, обов'язком яких є вирішення завдань щодо забезпечення стійкості визначеної сфери управління, в Україні тільки розпочинається.

Ця аналітична доповідь є продовженням попередніх досліджень з питань безпеки та стійкості критичної інфраструктури. У публікації запропоновано концептуальні засади та методологічні підходи щодо формалізації діяльності й розроблення необхідних інструментів забезпечення стійкості функціонування КІ та надання ЖВФ.

Перший розділ присвячено огляду політики й законодавства США, Великої Британії, ЄС та України з питань безпеки та стійкості КІ, що є елементом політики забезпечення національної стійкості та/чи національної готовності до надзвичайних ситуацій. Розглянуто особливості законодавства США, яке стосується регулювання діяльності з питань стійкості функції енергозабезпечення, зокрема на місцевому рівні. Подано узагальнення підходів щодо планування заходів безпеки та стійкості КІ та ЖВФ у різних країнах.

У другому розділі висвітлено основні складники діяльності суб'єктів забезпечення безпеки та стійкості КІ, а також зміст управлінських дій, які застосовуються залежно від етапу циклу реагування на ймовірну кризову ситуацію. Розроблено концептуальну модель формалізації вимог щодо стійкості надання ЖВФ. Проведено огляд практики реагування на порушення функціонування критичної енергетичної інфраструктури.

У третьому розділі схарактеризовано завдання та зміст діяльності суб'єктів планування стійкості функціонування КІ. На прикладі планування

заходів щодо стійкості енергозабезпечення життєдіяльності громад продемонстровано, як варто використовувати запропоновані підходи.

Четвертий розділ видання ознайомлює із загальними принципами та базовими вимогами щодо розроблення плану стійкості життєдіяльності громади. Подано опис змісту плану стійкості за циклом кризового реагування, уміщено приклади орієнтовного змісту й структури плану стійкості енергозабезпечення громад.

Зміст аналітичної доповіді спрямований на те, щоб допомогти суб'єктам управління опанувати основні засади концепту стійкості, мету й зміст управлінських дій з питань стійкості функціонування критичної інфраструктури та надання ЖВФ, а відтак розпочати практичну діяльність із досягнення цілей, визначених законодавством.

Це видання стане в пригоді під час формування цілей досягнення національної стійкості в різних сферах управління, розроблення формалізованих інструментів планування та практичного інструментарію регламентування діяльності суб'єктів реагування задля забезпечення стійкості функціонування визначених сфер управління.

Розділ 1. СТІЙКІСТЬ КРИТИЧНОЇ ІНФРАСТРУКТУРИ У СИСТЕМІ НАЦІОНАЛЬНОЇ СТІЙКОСТІ

1.1. Огляд політики та законодавства окремих країн з питань безпеки та стійкості критичної інфраструктури

Розвиток законодавства Сполучених Штатів Америки

Сполучені Штати Америки (США) мають значний досвід у створенні цілісних систем забезпечення національної безпеки, безперервності урядування, національної готовності й реагування у випадку виникнення кризових ситуацій.

Однією із систем, що охоплює всі аспекти життєдіяльності країни, є Національна система готовності США (The National Preparedness System¹). Її функціональне призначення – окреслити завдання та формалізувати процеси щодо забезпечення готовності всіх можливих учасників до спільної та координованої діяльності, аби домогтися сталого розвитку всього суспільства задля досягнення національної цілі – готовності до виникнення кризових ситуацій.

Загальне визначення мети цієї системи таке²: безпечна та стійка нація, яка володіє спроможністю на основі залучення зусиль усього суспільства *запобігати, захищати, пом'якшувати, реагувати та відновлюватися* після загроз і небезпек³, які становлять найбільший ризик.

Національна система готовності США з метою формування стійкості країни до всіх видів загроз та небезпек визначає в масштабах усього суспільства (whole community approach⁴) завдання щодо організації діяльності членів суспільства та інституцій з підготовки до виникнення кризових ситуацій, дій під час криз і відновлення після них, а також відображення цілей готовності та завдань у системі управлінських рішень різного рівня.

¹ National Preparedness System. URL: <https://www.fema.gov/emergency-managers/national-preparedness/system>

² Див.: URL: <https://www.fema.gov/emergency-managers/national-preparedness/goal>

³ Тут і далі будемо розрізняти терміни «небезпека» і «загроза» за критерієм наявності чи відсутності суб'єкта, що їх спричиняє. У випадку «небезпеки» суб'єкт не є чітко вираженим (наприклад, природні катаклізми чи технологічні аварії). Коли йдеться про «загрозу», то суб'єкт може бути ідентифікований (наприклад, особа, яка здійснила терористичний акт). Таке смислове розмежування зумовлює різні методи оперування термінами під час ідентифікації, оцінювання впливу, а також способів реагування на події, спричинені загрозами чи небезпеками. Водночас для цілей забезпечення стійкості функціонування КІ таке розмежування не є принциповим, про що детальніше йдеться далі.

⁴ Див.: URL: <https://www.fema.gov/glossary/whole-community>

Визначено Національну ціль готовності (The National Preparedness Goal⁵), що складається із 32 основних спроможностей (capabilities), набуття яких кожним членом суспільства та інституціями дозволить забезпечити стале функціонування країни навіть в умовах кризи.

Для визначення найбільш критичних загроз⁶ запроваджено періодичне оцінювання безпекового середовища та ризиків нації. Стратегічну оцінку національного ризику (The Strategic National Risk Assessment, SNRA)⁷ було започатковано на виконання політичної директиви президента США (PPD-8)⁸ у 2011 р., яка, власне, і започаткувала створення Національної системи готовності США.

Директива PPD-8 вимагала від Міністерства внутрішніх справ (Department of Homeland Security, DHS)⁹ проведення стратегічної оцінки національного ризику¹⁰, щоб допомогти визначити типи інцидентів, які становлять найбільшу загрозу національній безпеці. Відповідна оцінка ризику, яка проводиться, допомагає підвищити рівень усвідомлення всіх залучених суб'єктів щодо¹¹:

- визначення загроз та оцінювання ризиків, а також ідентифікації чинників, котрі сприяють розвитку основних спроможностей країни, що впливають на досягнення цільових показників готовності;

- підтримки розвитку спільного мислення (узгодженого розуміння) щодо стратегічних потреб і встановлення вимог до діяльності на всіх етапах циклу реагування: запобігання, захисту, пом'якшення наслідків, реагування та відновлення;

- розвитку спроможності на всіх урядових рівнях розуміти й усвідомлювати національні загрози та небезпеки і пов'язані з цим ризики, щоб забезпечити готовність і спроможність діяти незалежно, але спільно.

Згодом методологія проведення оцінки ризиків національного рівня розвивалась з урахуванням розширеного спектра загроз та уточнення методів оцінювання ризиків. Національний аналіз загроз і небезпек та оцінка ризиків

⁵ National Preparedness Goal. Second Edition. September 2015. URL: https://www.fema.gov/sites/default/files/2020-06/national_preparedness_goal_2nd_edition.pdf

⁶ Перелік загроз, що увійшли до SNRA, подано в *додатку 1*.

⁷ U.S. Department of Homeland Security. (2011). The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation. URL: <https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf>

⁸ Presidential Policy Directive on National Preparedness (PPD-8). March, 2011. URL: <https://www.dhs.gov/xlibrary/assets/presidential-policy-directive-8-national-preparedness.pdf>

⁹ The Department of Homeland Security. <https://www.dhs.gov/>

¹⁰ DHS розуміє «ризик» як потенціал для небажаного результату в результаті інциденту чи події, що визначається його ймовірністю та пов'язаними наслідками (*див.*: URL: https://emilms.fema.gov/is_0360/groups/224.html).

¹¹ The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation. URL: <https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf>

(The National Threat and Hazard Identification and Risk Assessment, THIRA)¹² забезпечує ідентифікацію не тільки загроз і небезпек¹³ та оцінку ризиків для нації, але й визначає цільові показники готовності та спроможності керувати ними¹⁴.

У рамках реалізації завдань Національної системи готовності США функціонує Національна система управління інцидентами (The National Incident Management System, NIMS)¹⁵, яка забезпечує координацію зусиль державних інституцій усіх рівнів державного управління, неурядових організацій та приватного сектору для спільного запобігання, захисту, пом'якшення, реагування та відновлення після інцидентів. NIMS надає всім залученим учасникам термінологічне, організаційне та методологічне забезпечення для успішного впровадження заходів реагування на кризові ситуації.

Також NIMS формує систему взаємодії різних юрисдикцій та інституцій з метою спільного використання ресурсів, координації та управління інцидентами, організації обміну інформацією. Загалом NIMS виокремлює п'ять рівнів складності інциденту (Tier 1 to 5)¹⁶, відповідно до яких встановлює вимоги (та індикатори) щодо спроможності залучених учасників узгоджено реагувати на загрози будь-якого типу й кризові ситуації будь-якого рівня складності.

Складником Національної системи готовності є система безперервності урядування. Директива президента США (PPD-40)¹⁷ зобов'язала органи

¹² National Risk and Capability Assessment. URL: <https://www.fema.gov/emergency-managers/national-preparedness/goal/risk-capability-assessment#thira>

¹³ Для цілей THIRA загрози та небезпеки (threats and hazards) поділяються на *три категорії*: природні небезпеки: природні явища; технологічні небезпеки (аварії або відмови систем і споруд); інциденти, спричинені людиною – навмисні дії противника.

¹⁴ 2019 National Threat and Hazard Identification and Risk Assessment (THIRA). Overview and Methodology. URL: https://www.fema.gov/sites/default/files/2020-06/fema_national-thira-overview-methodology_2019_0.pdf

¹⁵ The National Incident Management System. URL: <https://www.fema.gov/emergency-managers/nims>

¹⁶ Індекс складності інциденту визначається рівнем труднощів, тяжкості або загального опору, з яким стикається персонал з управління інцидентами або допоміжний персонал, намагаючись керувати чи підтримувати інцидент до успішного завершення або керувати одним типом інциденту чи події порівняно з іншим типом.

Рівень складності (Tier 1–5) – це сукупність факторів, що впливають на ймовірність контролю над інцидентом. Складність інциденту визначають, ураховуючи багато факторів, включно такі (але не обмежуючись ними): географічні межі (територія) впливу; рівень загрози життю та майну; політична чутливість щодо реагування; організаційна складність; юрисдикційні межі; цінності, які наражаються на ризик; погода під час реагування; стратегія і тактика дій; політика суб'єктів реагування; тип створеної впливом загрози ситуації – звична (рутинна) чи надзвичайна.

Під час прийняття рішень щодо рівня управління інцидентами враховують складність останніх. Наприклад, яким чином можна врегулювати інцидент, що виник: на місцевому рівні чи він потребує залучення ресурсів федерального рівня. Складність інциденту залежно від його типу оцінюється за п'ятибальною шкалою: від 5 – найменш складний інцидент до 1 – найскладніший тип інциденту (*див.*: Incident Complexity Guide Planning, Preparedness and Training. URL: <https://www.fema.gov/sites/default/files/documents/nims-incident-complexity-guide.pdf>).

¹⁷ Presidential Policy Directive on National Continuity Policy – 40 (PPD-40). July, 2016. Директива не є відкритим документом. Принципові її положення відображені в Керівництві щодо Стійкості (*див.*: Continuity Guidance Circular. URL: <https://www.fema.gov/emergency-managers/national-preparedness/continuity/circular>).

державної влади США підтримувати спроможність безперервно виконувати основні національні функції (National Essential Functions, NEFs)¹⁸. Уже сформовано чітку ієрархічну систему визначення відповідальності та завдань органів державної влади із забезпечення стійкості надання основних національних функцій¹⁹, у якій передбачено також залучення до діяльності недержавних суб'єктів. Керівники органів державної влади зобов'язані інтегрувати свої окремі програми готовності в повсякденну діяльність інституцій – виконання найважливіших функцій (Primary Mission Essential Functions, PMEFS)²⁰, щоб забезпечити надання визначених національних функцій за будь-яких умов. Наприклад, Міністерство енергетики США (Department of Energy, DOE) на підтримку національної функції «Забезпечення кризового реагування» (NEF 6 – Provide Emergency Response / Recovery) має виконувати функцію «Менеджмент енергетичної інфраструктури» (DOE # 3: Manage Energy Infrastructure)²¹.

Іншим складником Національної системи готовності є система забезпечення надання важливих для суспільства функцій у надзвичайних ситуаціях (Emergency Support Functions, ESF). Прикладом такої функції у сфері енергетики є ESF # 12 – «Енергія»²², яка визначає специфіку завдань для Міненерго США щодо забезпечення енергопостачання споживачів у кризових ситуаціях.

Орієнтування суб'єктів на забезпечення стійкості ЖВФ є важливою віхою в еволюції підходів США до управління у галузі національної безпеки. Діяльність з питань безпеки і стійкості КІ також узгоджується із загальною політикою, спрямованою на забезпечення національної готовності до криз.

Безпосередньо у сфері забезпечення захисту КІ одним із основних актів законодавства є Директива президента США щодо безпеки та стійкості критичної інфраструктури (PPD-21)²³. У цьому документі визначено загальну

¹⁸ National Essential Functions. URL: https://www.fema.gov/sites/default/files/2020-07/fema_continuity-brochure_050720_1.pdf

¹⁹ Federal Continuity Directive 1 (FCD 1). URL: <https://www.fema.gov/pdf/about/org/ncp/fcd1.pdf>

²⁰ Primary Mission Essential Functions. URL: <https://www.dhs.gov/publication/primary-mission-essential-functions-pmefs-department>

²¹ DOE # 3 – «Менеджмент енергетичної інфраструктури»: безперервний моніторинг та управління національною енергетичною інфраструктурою, у т. ч. управління стратегічним запасом нафти та/або запасом Північно-Східного резерву мазуту для систем тепlopостачання житла, реагування на збої в енергетичній інфраструктурі для забезпечення швидкого відновлення енергопостачання. Ця функція спрямована на виконання 6-ї та 8-ї функцій із переліку NEFs (див.: URL: https://www.dhs.gov/sites/default/files/publications/list_of_validated_pmefs_by_department_v2_fema.pdf).

²² Emergency Support Function #12 – Energy Annex. URL: https://www.fema.gov/sites/default/files/2020-07/fema_ESF_12_Energy-Annex.pdf

²³ Presidential Policy Directive Critical Infrastructure Security and Resilience (PPD-21). February 12, 2013. URL: <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>

рамку організації узгодженої діяльності країни щодо зміцнення й підтримання на федеральному рівні безпеки та стійкої КІ.

Директива містить три *основні стратегічні цілі*, що стосуються:

1) визначення функціональних взаємозв'язків в уряді для просування національної єдності зусиль щодо посилення безпеки та стійкості КІ;

2) забезпечення ефективного обміну інформацією шляхом визначення базових даних та системних вимог до діяльності федерального уряду в цій сфері;

3) упровадження функції інтеграції та аналізу для інформування про планування та оперативні рішення щодо забезпечення безпеки і стійкості КІ.

Також PPD-21 визначає відповідальним за реалізацію політики безпеки та стійкості критичної інфраструктури Міністерство внутрішніх справ (Department of Homeland Security, DHS) та окремі органи влади у конкретних секторах КІ США (Sector-Specific Agencies)²⁴. У цій Директиві наголошено на важливості залучення власників та Операторів КІ до здійснення «проактивних кроків для управління ризиками та зміцнення безпеки та стійкості критичної інфраструктури країни, ураховуючи всі види небезпек, які можуть мати негативний вплив на національну безпеку, економічну стабільність, громадське здоров'я та безпеку, або будь-яку їх комбінацію».

Конкретизовано цілеспрямованість такої діяльності: «Зусилля мають бути спрямовані на зменшення вразливості, мінімізацію наслідків, виявлення та усунення загроз, а також прискорення реагування та відновлення критичної інфраструктури».

У структурі DHS створено відповідний підрозділ – Агентство з кібербезпеки та безпеки інфраструктури (Cybersecurity and Infrastructure Security Agency, CISA)²⁵. На CISA покладено завдання з імплементації політики у сфері безпеки та стійкості КІ, а також і щодо координації національних зусиль. Мета – усвідомлення, управління та зменшення ризиків для найбільш важливої інфраструктури США.

У 2019 р. CISA запровадило інструмент національних критичних функцій (National Critical Functions, NCF)²⁶, які надаються / забезпечуються завдяки сталому функціонуванню КІ країни. Саме на забезпечення безперервності надання переліку національних критичних функцій спрямовується діяльність органів державної влади США, визначених відповідальними за захист

²⁴ У США визначено 16 секторів критичної інфраструктури. URL: <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>

²⁵ Див.: URL: <https://www.cisa.gov/>

²⁶ *Національні критичні функції* (National Critical Functions, NCF) – це функції, порушення чи дисфункція яких справлятимуть суттєвий негативний вплив на безпеку, національну економічну безпеку, національну громадську охорону здоров'я чи безпеку або будь-яку їх комбінацію (див.: URL: <https://www.cisa.gov/national-critical-functions>).

критичної інфраструктури країни. Проведення ризик-аналізу порушення таких функцій дає змогу точно встановити національну КІ, котра потребує захисту²⁷.

Запровадження інструменту NCF також відображає новий етап еволюції системи забезпечення захисту КІ, а саме: визначення основною метою діяльності в цій сфері забезпечення стійкості надання ЖВФ та акцентування уваги на важливості управління ризиками. Управління ризиками надання NCF²⁸ формує спроможність визначати пріоритетність національних зусиль за окремими напрямками, одночасно забезпечуючи узгодження зусиль усіх залучених до реагування учасників.

Розвиток законодавства Європейського Союзу

Європейський Союз (ЄС), усвідомлюючи нові виклики та загрози, у т. ч. спричинені широкомасштабною воєнною агресією РФ проти України, також посилив політику у сфері стійкості надання ЖВФ та функціонування критичної інфраструктури²⁹.

Дискусія, що відбулась у ЄС на фаховому та вищому політичному рівні, знайшла відбиття в Рекомендаціях, спрямованих на посилення зусиль Євросоюзу з підвищення стійкості критичної інфраструктури, які Рада ЄС прийняла в грудні 2022 р.³⁰. Ці Рекомендації фактично зафіксували нову мету політики ЄС в цій сфері, яка полягає у формуванні спроможності держав-членів підвищити стійкість щодо надання основних послуг на внутрішньому ринку, тобто послуг, котрі мають вирішальне значення для підтримки життєво важливих суспільних функцій, економічної діяльності, громадського здоров'я та безпеки чи навколишнього середовища у ЄС.

Пріоритетами нової політики є розроблення необхідних інструментів, забезпечення узгоджених зусиль і координації дій на рівні ЄС з підвищення готовності до та реагування на безпекові інциденти, що загрожують порушенню функціонування КІ та надання ЖВФ.

²⁷ Загалом виокремлено 55 таких національних критичних функцій, які поєднані у чотири групи: зв'язок та обмін інформацією (connect); розподілення (distribute); управління (manage); постачання (supply).

²⁸ Серед основних елементів такої системи зазначено: регулярне оцінювання загроз та ризиків критичної інфраструктури; формування Реєстру ризиків (The Risk Register); здійснення аналізу взаємозалежності критичної інфраструктури та критичних функцій (NCF); моделювання впливу загроз та ідентифікація сценаріїв, що потенційно можуть призвести до порушення надання критичних функцій на національному рівні; формування планів забезпечення безперервності надання критичних функцій на різних рівнях управління (секторальні плани, плани штатів, місцеві плани).

²⁹ Суходоля О. Стійкість критичної інфраструктури ЄС: посилення політики та координації : аналіт. зап. Серія «Національна безпека». Київ : НІСД, 2023. URL: <https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/stiykist-krytychnoyi-infrastruktury-yes-posylennya-polityky-ta>

³⁰ COUNCIL RECOMMENDATION on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure. Brussels, 9 December 2022 (OR.en) 15623/22. URL: <https://data.consilium.europa.eu/doc/document/ST-15623-2022-INIT/en/pdf>

У рамках заходів щодо підвищення готовності Євросоюзу до кризових ситуацій держави – члени ЄС повинні:

- застосовувати методологію оцінювання ризиків³¹ КІ на основі аналізу впливу загроз будь-яких типів (all-hazard approach), урахуваючи подальшу адаптацію національних підходів;

- розпочати розроблення заходів щодо підвищення стійкості КІ відповідно до положень новоприйнятих законодавчих документів у цій сфері, особливо акцентуючи увагу на співпраці та обміні відповідною інформацією між державами-членами та Єврокомісією, виявленні КІ транскордонного характеру та посиленні підтримки Операторів КІ для забезпечення стійкості такої критичної інфраструктури;

- розвивати національні механізми координації залучених акторів у процесі реагування, забезпечити підготовку оглядів міжсекторального реагування на суттєві збої в основних послугах, які надаються завдяки КІ. Започаткувати розроблення плану скоординованого реагування на порушення роботи КІ зі значним транскордонним значенням;

- заохочувати Операторів КІ та відповідні національні органи влади збільшувати свої спроможності, щоб мати можливість швидко відновити ЖВФ, надання яких ці оператори забезпечують;

- заохочувати та підтримувати Операторів КІ проводити стрес-тести (передусім в енергетичному секторі), під час реконструкції своєї інфраструктури будувати її так, щоб забезпечити максимальну стійкість до повного спектра ризиків, беручи до уваги пропорційність заходів реагування стосовно оцінки ризику та витрат;

- утілювати в життя заходи, спрямовані на усвідомлення відповідними зацікавленими сторонами необхідності підвищення стійкості критичної інфраструктури.

Хоча основну відповідальність за забезпечення безпеки КІ покладено на членів Євросоюзу, посилення координації на рівні ЄС визнано необхідним, особливо у світлі загроз, які можуть вплинути на декілька держав-членів одночасно. Тому сформульовано завдання: запроваджувати низку механізмів щодо координації в рамках ЄС між країнами-членами.

Наприкінці 2022 р. прийнято нову Директиву ЄС щодо стійкості критичних суб'єктів³² (CER Directive)³³, натомість попередня

³¹ *Оцінка ризику* – це загальний процес визначення характеру та масштабу ризику завдяки виявленню та аналізуванню потенційних відповідних загроз, уразливостей і небезпек, котрі можуть призвести до інциденту, а також у спосіб оцінювання потенційних втрат або збоїв у наданні основної послуги, які цей інцидент спричинив.

³² Під *критичними суб'єктами* (critical entities) розуміємо Операторів надання життєво важливих послуг, відповідно до термінології, визначеної законодавством України у сфері захисту критичної інфраструктури.

Директива 2008/114/ЄС щодо ідентифікації КІ була анульована. У новій Директиві акценти дещо зміщено: з «ідентифікації КІ та встановлення вимог щодо її захисту» до «забезпечення стійкості суб'єктів, що надають життєво важливі функції / послуги»³⁴.

Директива CER встановлює загальну рамку забезпечення стійкості надання ЖВФ суб'єктами, які експлуатують КІ (далі – Операторів КІ)³⁵, встановлює вимоги до країн ЄС щодо стійкості надання ЖВФ, запроваджує механізми взаємодії між Операторами КІ та уповноваженими державними органами на національному рівні, визначає повноваження Єврокомісії щодо координації національних зусиль та інституцій ЄС на рівні Союзу з метою забезпечення стійкості функціонування КІ.

Зокрема, Директива CER встановлює вимогу до кожної країни – члена ЄС прийняти на національному рівні Стратегію підвищення стійкості роботи Операторів КІ, які забезпечують надання життєво важливих послуг. Кожна розроблена Стратегія повинна містити певні складові частини, серед яких:

- стратегічні цілі та пріоритети підвищення стійкості Операторів КІ, беручи до уваги транскордонні й міжгалузеві залежності та взаємозалежності;
- опис заходів, необхідних для підвищення стійкості Операторів КІ, включно з оцінюванням ризиків забезпечення надання ЖВФ;
- опис процесу підтримки Операторів КІ, включно й заходи щодо посилення державно-приватного партнерства (ДПП);
- засади координації між уповноваженими органами країн – членів ЄС з реагування на загрози різного виду.

Встановлюються вимоги щодо проведення країнами-членами ризик-аналізу стійкості надання ЖВФ (щонайменше один раз на чотири роки) відповідно до вказаного переліку визначеного додатком до Директиви. Аналіз ризиків має враховувати загрози будь-якого типу. Крім того, враховувати загрози міжсекторального й транскордонного характеру, зокрема сформовані в третіх країнах, оцінювати їх негативний вплив на життєдіяльність громадян та внутрішній ринок ЄС. При аналізуванні ризиків Оператор КІ також має здійснювати оцінку впливу загроз усіх видів і враховувати залежність інших секторів КІ від послуг / функцій, які цей Оператор КІ забезпечує, чи залежність роботи цього Оператора КІ від функцій / послуг інших секторів.

³³ DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities and repealing Council Directive 2008/114/EC. Brussels, 30 November 2022 (OR.en) PE-CONS 51/22. URL: <https://data.consilium.europa.eu/doc/document/PE-51-2022-INIT/en/pdf>

³⁴ Суходоля О. Нова директива ЄС щодо стійкості критичної інфраструктури (CER DIRECTIVE): аналіт. зап. Серія «Національна безпека». Київ: НІСД, 2023. URL: <https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/nova-dyrektyva-yes-shchodo-stiykosti-krytychnoyi-infrastruktury>

³⁵ *Стійкість* – це здатність Оператора КІ запобігати, захищати, реагувати, протистояти, пом'якшувати, поглинати, пристосовуватись і відновлюватись після інциденту.

Директива CER вимагає від країн ЄС забезпечити застосування Операторами КІ належних та адекватних рівню загроз технічних, безпекових та організаційних заходів щодо забезпечення стійкості КІ, зокрема й тих, що необхідні для:

- запобігання виникненню інцидентів, ураховуючи заходи щодо зменшення впливу природних катастроф та адаптації до зміни клімату;
- забезпечення належного фізичного захисту приміщень та інфраструктури (наприклад, огорожі, бар'єри, інструменти та процедури моніторингу периметра, обладнання виявлення та контролю доступу);
- реагування на інциденти, протистояння їм і пом'якшення їхніх наслідків, ураховуючи впровадження процедур і протоколів управління ризиками та кризовими ситуаціями, а також процедур оповіщення;
- відновлення після інцидентів, ураховуючи заходи забезпечення безперервності бізнесу та визначення альтернативних ланцюгів постачання, щоб відновити надання ЖВФ;
- підвищення обізнаності персоналу, належним чином ураховуючи навчальні курси, інформаційні матеріали та навчання.

Країни ЄС мають забезпечити застосування Операторами КІ *планів стійкості*, які охоплюють вищенаведені заходи. У процесі моніторингу виконання вимог цієї Директиви уповноважені органи країн ЄС визначають адекватність та відповідність встановленим вимогам планів стійкості Операторів КІ.

З метою створення єдиних методичних підходів щодо проведення аналізу ризиків у Директиві CER подано *критерії оцінки суттєвого негативного ефекту* (Significant Disruptive Effect) впливу загроз на стійкість роботи Оператора КІ. Зокрема, треба враховувати:

- кількість користувачів, які покладаються на основні послуги, які відповідний суб'єкт надає;
- ступінь залежності інших секторів і підсекторів від відповідної основної послуги;
- вплив, який інциденти можуть спричинити з огляду на їхній ступінь і тривалість на економічну та суспільну діяльність, навколишнє середовище, громадську безпеку та безпеку або здоров'я населення;
- ринкову частку суб'єкта господарювання на ринку відповідної основної послуги або основних послуг (ЖВФ);
- географічну територію, яка може постраждати від інциденту, у т. ч. будь-який транскордонний вплив, зважаючи на вразливість, пов'язану зі

ступенем ізоляції певних типів географічних територій, як-от острівні регіони, віддалені регіони або гірські райони;

– важливість суб'єкта у підтримці необхідного рівня основних послуг, беручи до уваги наявність альтернативних засобів для надання таких основних послуг.

Країни надають підтримку Операторам КІ у зусиллях із підвищення їх стійкості, сприяють добровільному обміну інформацією щодо визначених Директивою завдань, можуть надавати фінансову допомогу Операторам КІ у випадках, коли це необхідно та обґрунтовано суспільними інтересами.

Директива CER запроваджує низку інструментів *моніторингу готовності та стійкості Операторів КІ до реалізації загроз* порушення ЖВФ. Одним із таких інструментів є організація Єврокомісією *консультативних місій* (advisory missions) для надання рекомендацій Операторам КІ в частині виконання положень Директиви. Консультативна місія протягом трьох місяців після завершення місії повідомляє про свої висновки щодо результатів оцінки Єврокомісією та країну ЄС. Єврокомісія, ґрунтуючись на результатах місії, повідомляє свою думку відповідній країні ЄС та Оператору КІ щодо того, чи виконують вони заходи, які можуть бути вжиті для підвищення стійкості роботи такого Оператора КІ. Країна ЄС має забезпечити, щоб його уповноважений орган і відповідний Оператор КІ враховували надані рекомендації й надавали інформацію Єврокомісії та державам-членам про заходи, які були реалізовані відповідно до такого висновку.

Директива CER запроваджує *механізм обміну інформацією та кращим досвідом* серед країн ЄС, Операторів КІ та інших залучених інституцій. Зокрема, створюється Група стійкості Операторів КІ, завданням якої визначено підтримку Єврокомісії, сприяння співпраці між країнами – членами ЄС та обміну інформацією з питань стійкості надання ЖВФ, а саме:

– підтримку Єврокомісії в наданні допомоги державам-членам у зміцненні їхньої спроможності сприяти стійкості Операторів КІ;

– сприяння обміну найкращими практиками стосовно ідентифікації Операторів КІ державами-членами, обміну інформацією щодо ризиків та інцидентів та інформацією і найкращими практиками щодо інновацій, досліджень і розробок, пов'язаних із стійкістю КІ;

– сприяння підготовці методичних рекомендацій;

– обмін інформацією з питань, що стосуються стійкості Операторів КІ, з відповідними інституціями, органами, службами та агентствами ЄС.

Варто зазначити, що політика ЄС та НАТО щодо забезпечення безпеки і стійкості КІ була взаємоузгоджена. На початку 2023 р. було оголошено про синхронізацію зусиль між ЄС та НАТО щодо стійкості критичної

інфраструктури³⁶. Також створена спільна Група з питань стійкості й захисту КІ, яка підготувала звіт щодо пріоритетів співробітництва між інституціями ЄС та НАТО в частині забезпечення безпеки функціонування європейської КІ та координації зусиль, спрямованих на посилення стійкості ЖВФ³⁷. НАТО та ЄС наголошують, що продовжуватимуть працювати над тим, щоб зробити КІ, технології й ланцюги постачань стійкішими до загроз і ризиків, що постійно змінюються, на основі паралельних і скоординованих оцінок, а також уживати заходів для пом'якшення потенційної вразливості.

Фактично прийняті рішення зафіксували новий етап розвитку політики ЄС у сфері захисту КІ. Підвищення стійкості КІ як національної, так і європейської, визнано серед пріоритетних напрямів безпекової політики ЄС, яка буде реалізовуватись у щільній співпраці з НАТО й третіми країнами, зокрема Україною, які залучені до розвитку транскордонної інфраструктури з європейськими країнами та беруть участь у забезпеченні сталості функціонування ланцюжків постачання.

Розвиток законодавства Великої Британії

Поточні виклики стосовно забезпечення національної безпеки та вивчені уроки кризового реагування зумовили зміни в політиці Великої Британії³⁸.

Основи державної політики Великої Британії у сфері готовності до реагування на кризові ситуації закладені 2004 р. законом «Про цивільні непередбачувані обставини» (The Civil Contingencies Act, CCA)³⁹. Цей документ закладає основу для розвитку системи цивільної готовності до надзвичайних ситуацій, визначає механізми роботи різних відомств на національному й місцевому рівнях та дозволяє урядові країни ухвалювати тимчасове законодавство під час виникнення надзвичайних ситуацій.

Уряд Великої Британії, ураховуючи результати досвіду реалізації цього закону та сучасні виклики й загрози функціонуванню КІ, визначив пріоритетні напрями посилення спроможностей країни з питань стійкості її життєдіяльності. Передусім це посилення відповідальності та встановлення чіткої підзвітності за міжвідомчі дії, які проводяться на місцевому рівні на різних етапах циклу

³⁶ НАТО і ЄС домовились створити Спеціальну групу з питань стійкості і захисту критичної інфраструктури. 2023. 11 Jan. URL: https://www.nato.int/cps/en/natohq/news_210611.htm?selectedLocale=uk

³⁷ EU-NATO Task Force on the Resilience of Critical Infrastructure: Final Assessment Report. URL: [https://commission.europa.eu/system/files/2023-06/EU-NATO_Final %20Assessment %20Report %20Digital.pdf](https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf)

³⁸ Лепіхов А. Нові підходи Великої Британії до забезпечення національної стійкості: аналіт. зап. Серія «Національна безпека». Київ: НІСД, 2023. URL: <https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/novi-pidkhody-velykoyi-brytaniyi-do-zabezpechennya-natsionalnoyi>

³⁹ The Civil Contingencies Act (UK). URL: <https://www.legislation.gov.uk/ukpga/2004/36/contents>

кризового реагування та встановлення зобов'язувальних стандартів стійкості щодо діяльності суб'єктів та інституцій, залучених до реагування.

Наприкінці 2022 р. було оприлюднено Рамкову концепцію національної стійкості (UK Government Resilience Framework)⁴⁰, мета якої – підвищення спроможностей країни *передбачати, оцінювати, запобігати, пом'якшувати, реагувати та відновлюватися після відомих, невідомих, прямих, непрямих і нових ризиків стійкості життєдіяльності суспільства*. У Рамковій концепції наголошується, що побудова стійкої нації вимагає докладання зусиль на всіх етапах циклу кризового реагування та усвідомленої уваги залучених учасників до різних аспектів забезпечення стійкості.

Рамковою концепцією передбачається, що Оцінка ризиків національній безпеці (National Security Risk Assessment, NSRA) залишатиметься основним інструментом для оцінки найсерйозніших ризиків. NSRA дозволяє урядові Великої Британії оцінити, порівняти найвищі ризики національного рівня, з якими стикається країна, та зосередити зусилля всіх залучених учасників на визначених пріоритетах. Задля того, щоб поінформувати широке коло учасників про основні висновки щодо оцінки ризиків, буде й надалі розроблятися Національний реєстр ризиків (National Risk Register, NRR)⁴¹.

Передбачається, що NRR⁴² зберігатиме функцію інструмента відкритого характеру стосовно основних загроз та ризиків для допомоги суб'єктам, які мають законодавчо визначені зобов'язання у сфері реагування на випадок надзвичайних ситуацій на національному та місцевому рівнях. Національний реєстр ризиків доповнюватимуть реєстри ризиків громад (Community Risk Register, CRR), створені на місцевому рівні. Базуючись на національних оцінках ризиків, CRR зосереджуються на ризиках, які є пріоритетними для певних громад. Розроблення й застосування CRR є відповідальністю визначених місцевих партнерів з питань стійкості, які, відповідно до САА, об'єднуються в рамках діяльності місцевих форумів стійкості (Local Resilience Forums, LRF)⁴³.

Місцеві форуми стійкості реалізують міжвідомчу модель планування готовності громад до виникнення кризових ситуацій та керують міжвідомчою діяльністю з реагування й відновлення через створення груп стратегічної координації та груп координації відновлення. Хоча LRF діють на основі механізму державно-приватного партнерства, проте законодавство (ССА та

⁴⁰ The UK Government Resilience Framework. December 2022. URL: <https://www.gov.uk/government/publications/the-uk-government-resilience-framework>

⁴¹ NRR містить інформацію про найбільш значні ризики, які можуть виникнути протягом наступних двох років і, відповідно, можуть мати широкий спектр впливу на Велику Британію (див.: National Risk Register. URL: <https://www.gov.uk/government/publications/national-risk-register-2020>).

⁴² National Risk Register. URL: <https://www.gov.uk/government/publications/national-risk-register-2020>

⁴³ Local Resilience Forums. URL: <https://www.gov.uk/government/publications/the-role-of-local-resilience-forums-a-reference-document>

урядові регуляторні акти) передбачає, що учасники реагування через LRF несуть колективну відповідальність за планування, підготовку та міжвідомчу взаємодію в процесі реагування на надзвичайні ситуації на місцевому рівні⁴⁴.

У Рамковій концепції оприлюднено наміри уряду Великої Британії підвищити спроможності та відповідальність місцевих форумів стійкості. Передбачається визначення завдань і повноважень керівника LRF та створення оплачуваної постійної посади для кваліфікованої та досвідченої особи, яка стане головним спеціалістом з питань стійкості (Chief Resilience Officer, CRO) для кожної сфери життєдіяльності. Відповідно, планується визначити механізми забезпечення CRO необхідними ресурсами та підтримкою, надати повноваження та запровадити важелі впливу, щоб об'єднати весь загальний стейкхолдерів для підвищення стійкості у відповідних сферах управління. Спеціалісти з питань стійкості надаватимуть звіти про свою діяльність виконавчим органам місцевої влади. Також будуть встановлені чіткі механізми забезпечення міжвідомчої діяльності на рівні LRF.

Для допомоги місцевим громадам уряд Великої Британії також запровадив Рамкову програму розвитку стійкості громад (Community Resilience Development Framework)⁴⁵. Посилені LRF та їхні партнери (інші стейкхолдери) і надалі відіграватимуть ключову роль у плануванні й реалізації заходів з реагування та відновлення. Водночас буде підтримуватися модель, за якої основним виконавцем завдань з реагування на визначені загрози й ризики будуть окремі секторальні органи влади (Lead Government Department, LGD), відповідальні за визначений сектор критичної інфраструктури. Секторальні органи з питань безпеки та стійкості функціонування КІ, яка забезпечує життєдіяльність громад, візьмуть на себе відповідальність за надання чітких вказівок LRF щодо реагування, забезпечуючи підтримку на місцевому рівні, якщо вона буде необхідна.

Уряд Великої Британії розробив окремий процедурний механізм щодо забезпечення координації залучених урядових інституцій та суб'єктів кризового реагування (The UK Government Concept of Operations, CONOPs)⁴⁶. Інструментом координації зусиль є спеціально створений координаційний центр (The Cabinet Office Briefing Rooms, COBR)⁴⁷. COBR є ключовим

⁴⁴ Докладно про особливості функціонування LRF відповідно до положень законодавства та проведення оцінювання ризиків у Великій Британії йдеться у монографії О. Резнікової (*див.*: Резнікова О. О. Національна стійкість в умовах мінливого безпекового середовища : монографія. Київ : НІСД, 2022. 532 с. С. 260–264; 271–275).

⁴⁵ Cabinet Office Community Resilience Development Framework. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/828813/20190902-Community_Resilience_Development_Framework_Final.pdf

⁴⁶ *Див.*: URL: <https://www.gov.uk/government/publications/the-central-government-s-concept-of-operations>

⁴⁷ *Див.*: URL: <https://ukdefencejournal.org.uk/the-cabinet-office-briefing-rooms-cobr-a-short-introduction-2/>

механізмом, за допомогою якого уряд Великої Британії реагує на ситуації, що вимагають термінового прийняття рішень.

Задля підтримки діяльності COBR у 2021 р. було створено Національний ситуаційний центр (The National Situation Centre, SitCen)⁴⁸, який за допомогою сучасних інформаційних технологій підвищує можливості аналізу та візуалізації даних для прийняття рішень⁴⁹. Загальною метою створення SitCen є отримання даних з різних джерел (приватний та державний сектори, також місцеві форуми стійкості та населення), необхідних для аналізу, та сприяння суб'єктам реагування під час кризової ситуації загальнодержавного рівня (ідентифікація загроз та оцінка ризиків, запобігання та підготовка до реагування, відновлення та вивчення уроків).

В основі спільних зусиль із забезпечення стійкості лежить ефективна співпраця уряду Великої Британії та власників і операторів, які управляють національною КІ⁵⁰. Багато з них уже мають високу обізнаність про ризики та плани щодо стійкості, проте уряд продовжуватиме працювати над підвищенням їхніх спроможностей, зокрема через стандартизацію процесів забезпечення стійкості функціонування КІ та надання ЖВФ. Насамперед уряд країни спиратиметься на стандарти стійкості для КІ, котрі вже існують в окремих секторах, водночас розвиватиме спільні гнучкі міжгалузеві стандарти, які мають забезпечити глибше загальне розуміння стійкості надання ЖВФ.

Національна комісія з інфраструктури (The National Infrastructure Commission)⁵¹ рекомендувала урядові опублікувати набір стандартів для основних послуг (передусім в енергетичному, водному, цифровому, автодорожньому та залізничному секторах КІ), які мають переглядатися та оновлюватися кожні п'ять років.

⁴⁸ SitCen розпочав роботу 30 вересня 2021 р. і вже встиг значно змінити швидкість збирання, аналізу та надання даних урядові. Під час надання уряду Великої Британії даних про широкомасштабне воєнне вторгнення Росії в Україну на початку 2022 р. SitCen діяв як центральний пункт збору інформації та аналізу наслідків для міжнародної та національної безпеки.

⁴⁹ Див.: URL: <https://www.telegraph.co.uk/news/2021/12/14/first-glimpse-inside-uks-new-white-house-style-crisis-situation/>

⁵⁰ У Великій Британії виокремлено 13 секторів критичної інфраструктури: зв'язок (підсектори: пошта, телекомунікації та мовлення); транспорт; цивільна ядерна промисловість; хімічна промисловість; оборона; енергетика; вода; харчування; служби екстреної допомоги (підсектори: поліція, пожежна служба, швидка допомога та Морська берегова охорона); охорона здоров'я; фінанси; уряд; космос. У кожному секторі є один або кілька галузевих органів влади – головні державні департаменти (LGD), які відповідають за сектор КІ (див.: URL: <https://www.npsa.gov.uk/critical-national-infrastructure-0>).

⁵¹ Див.: URL: <https://nic.org.uk/>

1.2. Забезпечення стійкості надання життєво важливих функцій / послуг: досвід США у сфері енергозабезпечення

Енергетичний сектор є виключно критичним для життєзабезпечення будь-якої країни, оскільки всі інші критичні сектори інфраструктури та спроможність країни забезпечити надання ЖВФ залежать від наявності електроенергії та/або палива для належного функціонування. Порухення функціонування критичної енергетичної інфраструктури може безпосередньо вплинути на безпеку та стійкість інших секторів КІ, громадську безпеку, функціонування економіки та на національну безпеку загалом.

Саме тому у виданні подальший аналіз дій суб'єктів забезпечення безпеки і стійкості функціонування КІ та надання ЖВФ буде здійснюватися на основі цільової функції «забезпечення споживачів електроенергією». Одночасно аналіз і визначення методологічних та організаційних засад планування стійкості функції / послуги «енергозабезпечення» базуватиметься на вивченні досвіду США (країни – лідера у сфері розвитку механізмів забезпечення безпеки та стійкості КІ) та України⁵² (країни, яка на момент підготовки дослідження набула найбільшого практичного досвіду з цього питання).

Зазначимо, що в США забезпечення стійкості надання ЖВФ базується на комплексі законодавчих актів різного управлінського рівня⁵³. Саме ці документи визначають високий рівень «зрілості» системи забезпечення стійкості КІ/ЖВФ, що дає змогу узгоджувати пріоритети діяльності та забезпечувати координацію дій різних суб'єктів реагування.

Організаційні й законодавчі аспекти забезпечення безпеки та стійкості енергетичної інфраструктури на національному рівні

Задля виконання президентської директиви щодо безпеки та стійкості критичної інфраструктури (PPD-21⁵⁴), Національного плану захисту критичної інфраструктури (National Infrastructure Protection Plan, NIPP⁵⁵) та рекомендацій

⁵² Суходоля О. Стійкість здійснення життєво важливих функцій: узагальнення досвіду реагування України на руйнування енергетичної інфраструктури : аналіт. зап. Серія «Національна безпека». Київ : НІСД, 2023. <https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/stiykist-zdiysnennya-zhyttyevo-vazhlyvykh-funktsiy-uzahalnennya>

⁵³ Це, зокрема, президентські директиви, закони федерального рівня та закони на рівні штатів, нормативні акти органів виконавчої влади (міністерств, агентств), добровільні та зобов'язальні акти галузевих асоціацій, корпоративні регламенти та процедури, а також низка рішень добровільного характеру, ухвалених у рамках різноманітних професійних чи громадських об'єднань.

⁵⁴ Див.: URL: <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>

⁵⁵ Див.: URL: <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/national-infrastructure-protection-plan-and-resources>

DHS розробляються секторальні плани (Sector-Specific Plans ⁵⁶), що відповідають специфіці функціонування КІ в окремих секторах та особливостям надання NCF.

У сфері енергетики затверджено Енергетичний секторальний специфічний план (2015) ⁵⁷, який визначає пріоритетні напрями розвитку спроможностей суб'єктів енергетичного сектору щодо забезпечення стійкості функції енергозабезпечення споживачів країни.

Міненерго США (Department of Energy, DOE) ⁵⁸ є секторальним відомством в енергетиці (зокрема, у сфері забезпечення споживачів електроенергією). Завдання, пов'язані із безпекою та стійкістю електроенергетичної інфраструктури, вирішує Офіс кібербезпеки, енергетичної безпеки та кризового реагування (Office of Cybersecurity, Energy Security, and Emergency Response, CESER) ⁵⁹, який є структурним підрозділом DOE та фокусується на підготовці до та реагування на загрози енергозабезпеченню потреб країни.

Так, цей підрозділ здійснює секторальну координацію й регулювання діяльності в цій сфері, задля чого ⁶⁰;

- виявляє та оцінює життєво важливу енергетичну інфраструктуру, готує рекомендації щодо зниження вразливостей;

- взаємодіє та здійснює обмін інформацією з приватним сектором енергетики, державними, місцевими органами влади, установами та громадськістю;

- надає рекомендації штатам і місцевим органам влади (територій) щодо забезпечення сталого енергозабезпечення ⁶¹ та підготовки місцевих планів гарантування енергозабезпечення (Energy Assurance Plans) ⁶²;

⁵⁶ Див.: URL: <https://www.cisa.gov/2015-sector-specific-plans>

⁵⁷ Див.: URL: <https://www.cisa.gov/publication/nipp-ssp-energy-2015> ; <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf>

⁵⁸ Див.: URL: <https://www.energy.gov/> ; <https://www.energy.gov/offices>

⁵⁹ Див.: URL: <https://www.energy.gov/ceser/office-cybersecurity-energy-security-and-emergency-response>

⁶⁰ Див.: URL: <https://www.energy.gov/ceser/energy-security> ; <https://www.energy.gov/ceser/emergency-response>

⁶¹ Зокрема, у травні 2022 р. CESER оприлюднив «Посібник із реагування на надзвичайні ситуації в енергетиці для штатів і територій» (Energy Emergency Response Playbook for States and Territories). Посібник допоможе розпочати планування щодо реагування на кризи у сфері енергозабезпечення споживачів, містить вказівки та шаблони для дій з реагування та інші додаткові ресурси щодо планування, моніторингу та реагування.

Зміст посібника зосереджується на організації процесу за основними етапами циклу кризового реагування (готовність, реагування, відновлення) на загрози енергозабезпеченню. Пропонується застосування ітеративного процесу збору інформації, оцінки фактичних або потенційних наслідків інциденту та вжиття заходів для обміну важливою інформацією, полегшення відновлення системи енергозабезпечення та пом'якшення впливу на залежні сектори та споживачів. Цей процес повторюється протягом кризи, супроводжуючи дії з реагування, які адаптуються до мінливих умов у міру розвитку ситуації (див.: URL: <https://www.energy.gov/ceser/doe-energy-emergency-response-playbook-states-and-territories>).

⁶² Див.: URL: [https://www.oe.netl.doe.gov/docs/prepare/State_Energy_Assurance_guidelines_Version_3.1_2009-12\[1\].pdf](https://www.oe.netl.doe.gov/docs/prepare/State_Energy_Assurance_guidelines_Version_3.1_2009-12[1].pdf)

- надає допомогу власникам та операторам енергетичних активів у підготовці до кризових ситуацій, під час реагування на них, мінімізації наслідків та відновлення пошкоджених енергетичних систем;
- взаємодіє з міжвідомчими партнерами для визначення допоміжних ресурсів задля стабілізації та відновлення енергетичних систем;
- забезпечує посилення готовності до кібербезпеки в енергетичному секторі й координацію реагування на кіберінциденти та відновлення;
- сприяє наданню юридичної та регулятивної допомоги (звільнення від жорстких вимог регулювання (waivers)) для пришвидшення відновлення пошкоджених енергетичних систем і забезпечення належного постачання енергії;
- забезпечує надання технічної експертизи для оцінювання пошкоджень енергетичних систем і допомоги у відновленні, логістиці та довгостроковому плануванні відновлення;
- збирає, оцінює, забезпечує обмін інформацією та візуалізаціями енергетичного сектору задля сприяння спільній обізнаності про ситуацію та планування узгоджених дій.

Цей підрозділ забезпечує виконання всіх процедур кризового реагування відповідно до рекомендацій DHS, зокрема щодо координації під час виконання ESF # 12 («Енергія»)⁶³ та відповідних завдань, визначених для DOE. Практичну діяльність із забезпечення законодавчого врегулювання, організації планової роботи суб'єктів та допомоги у кризовій ситуації також здійснює CESER.

Ураховуючи те, що понад 80 % енергетичних активів США перебувають у приватній власності, встановлення законодавчих вимог до забезпечення безпеки КІ допомагає залучити до активної діяльності Операторів енергетичної інфраструктури.

Законом «Про енергетичну політику» (The Energy Policy Act of 2005)⁶⁴ було внесено зміни до Закону «Федеральний енергетичний акт» (The Federal Power Act) та введено в дію поняття «стандарт надійності» (Reliability standard), крім того, запроваджено вимогу щодо їх застосування всіма суб'єктами електроенергетичної системи. Закон визначив, що стандарти затверджує американський енергетичний регулятор (Federal Energy Regulatory Commission, FERC)⁶⁵ у співпраці з організацією з питань надійності електропостачання (Electric Reliability Organization, ERO), яка є уповноваженою в

⁶³ Emergency Support Function # 12 (Energy) у рамках національної системи реагування FEMA спрямована на підтримання державних та приватних стейкхолдерів у подоланні бар'єрів та викликів, пов'язаних із збереженням функції енергопостачання у кризовій ситуації, а також процесом відновлення енергетичних систем.

⁶⁴ Див.: URL: <https://www.congress.gov/109/plaws/publ58/PLAW-109publ58.pdf>

⁶⁵ Див.: URL: <https://www.ferc.gov/>

електроенергетиці для розробки стандартів та їхнього впровадження. Закон уповноважив FERC або ERO (за погодженням з FERC) накладати штрафи на суб'єктів забезпечення енергопостачання за порушення стандарту надійності.

Пізніше FERC сертифікував Північноамериканську корпорацію надійності електропостачання (North American Electric Reliability Corporation, NERC)⁶⁶ як ERO. До цього часу NERC здійснила розробку 14 стандартів з питань безпеки та стійкості енергопостачання (Critical Infrastructure Protection, CIP)⁶⁷. NERC щільно співпрацює із Центром аналізу та обміну інформацією в електроенергетиці (Electricity Information Sharing and Analysis Center, E-ISAC)⁶⁸. Центр надає своїм членам і партнерам фахові експертизи та необхідну інформацію для підготовки до виникнення кризових ситуацій і зменшення кібер- та фізичних загроз безпеці енергетичним системам.

Законом також уповноважено міністра енергетики запроваджувати надзвичайні заходи (якщо президент США оголошує надзвичайну ситуацію в енергетиці), спрямовані на швидше та ефективніше пом'якшення ситуації та ліквідацію загрози щодо порушення надійності функціонування енергосистеми. Одним із таких заходів DOE є Регламент реагування на кризові ситуації (Grid Security Emergency Final Rule), яким урегульовано процедури захисту або відновлення надійності критичної електричної інфраструктури⁶⁹.

Для оперативного реагування у кризовій ситуації створено Секторальний консолідований центр кризового управління (Consolidated Emergency Operations Center⁷⁰), що працює у форматі цілодобового оперативного центру підтримки функціонування енергетичних систем. Центр кризового управління, укомплектований фахівцями з кризового менеджменту в електроенергетиці, надає суб'єктам сектору інформацію в режимі реального часу та синхронізує міжвідомчу й державну підтримку функцій управління надзвичайними ситуаціями в приватному секторі для реагування на загрози будь-якого типу будь-якій системі енергопостачання або національній безпеці.

Загалом Центр кризового управління саме як секторальний орган опікується завданнями забезпечення енергетичної стійкості країни, що дозволяє зменшити ймовірність тривалих відключень споживачів від електропостачання, обмежити обсяг і вплив відключень, якщо вони трапляються, і швидко відновлювати живлення після відключення.

⁶⁶ Див.: URL: <https://www.nerc.com/Pages/default.aspx>

⁶⁷ Стандарти NERC CIP – це обов'язкові стандарти безпеки, що застосовуються до організацій, які володіють або керують об'єктами, котрі є частиною електроенергетичної мережі США та Канади (див.: URL: <https://www.nerc.com/pa/Stand/Pages/default.aspx>).

⁶⁸ Див.: URL: <https://www.nerc.com/pa/CI/ESISAC/Pages/default.aspx>

⁶⁹ Див.: URL: <https://www.energy.gov/ceser/grid-security-emergency-final-rule-10-cfr-part-205>

⁷⁰ Див.: URL: <https://www.energy.gov/nnsa/leadership-and-offices/emergency-operations>

Важливо те, що DOE дає визначення⁷¹ енергетичній стійкості, трактуючи її як здатність мережі, будівель і спільнот протистояти і швидко відновлюватися після відключень електроенергії та продовжувати працювати з електроенергією, опаленням, охолодженням, вентиляцією та іншими енергозалежними послугами.

Забезпечення безпеки та стійкості енергозабезпечення на місцевому рівні

Вимоги, встановлені на федеральному рівні DHS щодо організації діяльності у секторах критичної інфраструктури, FEMA – щодо готовності до реагування на кризові ситуації (ESF # 12) та DOE – щодо забезпечення стійкості енергопостачання споживачам, потребують відповідного реагування на рівні штатів та місцевих громад.

Міненерго США, забезпечуючи виконання положень прийнятого 2021 р. Закону США «Про інвестиції в інфраструктуру та робочі місця» (Infrastructure Investment and Jobs Act, ІІА)⁷² стосовно розроблення планів енергетичної безпеки⁷³, опрацювало методологію розробки таких планів (State Energy Security Plan Guidance)⁷⁴.

Закон визначає, що плани енергетичної безпеки штатів (State Energy Security Plans, SESP)⁷⁵ мають забезпечити: оцінку енергетичної ситуації у штаті (формування «Енергетичного профілю штату»); захист енергетичної інфраструктури від будь-яких типів загроз; зменшення ризиків порушення енергозабезпечення споживачів штату; посилення спроможності штату в реагуванні на збої в енергетиці та відновлення після них; розвиток надійної, безпечної та стійкої енергетичної інфраструктури.

⁷¹ Див.: URL: <https://www.energy.gov/eere/energy-resilience>

⁷² Infrastructure Investment and Jobs Act (ІІА). URL: <https://www.congress.gov/bill/117th-congress/house-bill/3684/text>

⁷³ SEC. 40108. State Energy Security Plans. Infrastructure Investment and Jobs Act (ІІА).

⁷⁴ Див.: URL: <https://www.nga.org/wp-content/uploads/2022/05/State-Energy-Security-Plan-Framework-and-Guidance-FINAL.pdf>

⁷⁵ Законом визначено вимоги щодо змісту та структури Плану енергетичної безпеки штату, який має враховувати аспекти:

- (1) розглядати всі джерела енергії, регульованих і нерегульованих постачальників енергії;
- (2) формувати енергетичний профіль штату, включно оцінку виробництва, передачі, розподілу та кінцевого використання енергії;
- (3) розглядати потенційні небезпеки для кожного енергетичного сектору чи системи, включно фізичні загрози та вразливі місця; загрози та вразливості кібербезпеки;
- (4) забезпечити оцінку ризиків енергетичної інфраструктури та міжгалузевих взаємозалежностей;
- (5) забезпечити заходи зменшення ризиків для підвищення надійності та стійкості кінцевого використання енергії;
- (6) розглядати: регіональну (між штатами) координацію, планування та реагування на випадок криз; заохочувати найширше коло учасників (зокрема, індіанські племена) до діяльності у сфері планування й реагування, а також взаємодопомоги.

Кожний штат, ураховуючи свої особливості, розробляє власний підхід до підготовки плану. Але, зважаючи на вимоги з питань забезпечення безпеки, стійкості критичної енергетичної інфраструктури та процедури взаємодії на місцевому рівні у кризовій ситуації (відповідно до рамкових вимог FEMA), штати послуговуються типовими складовими структури цих планів, зокрема це такі пункти⁷⁶:

- формування «Енергетичного профілю штату»⁷⁷ – огляд поточного стану та пріоритети розвитку енергетики штату, що використовуються з метою сталого енергозабезпечення споживачів на тривалу перспективу, впровадження новітніх технологій та виконання національних цілей у сфері енергетики та суміжних сфер;

- детальний аналіз уразливостей та ризиків енергозабезпеченню споживачів штату⁷⁸ з врахуванням оцінки ризиків для штату, підготовлених секторальним органом (DOE)⁷⁹;

- заходи зниження уразливостей систем енергозабезпечення для зниження впливу загроз;

- вказівки щодо процесу координації заходів реагування та етапів реагування (підготовка, запобігання, реагування, відновлення);

- перелік основних принципів роботи під час кризової ситуації для кожної відповідальної посадової особи у штаті та федеральних відомствах;

- протоколи інформування громадськості та комунікації, які мають бути застосовані різними агенціями під час надзвичайної енергетичної ситуації.

Зазначимо, що уточнення законодавства в цій сфері базується на тривалій практиці розроблення місцевих планів безпеки енергопостачання. З 2009 р. вдосконалювалася методологія підготовки Плану гарантування енергозабезпечення (Energy Assurance Plans)⁸⁰. Розроблення на рівні штатів таких планів стало ефективним інструментом формалізації та координації дій

⁷⁶ Див.: URL: <https://www.energy.gov/ceser/doe-energy-emergency-response-playbook-states-and-territories>

⁷⁷ CESER Guidance on Developing a State Energy Profile. URL: https://www.energy.gov/sites/default/files/2022-08/DOE%20CESER%20Guidance_State%20Energy%20Profile%20Outline_FINAL_508_0.pdf

⁷⁸ Аналіз вразливості та ризиків (Vulnerability and Risk Analysis, VRA) забезпечує загальний огляд енергетичної інфраструктури та сприяє усвідомленому ставленню до проблем з боку всіх суб'єктів ключових енергетичних систем (електроенергетика, природний газ і нафта). Крім того, VRA визначає активи, що домінують на певних ринках або в певних географічних зонах, втрата яких призведе до серйозних наслідків.

VRA складається з двох основних частин:

1. Опис енергетичної інфраструктури та ролей окремих активів. Цей розділ також містить опис того, як певні об'єкти КІ пов'язані з іншою інфраструктурою та послугами, які вона забезпечує.

2. Аналіз ризиків визначеної критичної енергетичної інфраструктури, який дає розуміння можливих значних наслідків збоїв у наданні послуг через порушення функціонування КІ.

За результатами аналізу визначається пріоритетність заходів реагування (рейтинг) для забезпечення стійкості енергозабезпечення. Оцінка рейтингу VRA базується на алгоритмі, який описує ступінь критичності активу для економіки, громадської безпеки та безпеки в державі, а також його прями та непрямі наслідки для енергетичної системи (систем), якщо він був порушений або втратив свою функцію.

⁷⁹ Див.: URL: <https://www.energy.gov/ceser/state-and-regional-energy-risk-profiles>

⁸⁰ Див.: URL: <https://www.naseo.org/stateenergyplans>

органів державної влади (федеральних і місцевих) з усіма суб'єктами, що залучені до процесу енергозабезпечення штату для підготовки до реагування на потенційні збої в галузі енергопостачання. План також забезпечує краще усвідомлення державними органами влади та приватним сектором розуміння взаємозалежного характеру енергетичної галузі, ролей та обов'язків регіональних організацій і призначених державних установ у запобіганні виникненню кризи енергопостачання, пом'якшенні впливу загроз, реагуванні на надзвичайні ситуації та відновлення. Досить детальні плани штату Нью-Йорк можуть слугувати прикладом у розробленні таких документів ⁸¹.

Підрозділ Міненергетики США CESER з метою формування уніфікованого підходу до реагування на кризові ситуації з енергопостачання надає допомогу штатам під час підготовки планів ⁸². CESER також здійснює періодичний огляд ризиків порушення функції енергозабезпечення споживачів для штатів ⁸³, які вважаються базовими для подальшої підготовки заходів реагування, що включаються в плани енергетичної безпеки штатів.

Варто зважати на те, що реалізація заходів із забезпечення безпеки функціонування енергетичної інфраструктури потребує суттєвих ресурсів. Зважаючи на те, що оператори критичної енергетичної інфраструктури нерідко є природними монополіями, до діяльності в цій сфері долучаються регулятори, які мають сприяти інвестиціям операторів на заходи із забезпечення безпеки та стійкості функціонування КІ.

У США окремі штати приймають свої законодавчі вимоги, які діють поряд із федеральними законами. У рамках формування принципів ціноутворення на ринку окремі штати можуть дозволяти операторам компенсувати витрати на безпеку. Наприклад, закон штату Канзас дозволяє відшкодувати видатки на забезпечення заходів безпеки об'єктів критичної енергетичної інфраструктури через ціну продажу енергії ⁸⁴.

Регуляторні комісії штатів, які регулюють діяльність широкого спектра муніципальних природних монополій, повноцінно долучаються до планування стійкості на рівні місцевих громад. У сфері планування стійкості енергозабезпечення можна виокремити найбільш поширені повноваження та ролі, які відіграють регуляторні комісії штатів США (табл. 1).

⁸¹ Див.: URL: <https://www.nyserda.ny.gov/About/Publications/EA-Reports-and-Studies/Energy-Assurance-and-Energy-Emergency-Plans>

⁸² Див.: URL: <https://www.energy.gov/ceser/state-local-tribal-and-territorial-slitt-program>

⁸³ Див.: URL: <https://www.energy.gov/ceser/state-and-regional-energy-risk-profiles>

⁸⁴ The Kansas Energy Security Act, 2002. URL: <http://www.kansas.gov/government/legislative/bills/2004/2374.pdf>

Таблиця 1. Регуляторні комісії штатів у плануванні енергетичної стійкості

Роль регуляторних комісій штатів	Чисельність штатів
Активно долучається до розроблення планів енергетичної стійкості	31
Є відповідальною інституцією за розроблення планів енергетичної стійкості	6
Є координувальною інституцією у розробленні планів енергетичної стійкості	6
Бере активну участь у розробленні планів енергетичної стійкості, формуючи вимоги до функціонування систем енергозабезпечення у кризовій ситуації	19
Є членом Координаційного комітету з розроблення планів енергетичної стійкості	7
Відповідає за обмін інформацією на загальнодержавному рівні під час реагування на кризову ситуацію	1

Джерело: складено за⁸⁵.

Серед встановлених комісіями регуляторних вимог є вимога до операторів систем енергозабезпечення – вони повинні складати плани реагування на надзвичайні ситуації та відновлення енергозабезпечення, які регулярно оновлюються. Наявність таких планів є складовою частиною процесу ліцензування відповідних операторів.

Для допомоги всім учасникам забезпечення безпеки і стійкості енергопостачання створено низку допоміжних консультативних організацій. Для координації дій між штатами на випадок реалізації загроз існує Energy Emergency Assurance Coordinators Program, організована DOE, місцевими посадовцями з різних штатів. Створена також Координаційна рада секторів електроенергетики (Electricity Sub-Sector Coordinating Council)⁸⁶, яка надає підтримку щодо координації діяльності, спрямованої на підвищення надійності та стійкості підгалузі електроенергетики, включно фізичної і кібернетичної інфраструктури, та готовності до надзвичайних ситуацій в енергетичній галузі⁸⁷.

1.3. Розвиток законодавства України з питань стійкості функціонування критичної інфраструктури: стан та виклики

Україна активно формує систему законодавчих вимог щодо забезпечення стійкості функціонування критичної інфраструктури та надання життєво

⁸⁵ State Energy Assurance Guidelines. NASEO. 2009. Version 3.1. URL: https://www.naseo.org/Data/Sites/1/documents/energyassurance/eaguidelines/State_Energy_Assurance_Guidelines_Version_3.1.pdf

⁸⁶ Див.: URL: <https://www.electricitysubsector.org/>

⁸⁷ Див.: URL: <https://www.energy.gov/ceser/partnering-us>

важливих функцій/послуг як на національному, так і секторальному та місцевих рівнях. При цьому варто зазначити, що загальні підходи у цій сфері, співпадають із завданнями формування рамкової системи національної стійкості⁸⁸ та базуються на кращому світовому досвіді.

Першим законодавчим актом, який визначав пріоритети розбудови системи національної стійкості в Україні, стало рішення Ради національної безпеки і оборони України, введене у дію у вересні 2021 р. Указом Президента України⁸⁹. Затверджена цим рішенням Концепція забезпечення національної системи стійкості (далі – Концепція) визначала мету запровадження та основні принципи і механізми функціонування національної системи стійкості.

Концепція також вводила в правове поле низку важливих понять у цій сфері, зокрема такі:

національна система стійкості – комплекс цілеспрямованих дій, методів та механізмів взаємодії органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, інститутів громадянського суспільства, які гарантують збереження безпеки і безперервності функціонування основних сфер життєдіяльності суспільства і держави до, під час і після настання кризової ситуації;

національна стійкість – здатність держави і суспільства ефективно протистояти загрозам будь-якого походження і характеру, адаптуватися до змін безпекового середовища, підтримувати стале функціонування, швидко відновлюватися до бажаної рівноваги після кризових ситуацій.

У Концепції визначено базові елементи національної системи стійкості, до яких належать:

- 1) гарантована дієвість та спроможність до повноцінного функціонування системи державних органів, їх інституційна стійкість;
- 2) безпека та захищеність об'єктів критичної інфраструктури, зокрема:
 - стійке постачання продовольства, водопостачання, енергопостачання, постачання теплової енергії;
 - стійке функціонування транспортних систем;
 - кібербезпека;
 - захищеність та безперебійне функціонування інформаційних та комунікаційних послуг;
 - забезпечення оборони та правопорядку;

⁸⁸ Резнікова О. О. Національна стійкість в умовах мінливого безпекового середовища : монографія. Київ : НІСД, 2022. 532 с.

⁸⁹ Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 р. «Про запровадження національної системи стійкості»: Указ Президента України від 27.09.2021 № 479/2021. URL: <https://zakon.rada.gov.ua/laws/show/479/2021#Text>

здатність системи охорони здоров'я функціонувати в умовах посиленних навантажень;

3) спроможність єдиної державної системи цивільного захисту до дій в умовах загрози чи виникнення надзвичайних ситуацій;

4) здатність ефективно реагувати на неконтрольоване масове переміщення людей;

5) суспільна стійкість, зокрема, до інформаційних впливів;

б) фінансово-економічна стійкість, зокрема, безперервність основних бізнес-процесів.

Таким чином, Концепція розглядає стійкість функціонування КІ у якості одного із базових складників національної системи стійкості та підтверджує важливість забезпечення безпеки та стійкості КІ для політики національної безпеки України, що раніше було закріплено актами законодавства.

Завдання щодо створення державної системи захисту КІ було ініційовано наприкінці 2016 р. також рішенням Ради національної безпеки і оборони України⁹⁰. Тривалий процес розбудови законодавчої бази в цій сфері знайшов своє відображення в Законі України «Про критичну інфраструктуру» (2021)⁹¹, що суттєво активізувало процес практичної імплементації заходів стосовно забезпечення безпеки і стійкості КІ та надання життєво важливих функцій і послуг⁹² споживачам.

У цьому Законі визначено 17 життєво важливих функцій (відображають секторальну спрямованість), які рішенням Кабінету Міністрів України деталізовано в цілий набір основних послуг (138 типів) за секторальним розподілом⁹³. Також встановлюється завдання щодо підтримання ЖВФ у кризових ситуаціях, навіть у випадку порушення функціонування об'єктів критичної інфраструктури.

Як засвідчує світовий досвід, діяльність у цій сфері потребує інструменту координації зусиль усіх залучених учасників (держави, населення, приватного

⁹⁰ Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури: Рішення Ради національної безпеки і оборони України від 16.12.2016. URL: <https://zakon.rada.gov.ua/laws/show/n0014525-16#Text>

⁹¹ Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>

⁹² Закон містить низку важливих визначень, зокрема такі:

життєво важливі функції та/або – функції та/або послуги, реалізація яких забезпечується органами державної влади, органами місцевого самоврядування, установами, суб'єктами господарювання та організаціями будь-якої форми власності, збої, переривання та порушення надання яких призводять до швидких негативних наслідків для національної безпеки;

безпека критичної інфраструктури – стан захищеності критичної інфраструктури, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість критичної інфраструктури;

стійкість критичної – стан критичної інфраструктури, за якого забезпечується її спроможність функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після впливу загроз будь-якого виду.

⁹³ Деякі питання об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 № 1109. URL: <https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text>

бізнесу та ін.). Необхідний інструментарій узгодження та координації зусиль усіх залучених суб'єктів передбачений і в Україні. Законом встановлюється вимога щодо розроблення планів взаємодії та підтримання життєво важливих функцій / послуг на різних рівнях управління та у всіх секторах КІ.

Так, відповідно до статті 19 Закону секторальні органи у сфері захисту критичної інфраструктури розробляють і затверджують плани взаємодії та підтримання ЖВФ на випадок порушення функціонування об'єктів КІ.

Місцеві органи виконавчої влади відповідно до статті 20 Закону забезпечують:

1) розроблення й затвердження місцевих програм забезпечення безпеки та стійкості КІ, програм підвищення стійкості територіальних громад до кризових ситуацій, що спричинені припиненням або погіршенням надання важливих для їхньої життєдіяльності послуг чи здійснення ЖВФ;

2) розроблення, затвердження та погодження із заінтересованими органами місцевих планів взаємодії залучених суб'єктів у кризовій ситуації з метою підтримання ЖВФ, планів відновлення функціонування критичної інфраструктури.

Серед основних завдань Операторів КІ у статті 21 цього Закону визначено низку заходів, які повинні забезпечувати стійкість функціонування своїх об'єктів критичної інфраструктури та підтримку функціонування КІ суміжних секторів. Цими заходами є:

– проведення оцінки ризиків на об'єктах КІ та обмін інформацією про ризики та загрози з іншими суб'єктами національної системи захисту КІ;

– реагування на інциденти, кризові ситуації, а також ліквідація їх наслідків на об'єктах КІ у взаємодії з іншими суб'єктами національної системи захисту КІ; відновлення функціонування об'єктів КІ в разі виникнення аварій та ін.;

– взаємодія з підприємствами, які забезпечують централізоване водопостачання, централізоване водовідведення, постачання теплової енергії, енергопостачання, функціонування електронних комунікаційних мереж, транспортне обслуговування, медичну допомогу, безпеку та інші послуги, від яких залежить процес реагування на кризові ситуації та відновлення функціонування об'єктів критичної інфраструктури.

Отже, Україна на законодавчому рівні також сформуvala засади розвитку політики в цій сфері, а Закон України «Про критичну інфраструктуру» загалом відображає сучасні світові тенденції та узгоджується із положеннями Директиви CER Європейського Союзу.

Нагальна потреба забезпечувати стійкість функціонування КІ та надання ЖВФ зумовлена не тільки вимогами законодавства, а й практичними потребами.

Передусім це пов'язано із масштабними руйнуваннями критичної інфраструктури російськими військами, які вторглись на територію України в лютому 2022 р.

Зважаючи на масштабні руйнування енергетичної інфраструктури України, яких, починаючи з вересня 2022 р., армія країни-агресорки постійно завдає, Рада національної безпеки і оборони України рішенням «Про організацію захисту та забезпечення безпеки функціонування об'єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій» від 17 жовтня 2023 р. визначила як нагальні практичні завдання суб'єктам національної системи захисту КІ щодо забезпечення стійкості енергетичної інфраструктури та функції енергозабезпечення споживачів⁹⁴:

- Кабінету Міністрів України:

«розробити та затвердити у 2023 році з визначенням джерел фінансування План енергетичної стійкості України, який передбачатиме заходи щодо: системного моніторингу та аналізу загроз енергетичній інфраструктурі та ризиків для виконання життєво важливих функцій та/або надання життєво важливих послуг;

установлення вимог забезпечення безпеки і стійкості енергетичної інфраструктури відповідно до визначених загроз та їх урахування під час проєктування схем енергозабезпечення;

альтернативного (резервного) енергозабезпечення об'єктів критичної інфраструктури, які забезпечують виконання життєво важливих функцій та/або надання життєво важливих послуг, насамперед шляхом формування децентралізованих енергетичних систем на базі малих систем розподілу з урахуванням кращого іноземного та вітчизняного досвіду;

урахування пріоритетів споживачів щодо енергозабезпечення під час застосування графіків обмеження та/або припинення постачання енергії;

створення механізмів та розроблення порядку залучення всіх сил і ресурсів для подолання кризової ситуації»;

- Адміністрації Державної служби спеціального зв'язку та захисту інформації України, Міністерству розвитку громад, територій та інфраструктури України:

«підготувати у місячний строк методичні рекомендації для місцевих органів виконавчої влади та органів місцевого самоврядування щодо розроблення та затвердження місцевих програм забезпечення безпеки та

⁹⁴ Про рішення Ради національної безпеки і оборони України від 17 жовтня 2023 р. «Про організацію захисту та забезпечення безпеки функціонування об'єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій»: Указ Президента України від 17.10.2023 № 695. URL: <https://zakon.rada.gov.ua/laws/show/695/2023#n5>

стійкості критичної інфраструктури, програм підвищення стійкості територіальних громад до кризових ситуацій, викликаних припиненням або погіршенням надання важливих для їх життєдіяльності послуг чи для здійснення життєво важливих функцій».

Відповідні методичні рекомендації були підготовлені ⁹⁵, відтак розпочалася практична робота з місцевими органами влади щодо розроблення необхідних місцевих програм із забезпечення безпеки та стійкості функціонування КІ, стійкості надання ЖВФ та життєдіяльності громад.

Також рішенням Ради національної безпеки і оборони «Щодо додаткових заходів із посилення стійкості функціонування енергетичної системи та підготовки національної економіки до роботи в осінньо-зимовий період 2023/24 року» від 07 листопада 2023 р. ⁹⁶ визначено актуальні завдання:

• обласним, Київській міській державним адміністраціям за участю органів місцевого самоврядування у місячний строк:

«1) проаналізувати потенціал та ресурс регіону для максимального збільшення використання та виробництва (видобутку) альтернативних видів палива для сталого проходження осінньо-зимового періоду 2023/24 року;

2) вжити заходів щодо актуалізації (затвердження) регіональних стратегій та програм розвитку, місцевих програм щодо збільшення використання розподіленої генерації, альтернативних джерел енергії та підвищення енергоефективності із забезпеченням відповідного фінансування;

3) опрацювати питання залучення в установленому порядку ресурсів територіальних громад до подолання кризових ситуацій в енергетичній сфері;

4) затвердити плани заходів із забезпечення безпеки та стійкості критичної інфраструктури, яка забезпечує життєдіяльність територіальних громад, з урахуванням дій щодо посилення захисту таких об'єктів від фізичних та кіберзагроз;

5) затвердити перелік об'єктів критичної інфраструктури, які забезпечують виконання життєво важливих функцій у територіальних громадах;

⁹⁵ Про затвердження Методичних рекомендацій щодо розроблення та затвердження місцевих програм забезпечення безпеки та стійкості критичної інфраструктури, програм підвищення стійкості територіальних громад до кризових ситуацій, викликаних припиненням або погіршенням надання важливих для їх життєдіяльності послуг чи для здійснення життєво важливих функцій : Наказ Адміністрації Держспецзв'язку від 30.11.2023 № 997. URL: <http://surl.li/slody>

⁹⁶ Про рішення Ради національної безпеки і оборони України від 7 листопада 2023 р. «Щодо додаткових заходів із посилення стійкості функціонування енергетичної системи та підготовки національної економіки до роботи в осінньо-зимовий період 2023/24 року»: Указ Президента України від 07.11.2023 № 737/2023. URL: <https://zakon.rada.gov.ua/laws/show/737/2023#Text>

б) забезпечити підготовку вузлів під'єднання об'єктів критичної інфраструктури, які забезпечують виконання життєво важливих функцій у територіальних громадах, для випадків застосування схем резервного енергозабезпечення;

7) опрацювати питання щодо внесення змін до регіональних стратегій та програм розвитку стосовно встановлення автономних систем освітлення пішохідних переходів та енергозабезпечення світлофорів».

Також було рекомендовано регулятору енергетичних ринків (Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг, НКРЕКП) разом із обласними, Київською міською державними адміністраціями, за участю органів місцевого самоврядування «визначити джерела фінансування для забезпечення функціонування обладнання альтернативного (резервного) енергозабезпечення об'єктів критичної інфраструктури, які забезпечують виконання життєво важливих функцій у територіальних громадах».

Водночас практична імплементація положень Закону України «Про критичну інфраструктуру» свідчить про те, що суб'єкти національної системи захисту критичної інфраструктури України все ще орієнтуються на традиційні для них практики встановлення вимог щодо фізичної безпеки об'єктів КІ та здійснення контролю над діяльністю Операторів КІ. Серед причин, через які так відбувається, можна назвати недостатню наукову та методичну підтримку діяльності суб'єктів реагування на загрози стійкості функціонування критичної інфраструктури.

Саме задля створення методологічних засад і формування практичних рекомендацій щодо розвитку механізмів забезпечення стійкості надання визначених послуг / функцій, стимулювання та підтримки Операторів КІ, що забезпечують надання таких послуг, дослідження ризиків КІ, обміну інформацією та координації діяльності у форматі державно-приватного партнерства і підготовлена ця аналітична доповідь.

1.4. Узагальнення світового досвіду та узгодження підходів до планування заходів безпеки та стійкості критичної інфраструктури

Особливості розвитку систем реагування на кризові ситуації, аналіз яких уміщено в попередньому підрозділі, свідчать про те, що безпека та стійкість функціонування критичної інфраструктури – важливі складники національної системи стійкості.

Як зазначається в аналітичній доповіді фахівців Національного інституту стратегічних досліджень (НІСД), безпека та стійкість КІ є одним із основних елементів та етапом формування національної стійкості⁹⁷. З позицій системного підходу, сфера уваги системи безпеки та стійкості КІ стосується організаційно-функціональної структури визначеної сфери управління (переважно інфраструктури, що існує на фізичному рівні), яка забезпечує взаємодію, обмін ресурсами та інформацією. У свою чергу, національна система стійкості охоплює набагато ширше коло питань функціонування визначеної сфери управління, зокрема стосується якісних характеристик елементів, які є складниками цієї системи (ефективність здійснення владних функцій, сталість соціально-економічного розвитку, психологічна стійкість людини, якість освіти та охорони здоров'я тощо). Таким чином, система безпеки та стійкості критичної інфраструктури є складовою частиною системи національної системи стійкості, а результати її роботи будуть використовуватися в межах цієї більшої системи.

У різних країнах спостерігаються свої національні особливості розбудови системи безпеки та стійкості КІ, що зумовлено прийнятою в цих країнах моделлю організації здійснення владних повноважень та структурою органів державної влади. Однак аналіз поточних тенденцій свідчить про поступову трансформацію цієї системи: від забезпечення захисту КІ до стійкості її функціонування, що зробить можливим гарантувати надання ЖВФ споживачам, навіть у кризових ситуаціях.

Для подальшого розкриття змісту, цілей і завдань забезпечення стійкості функціонування КІ та надання ЖВФ пропонуємо власне розуміння окремих аспектів організації процесу планування стійкості, що спирається на позитивний світовий досвід, передусім здобутки США. На нашу думку, це допоможе узгодити підходи й дещо зменшити обсяг термінології, що використовується для опису діяльності в цій сфері, та формалізувати процес управлінської діяльності суб'єктів реагування та планування заходів забезпечення стійкості.

Загальна схема розподілу відповідальності у сфері безпеки та стійкості критичної інфраструктури

Попри те, що в різних країнах існують відмінні від інших інституційні системи та організаційні структури формування й реалізації державної політики

⁹⁷ Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналіт. доп. / [Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М.] / за заг. ред. О. М. Суходолі. Київ : НІСД, 2019. 224 с. URL: https://niss.gov.ua/sites/default/files/2019-05/Dopov_Suchodolya_print.pdf

у сфері безпеки та стійкості КІ, можна виокремити загальні риси розподілу відповідальності та повноважень між державними інституціями.

У кожній країні визначається орган державної влади, на який покладається завдання щодо формування державної політики з питань захисту КІ (здебільшого це визначений орган державної влади на рівні міністерства або спеціально утворений підрозділ у структурі уряду країни). Такий уповноважений урядом орган управління передусім розробляє стратегічні документи діяльності в цій сфері та забезпечує єдність методологічних підходів, відповідно до яких здійснюється захист КІ на всіх рівнях управління: національному, секторальному (визначені окремі галузі економіки, сфери діяльності), місцевому, об'єктовому.

Інша категорія державних органів (секторальні та функціональні органи) ураховують галузеву специфіку на рівні секторів КІ і, зважаючи на це, деталізують принципи регулювання питань щодо безпеки та стійкості критичної інфраструктури. Зазвичай такими органами влади є міністерства (незалежні департаменти чи агентства). Саме вони відповідають за забезпечення захисту КІ у відповідному секторі, а також стійкості функціонування всього ланцюжка постачання. Їх визначають відповідальними за стійкість надання окремих функцій / послуг.

Органи місцевої влади та самоврядування в рамках своєї діяльності ураховують місцеву специфіку забезпечення безпеки критичної інфраструктури. До того ж, місцеві органи виконавчої влади (у межах чинних систем реагування та національного законодавства) опікуються КІ місцевого рівня, саме вони є відповідальними за стійкість життєдіяльності громад.

Узгодженість завдань із забезпечення стійкості критичної інфраструктури та життєво важливих послуг

З методологічної точки зору, завдання із забезпечення стійкості функціонування КІ та стійкості «надання послуги / функції» розглядаються як тотожні. Тобто будемо вважати, що принципи планування заходів забезпечення стійкості окремих ЖВФ, визначення суб'єкта планування та координації дій залучених до реагування учасників є однаковими, як для стійкості функціонування КІ, так і для стійкості надання ЖВФ.

Відмінність полягає лише у визначенні сфери планування / управління, тобто стосується «охоплення» залучених до реагування учасників. Наприклад, для того, щоб забезпечити «стійкість надання послуги / функції», важливої для життєдіяльності суспільства та держави, потрібно залучити значно ширше коло учасників, ніж при забезпеченні «стійкості функціонування КІ». При цьому при

плануванні стійкості «надання послуги / функції» метою планування потенційно може бути навіть повне заміщення втраченої штатної КІ, за стійкість функціонування якої відповідає окремий Оператор КІ. Отже, завдання забезпечення стійкості ЖВФ на рівні країни не може покладатися виключно на Оператора КІ, який буде зосереджуватись на збереженні своєї ролі (власника чи операційного менеджера конкретних інфраструктурних об'єктів).

Розмежування ролей «суб'єкт» та «стейкхолдер» у рамках забезпечення стійкості

Відповідно до загального для всіх країн підходу, забезпечення національної стійкості є завданням для всіх учасників, котрі беруть участь у забезпеченні функціонування окремих сфер управління (зокрема, зусилля всієї нації необхідні для забезпечення національної стійкості; зусилля всіх членів територіальної громади – для забезпечення стійкості громади). Водночас різні учасники відповідно до встановленої моделі організації життєдіяльності відповідної сфери управління виконують різні ролі та мають визначені законодавством повноваження та відповідальність.

Доцільно розмежувати залучених суб'єктів реагування на учасників, які володіють владними повноваженнями у відповідній сфері управління (уряд країни може встановити для них завдання щодо планування стійкості), та інших учасників, котрі можуть бути залучені до виконання окремих завдань із забезпечення стійкості (добровільно або на контрактній основі).

Надалі будемо застосовувати термін «суб'єкт» стосовно учасників, які мають законодавчо визначені завдання й повноваження та уповноважені (можуть бути) на забезпечення стійкості надання окремої ЖВФ у відповідній сфері або функціонування визначеної сфери управління.

Під «стейкхолдером» будемо розуміти всіх інших учасників, які певним чином зацікавлені в наданні такої ЖВФ або впливають на процес її надання у відповідній сфері управління, тобто певною мірою залежать від неї або можуть впливати на її діяльність.

І саме визначений таким чином «суб'єкт» має забезпечити планування стійкості окремої ЖВФ чи сфери управління та залучення до процесу планування й реагування всіх інших стейкхолдерів.

Суб'єкт, відповідальний за розроблення «планів стійкості»

Відповідальність за розроблення планів дій, рекомендацій або вимог до забезпечення стійкості функціонування КІ та надання ЖВФ покладається на

інституцію, яка має повноваження та інструментарій долучення до діяльності всіх стейкхолдерів, що працюють у відповідних сферах планування (технологічних, територіальних, рівнів державного управління).

Базуючись на положеннях Закону України «Про критичну інфраструктуру», наведемо приклади суб'єктів планування стійкості за різними рівнями державного управління (різними сферами управління):

- суб'єктом планування *стійкості функціонування об'єктів критичної інфраструктури* є Оператор КІ;

- суб'єктом планування *стійкості надання послуги / функції* є:

- на загальнодержавному рівні (галузі) – орган влади, визначений відповідальним за формування політики у окремому секторі КІ;

- на місцевому рівні – орган влади, визначений відповідальним за життєдіяльність місцевої громади;

Плани стійкості надання ЖВФ є своєрідною формальною рамковою угодою між усіма залученими учасниками, яка визначає та узгоджує сукупність дій, спрямованих на забезпечення безперервності надання окремих функцій / послуг кінцевим споживачам відповідної сфери управління (сектору, галузі) чи рівня управлінської вертикалі (громада села, району, області).

Усвідомлення принципів застосування концепції аналізу ризиків

Важливим елементом організації планування стійкості будь-якої сфери управління є проведення ідентифікації загроз та оцінювання ризиків. У світовій практиці вже розроблені міжнародні стандарти, що описують методологію оцінювання ризиків, яка передбачає оцінку потенційних прямих і непрямих наслідків впливу окремих загроз⁹⁸.

Проте зауважимо, що методологія перебуває на стадії активного розвитку та характеризується широкою різноманітністю підходів. Єдиного універсального підходу на сьогодні не існує, і різні країни (навіть різні інституції однієї країни) застосовують різні підходи щодо оцінювання ризиків порушення функціонування КІ.

Проведений порівняльний огляд методологій аналізу ризиків, які існують у різних країнах⁹⁹, уможливив виокремити низку проблем у застосуванні

⁹⁸ ДСТУ ІЕС/ISO 31010:2013 «Керування ризиками. Методи загального оцінювання ризиків». URL: https://zakon.isu.net.ua/sites/default/files/normdocs/iso_31010.pdf

⁹⁹ National Risk Assessments: A Cross Country Perspective. URL: <https://www.oecd.org/gov/national-risk-assessments-9789264287532-en.htm>; Національні системи оцінювання ризиків і загроз: кращі світові практики, нові можливості для України: аналіт. доп. / [Резнікова О. О., Войтовський К. Є., Лепіхов А. В.]; за заг. ред. О. О. Резнікової. Київ: НІСД, 2020. 84 с.; Kohler K. National Risk Assessments of Cross-Border Risks. Center for Security Studies (CSS). ETH Zürich, 2023. URL: <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/RR-Reports-2023-National-Risk-Assessments-of-Cross-Border-Risks.pdf>

методів оцінювання ризиків щодо питань забезпечення стійкості функціонування КІ та надання ЖВФ. Наприклад, спостерігається фактично рівноцінне використання різних термінів при визначенні та аналізі одних і тих само дій чи подій, існує суттєва неврегульованість принципів вибору загроз / небезпек та критеріїв оцінювання наслідків їхнього впливу. Йдеться, зокрема, про суперечності у застосуванні й розумінні змісту низки термінів: «загрози» (threats), «небезпеки» (hazards), «уразливості» (vulnerability), «вплив» (impact), «наслідки» (consequences), «ризик» (risks), які використовують для розкриття алгоритмів оцінювання негативних наслідків впливу визначених чинників на функціонування визначеної сфери управління.

Коротко на прикладі досвіду США та Великої Британії продемонструємо деякі нюанси вживання вказаних термінів, нечіткості та суперечності.

У США запроваджено базовий інструмент THIRA¹⁰⁰, що застосовується під час оцінювання ризиків надзвичайних ситуацій (здійснюється в системі FEMA)¹⁰¹ та для інших систем реагування, зокрема CISA, у сфері планування заходів забезпечення стійкості КІ¹⁰². Відповідно до THIRA визначення ризику здійснюється через оцінювання впливу загроз і небезпек на параметри функціонування визначеної сфери управління. При цьому терміни «загроза» і «небезпека» інколи використовуються як взаємозамінні¹⁰³.

Методологія визначення ризику передбачає оцінку вірогідності реалізації загрози / небезпеки та наслідків її впливу для різних рівнів¹⁰⁴. Критерії оцінювання наслідків впливу загроз рекомендується приймати у широкому діапазоні, зважаючи на контекст функціонування окремої сфери управління.

¹⁰⁰ 2019 National Threat and Hazard Identification and Risk Assessment (THIRA). Overview and Methodology. URL: https://www.fema.gov/sites/default/files/2020-06/fema_national-thira-overview-methodology_2019_0.pdf

¹⁰¹ National Risk and Capability Assessment. URL: <https://www.fema.gov/emergency-managers/national-preparedness/goal/risk-capability-assessment#thira>

¹⁰² Див.: URL: <https://www.cisa.gov/resources-tools/resources/threat-and-hazard-identification-and-risk-assessment-thira-comprehensive>

¹⁰³ У глосарії термінів, що застосовуються під час оцінювання ризиків, подано такі визначення:

Risk: The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

Threat: A natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Vulnerability: A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard (див.: Department of Homeland Security. DHS Risk Lexicon. 2010. URL: <http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>).

¹⁰⁴ Методологія CISA у сфері планування заходів забезпечення стійкості КІ пропонує проводити аналіз за трьома рівнями правдоподібності настання ризиків (наслідків реалізації загрози):

звичний: один раз на п'ять років. На цьому рівні системи критичної інфраструктури повинні залишатися функціональними і не зазнавати будь-яких значних пошкоджень або збоїв;

нормальний (припущення): один раз на 50 років. На цьому рівні системи інфраструктури повинні зазнавати мінімальних пошкоджень або збоїв, як це визначено проєктними рівнями функціональності;

екстремальний: один раз на 200+ років. На цьому рівні можна очікувати серйозних пошкоджень або збоїв, але критична інфраструктура повинна працювати на мініальному рівні.

Так, у Стратегічній національній оцінці ризику (SNRA) оцінювання наслідків впливу здійснюється за шістьма категоріями: втрата життя; травми та хвороби; прямі економічні витрати; переміщення людей; психологічний стрес; вплив на навколишнє середовище. Водночас під час підготовки Національного індексу ризику (The National Risk Index, NRI)¹⁰⁵, завдяки якому оцінюють природні небезпеки життєдіяльності місцевих громад, критеріями оцінювання наслідків впливу небезпеки обрано три складники: оцінку економічних втрат; оцінку вразливості населення; оцінка впливу на стійкість громад¹⁰⁶.

Міністерство енергетики США рекомендує суб'єктам управління, які здійснюють оцінювання ризиків енергозабезпеченню на місцевому рівні, під час планування заходів реагування враховувати три сценарії, що справлятимуть найбільший вплив на життєдіяльність громади (Tier 1–3)¹⁰⁷. Зазначимо, що визначення критичності впливу сценарію може здійснюватися за окремим набором критеріїв¹⁰⁸, які акцентують увагу на спроможності залучених суб'єктів виконувати їхні завдання, а не на впливові на життєдіяльність громади.

Методологія підготовки Національного реєстру ризиків Великої Британії (NRR) дещо відрізняється від практики США. Зокрема, до NRR уводять загрози національного рівня і природного, і зловмисного характеру¹⁰⁹. Підготовка переліку таких загроз переважно базується на науково-експертному аналізі¹¹⁰: спочатку визначають широкий набір загроз, потім проводять критичну оцінку

¹⁰⁵ Див.: URL: <https://hazards.fema.gov/nri/>

¹⁰⁶ Див.: URL: https://www.fema.gov/sites/default/files/documents/fema_national-risk-index_technical-documentation.pdf

¹⁰⁷ У Методології оцінювання ризиків в енергетичній сфері (див.: Energy Emergency Response Playbook for States and Territories. DOE USA. 2022) також пропонується брати за основу три рівні.

- Tier 3: Enhanced Watch. Рівень 3 (Посилена готовність). Відображає події, вплив яких на ланцюги постачання енергії та/або енергетичні послуги, в основному усуваються промисловістю (Операторами КІ) без підтримки з боку уряду (на місцевому або національному рівні). Державні інституції та регулятори енергетики повинні посилити моніторинг ситуації, щоб зрозуміти, чи потрібно посилювати заходи реагування та коли.

- Tier 2: Significant Events. Рівень 2 (Значні події). Відображає події, за настання яких спостерігаються значні збої в ланцюгах постачання енергії та/або енергетичних послугах з довгими часовими рамками для відновлення. Реагування на ці події зазвичай перевищує ресурси місцевої влади. Промисловість також переважно звертатиметься по допомогу до уряду, щоб прискорити відновлення енергетичної інфраструктури або пом'якшити вплив на населення, яке постраждало, чи життєво важливі сектори.

- Tier 1: Major Events. Рівень 1 (Критичні події). Відображає події, які характеризуються значним порушенням ланцюгів постачання енергії та/або енергетичних послуг із подовженими або невизначеними часовими рамками для відновлення. Події цього рівня вимагають масового реагування на всіх рівнях уряду, щоб забезпечити допомогу, прискорити відновлення та пом'якшити вплив на населення, яке постраждало, та рятувальні сектори.

¹⁰⁸ Це – географічні межі; рівень загрози життю та майну; політична чутливість; організаційна складність; юрисдикційні межі; цінності, які потрапляють під ризик; погода; стратегія і тактика дій; політика суб'єктів реагування; звична чи надзвичайна ситуація.

¹⁰⁹ У Великій Британії під «ризиком» мається на увазі будь-яка подія, що створює серйозну загрозу суспільній безпеці та безпеці засобів існування на місцевому чи національному рівнях.

¹¹⁰ The National Risk Register. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/952959/6.6920_CO_CCS_s_National_Risk_Register_2020_11-1-21-FINAL.pdf

вірогідності їх реалізації та формують один «обґрунтовано найгірший сценарій» (reasonable worst case scenario)¹¹¹. Насамкінець оцінюють вплив визначеного ризик-сценарію за вісьмома складниками: економічні втрати; кількість смертей; чисельність евакуйованих; суспільне сприйняття; екологічні збитки; вплив на основні послуги; вплив на електрозабезпечення; вплив на міжнародні відносини.

Варто, проте, звернути увагу на деяку термінологічну неоднозначність у документах, що стосуються оцінювання ризиків у Великій Британії. Зокрема, у методології підготовки NRR як маркування чинника впливу вживається термін «ризик»¹¹². При цьому в інших документах поняття «ризик» трактується як «загроза» або «уразливість»¹¹³.

Та все ж, вищенаведені приклади неузгодженості термінів, які вживаються, та розбіжності у виборі критеріїв оцінювання впливу загроз не є принциповими під час розроблення методології визначення пріоритетності дій щодо реагування на загрози стійкості функціонування КІ чи надання ЖВФ. Ці розбіжності зумовлені тим, що різні країни та/чи інституції закономірно обирають відповідні трактування змісту термінів, а також різні підходи щодо пояснення алгоритмів оцінювання ризиків, які застосовуються¹¹⁴.

Не вдаючись до окремого термінологічного та лексичного аналізу, пропонуємо спрощений підхід щодо оперування цими термінами, вихідною моделлю якого обрано міжнародний стандарт, що надає визначення терміна «ризик»¹¹⁵, у якому *ризик* (risk) розуміється, зокрема, як вплив невизначеностей на цілі об'єкта управління.

У контексті цього дослідження поняття «**ризик**» будемо трактувати як *загальну оцінку впливу будь-якого чинника впливу (події, інциденту,*

¹¹¹ Це означає, що такі події є найгіршим правдоподібним виявом цього конкретного ризику. Щоб дати можливість відповідним органам здійснити планування реагування на сценарій реалізації загрози, їх оцінюють з точки зору правдоподібності (реалізації обґрунтовано найгіршого сценарію в наступному році) та впливу (обґрунтовано найгіршого сценарію з використанням набору критеріїв оцінки впливу).

¹¹² У документі чинник впливу («загроза») та наслідки, що виникають через його вплив («ризик»), маркуються одним терміном. При цьому «ризик» розкривається як погані погодні умови, технологічні аварії, кібератаки чи диверсії, тобто і як «загрози» і як «небезпеки».

¹¹³ The UK Government's National Technical Authority for Physical and Personnel Protective Security. Protective Security Risk Management. URL: <https://www.npsa.gov.uk/protective-security-risk-management-psrm-0>

¹¹⁴ Наприклад, у Кодексі цивільного захисту України термін «надзвичайна ситуація» використовується у значенні «наслідки», з деталізацією впливу (за окремими критеріями) «небезпечних подій чи чинників» (тобто загроз):

«24) Надзвичайна ситуація – обстановка на окремій території чи суб'єкті господарювання на ній або водному об'єкті, яка характеризується порушенням нормальних умов життєдіяльності населення (наслідок – *Коментар авт.*), спричинена катастрофою, аварією, пожежею, стихійним лихом, епідемією, епізоотією, епіфітотією, застосуванням засобів ураження або іншою небезпечною подією (загрози – *Коментар авт.*), що призвела (може призвести) до виникнення загрози життю або здоров'ю населення, великої кількості загиблих і постраждалих, завдання значних матеріальних збитків, а також до неможливості проживання населення на такій території чи об'єкті, провадження на ній господарської діяльності (критерії оцінки наслідків впливу загроз – *Коментар авт.*);».

¹¹⁵ ISO Guide 73:2009. Risk management – Vocabulary. URL: <https://www.iso.org/ru/standard/44651.html>

невизначеності тощо) на функціонування сфери управління (наприклад, об'єкта критичної інфраструктури чи громади), що спричиняє «негативні» наслідки.

З метою узгодження й уніфікації дефініцій та логіки їх застосування пропонуємо, спираючись на це визначення ризику, нижченаведені терміни використовувати в такому значенні:

загроза (threat, risk source) – явище, чинник, подія, сукупність подій, що відбуваються стихійно (природні явища) чи внаслідок цілеспрямованих дій (зокрема, зловмисних), які здійснюють вплив на об'єкт (сферу правління) та здатні спричинити негативні наслідки¹¹⁶;

уразливість (vulnerability) – чутливість об'єкта управління до впливів, уразливе місце в його захисті від загроз, відсутність «запобіжників» проти них;

наслідок (consequence, impact) – результат впливу загрози на цілі функціонування об'єкта управління (сфери управління), що переважно вимірюється через оцінку величини відхилення параметрів об'єкта / сфери управління від цільових, проектних значень.

Отже, послуговуючись уточненим значенням термінів, можемо сформулювати *модель оцінювання ризику*: «загроза» унаслідок існування «вразливості» об'єкта управління до цієї загрози здатна спричинити погіршення значень цільових параметрів функціонування об'єкта (негативні «наслідки») (рис. 1).



Рис. 1. Модель оцінювання ризику
Джерело: розроблено автором.

¹¹⁶ Під *загрозою* будемо розуміти всі чинники впливу на об'єкт управління (планування стійкості сфери управління) незалежно від характеру їх утворення (тобто і «небезпеки», і «загрози»), оскільки їхній вплив потенційно матиме однаковий ефект, призводячи до порушення функціонування КІ.

Ризик зростає, якщо підвищується правдоподібність (likelihood) реалізації загрози та посилюються спричинені нею наслідки (consequences)¹¹⁷. Тобто за величиною ризику можна визначати рівень критичності загрози, щоб встановити значущість її впливу на цілі об'єкта управління, ранжувати загрози та, відповідно, визначити пріоритети заходів забезпечення безпеки та стійкості функціонування відповідного об'єкта управління¹¹⁸.

Зауважимо: для ранжування критичності загроз необхідно встановити переліки визначених індикаторів, які би відображали наслідки впливу загроз, а також критеріїв оцінювання відхилення параметрів функціонування об'єкта від цільових значень. Як зазначено вище, не існує єдиного універсального набору критеріїв оцінки впливу загроз. Такий набір критеріїв встановлюється суб'єктом організації оцінювання ризиків визначеної сфери управління (наприклад, ризики порушення функціонування об'єкта КІ, зниження рівня надання ЖВФ, порушення життєдіяльності громади тощо).

Про цей аспект планування заходів забезпечення стійкості КІ та стійкості надання ЖВФ йдеться у наступних розділах публікації.

Організація та координація забезпечення стійкості

Досвід інших країн та низка завдань щодо планування стійкості КІ та надання ЖВФ, необхідних для підтримання життєдіяльності громад, свідчить про існування суттєвих викликів та проблем, які постають перед суб'єктом планування.

Фахівці Національного інституту стратегічних досліджень визначають комплекс законодавчих та організаційних проблем і перешкод, що постають під час забезпечення стійкості на місцевому рівні¹¹⁹. Зокрема, наголошується, що «заходи із забезпечення стійкості регіонів і територіальних громад в Україні мають фрагментарний і не упорядкований характер. Відсутність у державі єдиного розуміння механізму забезпечення національної стійкості, процесів, які

¹¹⁷ Пропонується, щоб визначення переліку критеріїв оцінки «наслідків» для конкретної сфери управління здійснював суб'єкт планування стійкості. Зокрема, це можуть бути стратегічні цілі розвитку визначеної сфери управління, відображені у затверджених законодавством документах (*див.*: Енергетична безпека України: перспективна модель управління ризиками : монографія / [О. М. Суходоля, Ю. М. Харазішвілі, Г. Л. Рябцев] ; за ред. О. М. Суходолі. : НІСД, 2023. 152 с. DOI: <https://doi.org/10.53679/NISS-book.2023.01>). З огляду на предмет дослідження в додатку 4 пропонуємо перелік відповідних критеріїв.

¹¹⁸ Варто зазначити, що задача «оцінювання ризиків» у подальшому може доповнюватись задачею «управління ризиками», яка дещо розширює спектр діяльності суб'єкта управління. Поряд із заходами «запобігання» і «пом'якшення» впливу загроз на об'єкт (заходи захисту об'єкта управління), «реагування» на реалізацію загроз і «пом'якшення» наслідків їх впливу, заходів «відновлення» об'єкта та «ліквідації» негативних наслідків впливу можуть застосовуватися заходи «передачі» чи «розподілу» ризиків (передача частини негативних наслідків (збитків) іншим суб'єктам), наприклад через механізм страхування або ж аутсорсингу окремих повноважень / процесів.

¹¹⁹ Організація системи забезпечення національної стійкості на регіональному і місцевому рівнях : аналіт. доп. / [Резнікова О. О., Войтовський К. Є., Лепіхов А. В.] ; за заг. ред. О.О. Резнікової. Київ : НІСД, 2021. 112 с.

він охоплює, а також організації національної системи стійкості суттєво ускладнює запровадження відповідних процесів на рівні регіонів і територіальних громад. Низка проблем у сфері організаційного і правового забезпечення постала на заваді формуванню стійкості регіонів і територіальних громад».

Науковці НІСД акцентують на проблемі відсутності комплексного механізму координації діяльності у рамках повного циклу забезпечення національної стійкості (оцінювання ризиків, виявлення уразливостей, забезпечення готовності, планування, реагування, післякризове відновлення). Щодо кризового реагування, то існує проблема взаємодії різних систем реагування на кризові ситуації комплексного характеру. Зазначається, що існуючі формати міжвідомчої взаємодії зорієнтовані передусім на забезпечення готовності та реагування з боку уповноважених органів на певні види загроз (передусім терористичну, воєнну) і надзвичайні ситуації.

Проблеми взаємодії різних систем при реагуванні на кризові ситуації досліджувались в монографії фахівців Національного інституту стратегічних досліджень, що присвячена питанням розвитку системи захисту критичної інфраструктури¹²⁰. Задля вирішення цих проблем в одному із секторів КІ, а саме в енергетичному, було обґрунтовано необхідність створення міжвідомчого кризового центру при секторальному органі державної влади (Міненерго України), з визначенням переліку завдань, організаційної структури та посадового складу такого центру кризового реагування.

У 2020 р. рішенням Кабінету Міністрів України такий координаційний Антикризовий енергетичний штаб був утворений.¹²¹ З моменту широкомасштабної збройної агресії РФ проти України цей штаб забезпечував виконання координаційної функції, фактично вирішуючи нагальні проблеми, які виникали під час реагування на порушення функціонування критичної енергетичної інфраструктури¹²². Ураховуючи масштабність викликів стійкості надання функції «енергозабезпечення» під час війни, антикризові штаби були створені на рівні місцевих органів влади (при обласних державних адміністраціях¹²³ та органах місцевого самоврядування¹²⁴).

¹²⁰ Developing The Critical Infrastructure Protection System in Ukraine : monograph / [S. Kondratov, D. Bobro, V. Horbulin, et al.]; general editor O. Sukhodolia. Kyiv : NISS, 2017. 184 p. URL: https://niss.gov.ua/sites/default/files/2017-11/niss_Engl_findruk-0e9af.pdf

¹²¹ Про утворення Антикризового енергетичного штабу : Постанова Кабінету Міністрів України від 24.04.2020 № 312. URL: <https://zakon.rada.gov.ua/laws/show/312-2020-%D0%BF#Text>

¹²² Справедливий і рівномірний розподіл електроенергії між споживачами обговорили на засіданні Антикризового енергетичного штабу. 2022. 21 груд. URL: <https://www.kmu.gov.ua/news/spravedlyvyi-i-rivnomirnyi-rozpodil-elektroenerhii-mizh-spozhyvachamy-obhovoryly-na-zasidanni-antykryzovoho-enerhetychnoho-shtabu>

¹²³ Наприклад, наказ Сумської обласної державної адміністрації «Про утворення антикризового енергетичного штабу в Сумській області» (див.: URL: http://sm.gov.ua/images/docs/dostup/2022/11_23.pdf).

Досвід енергетичної сфери у створенні форм координації діяльності на випадок кризової ситуації був поширений на інші аспекти підтримання нормальних умов життєдіяльності громад. У 2023 р. Кабінет Міністрів України створив загальнодержавний Координаційний штаб оперативного реагування з метою сприяння координації діяльності центральних та місцевих органів виконавчої влади, а також інших державних органів, органів місцевого самоврядування, суб'єктів господарювання всіх форм власності (за згодою) з питань оперативного реагування та забезпечення створення нормальних умов життєдіяльності населення під час обмеження та/або припинення постачання електричної енергії¹²⁵, та доручив місцевим органам виконавчої влади створити подібні штаби на місцевому рівні.

Водночас, поряд із очевидним прогресом щодо створення механізмів координації зусиль з підтримання життєдіяльності громад на випадок кризової ситуації, важливим є аспект, пов'язаний із необхідністю узгоджувати пріоритети стійкості функціонування КІ та надання ЖВФ із діяльністю щодо стратегічного планування розвитку громад та ширшим спектром пріоритетів забезпечення національної безпеки.

Обсяг завдань значно перевищує проблеми, пов'язані із забезпеченням координації, обміном інформацією та взаємодією різних суб'єктів у кризовій ситуації. Спектр завдань із забезпечення стійкості виходить далеко за межі процедур кризового реагування. Заходи щодо запобігання впливу загроз, реагування на цей вплив, заходи з відновлення нормального функціонування КІ та надання ЖВФ є надзвичайно капіталоемними. До того ж, ці заходи мають бути сплановані й реалізовані (інвестування ресурсів на довгострокову перспективу) заздалегідь у нормальному режимі функціонування КІ та життєдіяльності громади. У нормальному режимі також мають бути визначені необхідні рівні безпеки КІ (плани захисту від впливу визначених загроз) та процедури кризового реагування (плани взаємодії на випадок порушення функціонування КІ).

Планування стійкості має бути узгоджено із планами соціально-економічного розвитку громад та участі всіх стейкхолдерів у процесі планування й реалізації підготовлених планів¹²⁶. Крім того, заходи із забезпечення стійкості громад, стійкості функціонування КІ, яка забезпечує

¹²⁴ Наприклад, робота штабу м. Києв (див.: URL: https://kyivcity.gov.ua/news/krizovi_pitannya_schodo_elektroenergi_opratsovuvatimut_v_ramkakh_miskogo_shtabu_t_a_priyatimutsya_okremi_rishennya_v_interesakh_kiyan_petro_panteleyev/).

¹²⁵ Про утворення Координаційного штабу із оперативного реагування та забезпечення створення нормальних умов життєдіяльності населення під час обмеження та/або припинення постачання електричної енергії: Постанова Кабінету Міністрів України від 22.09.2023 № 1033. URL: <https://zakon.rada.gov.ua/laws/show/1033-2023-%D0%BF#Text>

¹²⁶ APEC Energy Resiliency Principle. URL: https://mddb.apec.org/Documents/2020/EWG/EWG59/20_ewg59_023.pdf

життєдіяльність громад, повинні узгоджуватися із завданнями більшої сфери управління. Наприклад, стосовно енергетичної інфраструктури плани стійкості енергозабезпечення громад мають стати складовими частинами плану енергетичної стійкості України.

Отже, основною метою цього дослідження є визначення змісту діяльності потенційних суб'єктів забезпечення стійкості функціонування КІ та надання ЖВФ на місцевому рівні. Усвідомлення діапазону завдань, змісту та можливих механізмів діяльності потенційних учасників реагування у перспективі дозволить запропонувати організаційно-інституційні зміни відповідно до післявоєнної політичної та адміністративної моделі організації влади в Україні.

Розділ 2. БЕЗПЕКА ТА СТІЙКІСТЬ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ФОРМАЛІЗАЦІЯ МОДЕЛІ ТА ВСТАНОВЛЕННЯ ВИМОГ

2.1. Безпека критичної інфраструктури як складова частина планів стійкості

Країна створює перелік життєво важливих функцій / послуг та визначає відповідальні інституції, діяльність яких зосереджується на питаннях стійкості забезпечення цих послуг¹²⁷. Ці інституції розробляють і реалізують плани стійкості ЖВФ та плани захисту критичної інфраструктури, яка забезпечує їх надання¹²⁸.

Зазвичай аспекти безпеки КІ врегульовуються завдяки низці механізмів та інструментів, що розроблені для визначення необхідного рівня безпеки та забезпечення захисту КІ. Законом України «Про критичну інфраструктуру» для цих цілей визначено такі інструменти: проєктні загрози (національні, секторальні та об'єктові), плани захисту КІ та плани взаємодії залучених суб'єктів національної системи захисту КІ у процесі виконання завдань із захисту критичної інфраструктури. Такі плани переважно складають задля забезпечення безпеки визначених конкретних об'єктів КІ.

Цей інструментарій дає змогу сформувати цілісний механізм визначення базового рівня захисту відповідно до ідентифікованих загроз КІ, укласти перелік заходів захисту КІ та розробити узгоджений план взаємодії всіх стейкхолдерів.

Базовий рівень захисту КІ / базовий рівень вимог до організації захисту пропонується встановлювати за результатами ідентифікації та аналізу впливу загроз¹²⁹. На основі проведеної оцінки формується перелік найбільш актуальних загроз критичній інфраструктурі та сценаріїв їх реалізації, що формалізується у проєктній загрозі¹³⁰.

¹²⁷ В Україні визначено понад 120 основних послуг (які варто вважати відповідником ЖВФ) у 25 секторах КІ (див.: Про Деякі питання об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 20.10.2020 № 1109. URL: <https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text>).

¹²⁸ Див.: Підпункт 4) пункту 1 статті 19 «Секторальні органи у сфері захисту критичної інфраструктури» Закону України «Про критичну інфраструктуру» (див.: URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>).

¹²⁹ Щорічну оцінку ризиків і загроз критичній інфраструктурі національного рівня здійснює Уповноважений орган у сфері захисту критичної інфраструктури (стаття 16 Закону України «Про критичну інфраструктуру»), залучаючи функціональні та секторальні органи у сфері захисту критичної інфраструктури.

¹³⁰ Підготовка проєктних загроз критичній інфраструктурі здійснюється на різних рівнях управління: національному, секторальному, об'єктовому.

Проектна загроза критичній інфраструктурі є документом, який визначає властивості, характеристики реальних і потенційних загроз для об'єктів КІ. На зниження вірогідності реалізації цих загроз та пом'якшення наслідків їхнього впливу спрямовується розроблення плану захисту. Під час проведення аналізу наслідків впливу загроз необхідно враховувати сценарії реалізації останніх, зокрема потенційні цілі впливу (наприклад, вплив на персонал, системи управління, окремі технологічні установки чи будівлі (об'єкти), територію об'єкта КІ тощо). Визначена правдоподібність реалізації загрози (від 1 до 5) зумовлює базовий рівень вимог щодо захисту (заходи реагування на визначений рівень загроз), який має бути забезпечений Оператором КІ. Подібний підхід реалізовано в США у спосіб запровадження стандартів управління ризиками Операторами КІ¹³¹.

На основі проектної загрози Оператори КІ розробляють плани захисту, реагування та взаємодії із залученими суб'єктами на випадок реалізації визначеної загрози. Прикладом застосування такого механізму є рекомендації з розроблення плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «кібератака / кіберінцидент»¹³².

Заходи захисту щодо кожної із визначених загроз (сценаріїв) можна розробити, урахувавши кілька рівнів захисту (наприклад, від рівня 1 – низьковитратні заходи Оператора КІ до рівня 5 – максимальне залучення сил ресурсів визначеного рівня управління). Рівень захисту – визначений комплекс заходів забезпечення захисту КІ відповідно до рівня впливу загроз, визначених проектною загрозою об'єктового рівня.

Рекомендації щодо розмежування заходів захисту за рівнями захисту наведено у *табл. 2*.

Конкретні заходи захисту розробляє Оператор КІ із залученням інших стейкхолдерів. На основі розроблених заходів та визначення необхідних ресурсів і повноважень, які необхідні для практичної імплементації заходів, формуються плани взаємодії Операторів КІ із усіма іншими суб'єктами реагування (*табл. 3*).

¹³¹ Стандарт визначає критерії та процеси, які особи, відповідальні за безпеку об'єкта, мають використовувати для визначення рівня безпеки об'єкта. Цей стандарт забезпечує вказівки щодо налаштування засобів протидії для всіх невійськових федеральних об'єктів (*див.*: The Risk Management Process: An Interagency Security Committee Standard. CISA, 2021. URL: <https://www.cisa.gov/resources-tools/resources/isc-standard-risk-management-process>).

¹³² Про затвердження Рекомендацій з розроблення плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «кібератака/кіберінцидент»: Наказ Адміністрації Держспецзв'язку від 01.12.2023 № 1011. URL: <http://surl.li/smppz>

Таблиця 2. Заходи щодо захисту критичної інфраструктури залежно від його рівня та відповідальні за їх реалізацію суб'єкти реагування

Орієнтовні заходи захисту критичної інфраструктури	Відповідальні суб'єкти та їхні функції
<i>Рівень захисту 1</i> (низьковитратні заходи Оператора КІ)	
Застосовуються організаційно-технічні заходи: пропускний режим; камери спостереження; інструкції на робочому місці; базове технологічне обладнання; фізична безпека персоналу тощо	Заходи розробляє й реалізовує власними силами та ресурсами Оператор КІ відповідно до вимог штатного режиму та рекомендацій уповноваженого, секторальних і функціональних органів щодо забезпечення захисту від визначених типів загроз
<i>Рівень захисту 2</i> (заходи активації готовності Оператора КІ)	
Приймаються організаційні та упроваджуються технічні рішення щодо посилення захисту об'єкта КІ: цілодобова фізична охорона території та окремих об'єктів; системи візуального контролю периметру й території; сигналізація; додаткові технічні рішення; інструктаж персоналу; перевірка готовності систем та ресурсів тощо	Оператор КІ ухвалює рішення, а потім реалізовує їх власними силами та ресурсами за консультаційної підтримки уповноваженого, секторальних та функціональних органів, а також місцевих учасників реагування на території розміщення критичної інфраструктури
<i>Рівень захисту 3</i> (заходи реагування на об'єктовому рівні)	
Посилюються організаційні та вдосконалюються інженерно-технічні рішення щодо захисту об'єкта КІ та прилеглої території: детальний інструктаж персоналу щодо дій; посилення режиму охорони та пропускного режиму; обладнання додаткових фізичних бар'єрів та запровадження інженерно-технічних рішень щодо запобігання реалізації (впливу) загрози; підготовка обладнання матеріалів, ресурсів, необхідних для функціонування КІ на випадок впливу загрози тощо	Оператор КІ ухвалює та впроваджує рішення власними силами з активацією заходів і ресурсів, передбачених планами захисту та взаємодії інших Операторів, а також із залученням сил і ресурсів інших стейкхолдерів (суб'єкти реагування та місцеві учасників) у випадках та порядку, визначеному законодавством

Орієнтовні заходи захисту критичної інфраструктури	Відповідальні суб'єкти та їхні функції
Рівень захисту 4 (заходи реагування із залученням сил та ресурсів територіального розміщення КІ)	
Упроваджуються організаційні та інженерно-технічні рішення, передбачені для реагування на критичний вплив загрози: посилення сил безпеки та охорони; використання передбачених на випадок кризового реагування ресурсів та матеріалів; залучення сил та ресурсів, а також координація дій залучених суб'єктів реагування відповідно до планів взаємодії	Оператор КІ й інші залучені стейкхолдери та суб'єкти системи захисту спільно розробляють заходи захисту й реалізують їх відповідно до планів взаємодії на визначеному рівні управління
Рівень захисту 5 (заходи надзвичайного реагування)	
Реалізуються рішення, передбачені для кризового реагування державного рівня: повноцінне застосування суб'єктами національної системи захисту планів взаємодії та використання всіх наявних сил і ресурсів на випадок кризового реагування тощо	Оператор КІ та інші суб'єкти національної системи захисту спільно приймають рішення й реалізують відповідні заходи за допомогою сил і засобів сектору безпеки та оборони України відповідно до планів взаємодії. У випадках запровадження надзвичайного / воєнного стану Оператор КІ діє відповідно до визначеного законодавством порядку та надає допомогу в реалізації заходів захисту

Джерело: розроблено автором.

Пропонований механізм визначення базового рівня захисту КІ дозволяє формалізувати процес розроблення планів захисту та взаємодії для забезпечення безпеки КІ. Але потрібно звернути увагу на висвітлені нижче важливі аспекти планування.

Загалом державна політика (чи стандарти корпоративної культури) щодо управління ризиками може спростити методологію формування вимог до забезпечення безпеки КІ, тобто вимог до формування плану захисту. Відповідні державні інституції можуть визначати необхідність оцінювання загроз, і, до речі, не завжди за п'ятирівневою шкалою критичності впливу. Наприклад, інституції США у практичній діяльності використовують три рівні такого впливу (Tiers 1–3), а у Великій Британії для подальшого аналізу беруть один рівень (*обґрунтовано найгірший сценарій*). Тобто Оператор КІ може розробляти скорочений набір заходів захисту відповідно до проведеного оцінювання ризиків реалізації загроз.

Окрім того, забезпечення безпеки КІ (підвищення опірності КІ до впливу загроз) є елементом ширшого завдання – забезпечення стійкості надання ЖВФ. Питання стійкості надання таких функцій / послуг виходить за межі відповідальності та спроможності окремих Операторів КІ і вимагає залучення широкого кола учасників та формального нормативного закріплення завдань для кожного з них.

Відповідно, постає завдання щодо розроблення методології формалізації завдань і заходів забезпечення стійкості КІ та надання послуг. Такі зусилля спрямовуються на забезпечення стійкості країни до загроз будь-якого типу та надання ЖВФ визначеного рівня для кінцевих споживачів, навіть за умов втрати критичної інфраструктури.

Таблиця 3. Формалізація розроблення планів захисту КІ та взаємодії суб'єктів реагування

Складники сценарію впливу загрози	Рівень захисту КІ					Заплановані заходи та відповідальні за них		Плани взаємодії
	1	2	3	4	5	Оператор КІ	Суб'єкти системи захисту КІ	
Сценарій 1								
Об'єкт	311, 312	313, 314	315, 316			311, 312, 314	313, 315, 316 – суб'єкти 1, 4	Оператор КІ; суб'єкти 1, 4
Персонал	321, 322	323, 324	325, 326			321–324		
Система управління	331, 332	333, 334	335, 336	337		331–334	333, 336 – суб'єкт 1; 335–337 – суб'єкти 3, 4	Оператор КІ; суб'єкти 1, 3, 4
Територія	341, 342	343, 344	345, 346	347, 348	349, 3410	341–345, 347	345 – суб'єкти 1, 2; 346 – суб'єкт 6; 347, 348 – суб'єкт 3	Оператор КІ; суб'єкти 1–3, 6
Сценарій 2								
Об'єкт	361, 362	363, 364	365, 366	367		361–333, 366	364 – суб'єкти 1, 3; 365 – суб'єкт 4; 346, 367 – суб'єкт 5	Оператор КІ; суб'єкти 1, 3–5
Персонал	371, 372	373, 374	375, 376	377, 378	379, 3710	371–376	367 – суб'єкти 1, 3; 368 – суб'єкт 2; 379, 3710 – суб'єкти 6, 9	Оператор КІ; суб'єкти 1–3, 6, 9
Система управління	381, 382	383, 384	385			381–385		
Територія	391, 392	393, 394	395, 396	397, 398	399	391–395, 398	396–399 – суб'єкти 6, 7–9	Оператор КІ та Суб'єкти 6, 7–9

Примітка. Літера З означає «захід»; цифри після неї вказують на його порядковий номер; кольори комірок вказують на заходи реагування відповідно до визначеного рівня впливу загроз (від 1 до 5) за даним сценарієм; заходи, визначені у позначених кольором комірках, обов'язкові для включення до плану захисту; заходи, позначені в комірках без кольору, вказують на потенційні заходи реагування (на випадок, якщо рівень загроз підвищиться).

Джерело: розроблено автором.

2.2. Формалізація вимог щодо стійкості надання життєво важливих функцій / послуг та функціонування критичної інфраструктури

Національна система готовності (The National Preparedness System¹³³) окреслює завдання та формалізує процес забезпечення готовності всіх можливих учасників до спільної та координованої діяльності задля забезпечення сталого розвитку суспільства та стійкості до загроз будь-якого типу. Метою цієї системи є стійка та безпечна нація, яка володіє спроможністю, залучаючи зусилля всього суспільства, *запобігати, захищати, пом'якшувати, реагувати* та *відновлюватися* після загроз і небезпек, що становлять найбільший ризик¹³⁴.

Важливим є зміст діяльності, характерний для цих етапів циклу кризового реагування:

- *запобігання* – не допущення, уникнення або припинення впливу загроз та небезпек;
- *захист* – убезпечення громадян, активів, об'єктів від найбільших загроз і небезпек таким чином, щоб національні інтереси, прагнення та спосіб життя процвітали;
- *пом'якшення наслідків* – зменшення втрат життя та майна шляхом послаблення наслідків впливу загроз (виникнення потенційних катастроф);
- *реагування* – швидкі дії у відповідь на виникнення загроз та кризових ситуацій;
- *відновлення* – забезпечення своєчасного відновлення, зміцнення та відбудови інфраструктури, житла та економіки тощо громад, які постраждали.

Національні цілі готовності (The National Preparedness Goal¹³⁵) конкретизують завдання, визначають набір основних спроможностей і компетентностей у відповідних п'яти сферах діяльності для забезпечення національної готовності до виникнення кризових ситуацій¹³⁶. При цьому наголошується, що необхідні спроможності не розглядаються завданням для окремого суб'єкта реагування (уряду, органу влади чи організації), а є вимогою щодо забезпечення взаємодії між усіма стейкхолдерами та об'єднання зусиль усього суспільства.

¹³³ National Preparedness System. URL: <https://www.fema.gov/emergency-managers/national-preparedness/system>

¹³⁴ Див.: URL: <https://www.fema.gov/emergency-managers/national-preparedness/goal>

¹³⁵ National Preparedness Goal. Second Edition. September 2015. URL: https://www.fema.gov/sites/default/files/2020-06/national_preparedness_goal_2nd_edition.pdf

¹³⁶ Див.: URL: <https://www.fema.gov/emergency-managers/national-preparedness/mission-core-capabilities>

Отже, стійкість функціонування КІ та надання ЖВФ суспільству досягається завдяки узгодженому комплексу заходів циклу кризового реагування, котрі зазначені нижче.

1. Запобігання або уникнення впливу загроз

Йдеться про реалізацію заходів щодо формування спроможностей для уникнення, запобігання або припинення впливу ідентифікованих загроз. Водночас застосовуються заходи профілактики щодо загроз, підвищення рівня усвідомленості стосовно всіх типів загроз, здійснюється розвиток спроможностей реагування різних стейкхолдерів.

2. Захист від впливу загроз

Захист КІ, людей, функцій / послуг тощо від найбільших загроз будь-якого типу (all-hazards approach) має здійснюватися так, щоб реалізація національних інтересів, проєктні режими функціонування КІ, спосіб життя громадян країни зберігалися й розвивалися. Заходи під час цього етапу циклу кризового реагування зосереджуються на діях, спрямованих на підвищення опірності до впливу найбільших загроз.

3. Пом'якшення впливу загроз, зменшення людських втрат і матеріальних збитків

Цей етап передбачає застосування заходів, які необхідні для зменшення наслідків реалізації загроз. Ідея таких заходів полягає в тому, що країна та суспільство стають значно стійкішими, якщо наслідки реалізації загроз, тривалість їхнього впливу, фінансові та людські витрати на реагування та відновлення буде зменшено. Заходи щодо пом'якшення стосуються різних сфер життєдіяльності країни (окремі особи, приватний і некомерційний сектори, громади, КІ, довілля та ін.), що вимагає розуміння загроз та оцінки ризиків їх реалізації. Тобто на цьому етапі все суспільство, залучені стейкхолдери відіграють важливу роль¹³⁷ та потребують залучення до обміну інформацією та планування стійкості громади, країни, КІ чи ЖВФ.

4. Реагування на реалізацію та вплив загроз

Швидке та ефективне реагування дозволяє суттєво знизити наслідки впливу загроз. Заходи цього етапу зосереджуються на скоординованих діях різних стейкхолдерів, спрямованих на: порятунок та підтримку життя людей, стабілізацію ситуації, швидке задоволення визначеного рівня основних потреб, базових послуг / функцій, збереження функціональності інфраструктури, громади, створення безпечного середовища життєдіяльності та підтримку переходу до відновлення. Залучення громади є життєво важливою ланкою для

¹³⁷ Залежно від методології виокремлення етапів циклу кризового реагування пропонувані заходи такого змісту можуть увійти до етапу «Захист» або «Реагування».

додаткової підтримки суб'єктів реагування і часто може бути основним джерелом робочої сили в перші години та дні кризи.

5. Відновлення функціонування КІ, послуг / функцій, життєдіяльності

Це заходи, спрямовані на своєчасне відновлення, зміцнення та відродження інфраструктури, житла та економіки, а також охорони здоров'я, організаційної структури забезпечення життєдіяльності громад. Під час цього етапу циклу реагування на кризову ситуацію заходи з відновлення мають передбачати підвищення стійкості до загроз, спільне інклюзивне планування всіма зацікавленими стейкхолдерами, розвиток їхнього потенціалу для ефективного управління процесом відновлення. Ця місія потребує вивчення уроків з кризової ситуації, розроблення заходів щодо відновлення функціонування КІ, життєдіяльності громад тощо на базі кращих доступних технологій і практик (Bounce Back Better), недопущення подібних ситуацій повторно.

Загальні вимоги щодо стійкості функціонування КІ формуються з урахуванням цієї ширшої рамки забезпечення національної безпеки та сталості суспільного розвитку.

Водночас у системі безпеки та стійкості функціонування КІ для визначення завдань залучених учасників відповідно до етапів циклу реагування на кризову ситуацію виокремлено чотири групи заходів, що різняться за змістом (*табл. 4*).

Таблиця 4. Зміст діяльності та приклади заходів із забезпечення стійкості критичної інфраструктури за різних режимів її функціонування

Зміст діяльності	Приклади заходів
Режим функціонування КІ – Штатний	
<p>Ідентифікація потенційних загроз і можливих наслідків їх реалізації; підготовка заходів із запобігання впливу загроз (зокрема, організація захисту КІ), пом'якшення наслідків впливу; планування взаємодії на випадок виникнення кризи; вивчення уроків реагування (власного та світового досвіду). Діяльність відображає спроможність КІ стабільно функціонувати у проєктному режимі, готовність суб'єктів реагувати на визначений спектр і рівень загроз з метою забезпечення стійкості надання функцій / послуг</p>	<p>Ідентифікація критичних загроз і визначення вимог щодо рівня захисту. Підготовка сил та засобів захисту відповідно до визначеного рівня загроз / небезпек. Встановлення / моніторинг засобів контролю фізичного доступу. Розроблення планів стійкості функціонування КІ, надання послуг (планів безперервності бізнесу). Підготовка планів взаємодії залучених суб'єктів для забезпечення захисту КІ та взаємодії на випадок виникнення кризових ситуацій і порушення надання функцій / послуг. Навчання персоналу. Проведення регулярних тренінгів для перевірки планів дій залучених суб'єктів. Створення механізмів обміну інформацією</p>
Режим функціонування КІ – Готовність та запобігання	
<p>Уникнення, протидія та/або поглинання впливу загрози, зменшення серйозності впливу або наслідків реалізації загроз. Діяльність відображає спроектовану у штатному режимі надійність функціонування КІ в умовах впливу визначеного рівня загроз та готовність суб'єктів реагування до дій</p>	<p>Модернізація об'єктів КІ для уникнення критичного впливу природних небезпек (наприклад, обладнання для захисту від повеней, бар'єри проти паводків) та визначених пріоритетних фізичних загроз. Оновлення обладнання, що не відповідає вимогам захищеності до ідентифікованих загроз. Підготовка та активація готовності суб'єктів реагування до реалізації визначених загроз. Підготовка заходів щодо пом'якшення наслідків впливу різних небезпек / загроз. Створення резервних центрів управління (виробництв), що можуть продовжувати роботу після інциденту та сприяти відновленню. Усвідомлення міжсекторальної залежності від ключових зовнішніх ресурсів (електроенергії, палива, води, зв'язку), підготовка додаткових запасів (наприклад, палива, резервних генераторів, резервного зв'язку)</p>

Зміст діяльності	Приклади заходів
Режим функціонування КІ – Реагування	
<p>Виконання заходів, які розроблені задля реагування на реалізацію загрози / небезпеки та адаптації до несприятливих наслідків. Діяльність відображає підготовленість, оперативну майстерність і винахідливість суб'єктів реагування в управлінні кризою</p>	<p>Підтримка на місці можливостей реагування на визначені загрози (наприклад, кліматичні умови, розливи хімікатів, пожежі, вибухові речовини, збройний напад). Налагодження відносин із місцевими службами швидкого реагування та міжгалузевими партнерами. Заходи задля розвитку спроможностей суб'єктів реагування до управління інцидентами на місці (доступність ресурсів, навчений персонал, оперативний центр, що функціонує, розуміння міжсекторальних проблем тощо)</p>
Режим функціонування КІ – Відновлення	
<p>Реалізація заходів, розроблених для того, щоб допомогти повернути параметри функціонування КІ (робочі умови) до необхідного цільового рівня (на кращому рівні). Діяльність відображає здатність швидко відновити роботу послуг</p>	<p>Встановлення пріоритетних угод щодо відновлення з ключовими постачальниками послуг / функцій, від яких залежить відновлення цільових параметрів функціонування КІ (наприклад, угоди з постачальниками обладнання, підтримка аварійного постачання, підготовлені ремонтні команди). Оцінка та планування часу і короткострокових заходів, необхідних для відновлення повноцінної роботи після збою (також заходи швидкої заміни / ремонту критичних компонентів). Визначення стратегії довгострокового розвитку (наприклад, відновлення до «проектного» рівня чи трансформація з урахуванням вивчених уроків)</p>

Джерело: адаптовано автором з урахуванням ¹³⁸.

Вимоги щодо забезпечення стійкості подамо схематично як зразок моделі кризового реагування для забезпечення стійкості цільової функції (рис. 2).

Варто порівняти вимоги Закону України «Про критичну інфраструктуру» щодо формалізації дій суб'єктів національної системи захисту критичної інфраструктури у чотирьох режимах функціонування КІ та місій суб'єктів Національної системи готовності та системи безпеки і стійкості КІ США у зіставленні із типовими етапами розвитку кризової ситуації.

¹³⁸ Methodology for Assessing Regional Infrastructure Resilience. Lessons Learned from the Regional Resiliency Assessment Program. CISA 2021. URL: [https://www.cisa.gov/sites/default/files/publications/DIS_DHS_Methodology_Report_ISD %20EAD %20Signed_ with %20alt-text_0.pdf](https://www.cisa.gov/sites/default/files/publications/DIS_DHS_Methodology_Report_ISD_%20EAD_%20Signed_with_%20alt-text_0.pdf)



Рис. 2. Модель кризового реагування для забезпечення стійкості цільової функції
 Джерело: розроблено автором.

Застосування розробленої моделі дозволяє обґрунтувати підходи до формалізації заходів та цілей розроблення планів стійкості, зокрема щодо визначення:

- штатного діапазону параметрів, рівня допустимих загроз, порядку та часу попередження інших систем щодо загроз, штатної процедури реагування тощо;
- параметрів критичних загроз, засобів і процедур запобігання та пом'якшення впливу загроз, порядку взаємодії з іншими системами під час протидії загрозі тощо;
- процедур реагування, час реагування, процедур отримання допомоги тощо;
- вимог щодо резервування, процедур взаємодії при відновленні, часу відновлення тощо¹³⁹;
- допустимого діапазону та часу обмеження функціональності, адаптації до нової ситуації, вивчення уроків системою управління тощо.

¹³⁹ Наприклад, на думку одного із Операторів системи розподілу в Україні, час переходу об'єктів КІ на резервні джерела енергії (на випадок втрати централізованого електрозабезпечення) не повинен перевищувати 30 хвилин.
 (див.: Енергетики ДТЕК разом з Київською обласною військовою адміністрацією та ДСНС перевірили готовність критичної інфраструктури Київщини за потреби працювати від альтернативного живлення / ДТЕК. 2023. 26 жовт. URL: <http://surl.li/snjhs>).

Розроблену модель забезпечення стійкості ЖВФ та визначення параметрів регулювання варто застосовувати до кожної із загроз та/або сценаріїв її реалізації¹⁴⁰.

Ця модель допомагатиме суб'єктам, які відповідальні за планування стійкості, здійснювати розроблення чіткого порядку дій, аналізувати загрози та ризику та дозволить усвідомити необхідні параметри цільової функції¹⁴¹ (час аварійного реагування, відновлення та рівні обмеження функціональності), а також можливості регулювання цих параметрів¹⁴² (заходи щодо підвищення готовності до впливу загроз, пом'якшення такого впливу, реагування на вплив загрози, відновлення проєктних параметрів надання послуги).

2.3. Узагальнення практики реагування на порушення функціонування критичної енергетичної інфраструктури

Порівняльний аналіз дій залучених суб'єктів реагування можна провести, виокремлюючи певні етапи кризового реагування та визначаючи відповідні завдань і механізми реагування. Це допоможе осмислювати кращий досвід, удосконалювати планування стійкості функціонування КІ та надання ЖВФ на різних рівнях управління.

У цій публікації на прикладі України (блокування постачання палива, фізичне руйнування інфраструктури) та США (природні впливи та кібератака) висвітлено узагальнені результати аналізу цих чотирьох випадків порушення послуги енергозабезпечення споживачів, що сталось унаслідок впливу різних загроз (додаток 2).

Зіставлення причин виникнення кризової ситуації, динаміки її розвитку, дій залучених суб'єктів реагування дозволяє сформулювати такі узагальнення:

– кожна загроза зумовлює формування унікальних вимог щодо безпеки та стійкості функціонування КІ, що, своєю чергою, потребує усвідомлення всіма суб'єктами реагування (йдеться про органи державної влади на різних

¹⁴⁰ Сценарій реалізації загроз може містити не тільки послідовність подій, тривалість впливу, критичність впливу, але й сукупність різних загроз (комплексні загрози).

¹⁴¹ Цільові параметри реагування визначаються нормативно-правовими актами, також завдяки аналізуванню потреб споживачів послуги (наприклад, встановлюється допустимий термін відсутності електроенергії відповідно до технологічних вимог (лікарні, відведення води, хімічне виробництво)), потреб / вимог конкретних споживачів (громади).

¹⁴² Можливі рішення з регулювання параметрів (повернення до проєктних режимів функціонування) визначаються заздалегідь заходами щодо: підвищення готовності до впливу загроз (посилення захисту, накопичення ресурсів та обладнання); пом'якшення (диверсифікації джерел енергоживлення, використання запасів та ресурсів усіх, заміщення послуг / функцій іншими); реагування (скорочення потреб, використання резервних джерел енергії); відновлення (ремонт та відбудова, нові способи забезпечення потреб споживачів тощо).

рівнях управлінської вертикалі, Операторів КІ, споживачів послуг) та іншими стейкхолдерами загроз і наслідків їх реалізації (ризиків);

- ідентифікація загроз КІ та оцінка наслідків їх реалізації (ризиків), зокрема порушення функціонування / руйнування конкретної КІ у відповідній сфері планування (країна, галузь, територіальна громада, підприємство), стають основою для планування системи заходів забезпечення безпеки КІ;

- оцінка ризиків реалізації загроз (сукупних наслідків впливу загроз) є інструментом визначення кола стейкхолдерів, яких необхідно залучити до реалізації заходів захисту;

- необхідними є визначення та формалізація вимог до всіх учасників, які залучені до реагування на визначений тип загрози, та їхньої відповідальності;

- потрібно вчасно здійснювати розроблення планів стійкості, що ґрунтуються на сформованій системі взаємодії всіх залучених учасників реагування з метою забезпечення стійкості надання ЖВФ;

- усі залучені до реагування суб'єкти повинні мати чітке уявлення про розвиток ситуації, що вимагає забезпечення обміну інформацією між ними;

- забезпечення стійкості надання ЖВФ виходить за межі відповідальності Операторів КІ та потребує врегулювання процедур реагування та взаємодії на вищому рівні державного управління (регіональному, національному);

- важливим елементом забезпечення стійкості є вивчення уроків з попередніх інцидентів та відповідне коригування механізмів і заходів реагування.

Розділ 3. ЗАСАДИ РОЗРОБЛЕННЯ ПЛАНУ СТІЙКОСТІ ФУНКЦІОНУВАННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА НАДАННЯ ЖИТТЄВО ВАЖЛИВИХ ФУНКЦІЙ НА РІВНІ ТЕРИТОРІАЛЬНИХ ГРОМАД

3.1. Організація планування стійкості життєдіяльності громад

Наукові розвідки фахівців Національного інституту стратегічних досліджень у сфері розбудови національної стійкості засвідчують, що «відсутність в Україні єдиного розуміння механізму забезпечення національної стійкості, процесів, які він охоплює, а також організації національної системи стійкості суттєво ускладнює запровадження відповідних процесів на рівні регіонів і територіальних громад»¹⁴³.

Саме на подолання проблеми усвідомлення цілей та змісту діяльності суб'єктів забезпечення стійкості функціонування КІ, яка підтримує життєдіяльність громад, а також можливих механізмів формалізації такої діяльності спрямовується це дослідження.

Основними механізмами підвищення стійкості життєдіяльності громад мають стати постійно діючі формати взаємодії органів державної та місцевої влади, підприємств та організацій, жителів громад та інших стейкхолдерів¹⁴⁴, а також розроблений на місцевому рівні формалізований документ, який би окреслював дії, що потребують координування, всіх залучених учасників реагування при підготовці до виникнення кризової ситуації, під час реагування на її виникнення та відновлення після подолання кризи¹⁴⁵.

Наявність розробленого заздалегідь до виникнення кризової ситуації плану стійкості дозволяє громадам краще підготуватись до майбутніх викликів і швидше, із меншими втратами подолати потенційну кризу. Навіть якщо криза сталася, стійка громада переважно знатиме, як зменшити потенційні збитки та якнайшвидше відновитись на вищому ступені готовності до майбутніх викликів.

У США з метою надання підтримки громадам розроблено методичні рекомендації щодо забезпечення стійкості життєдіяльності громад¹⁴⁶, які

¹⁴³ Організація системи забезпечення національної стійкості на регіональному і місцевому рівнях : аналіт. доп. / [Резнікова О. О., Войтовський К. Є., Лепіхов А. В.] ; за заг. ред. О. О. Резнікової. Київ : НІСД, 2021. 112 с.

¹⁴⁴ Прикладом подібної форми організації співпраці різних стейкхолдерів є досвід Великої Британії щодо створення місцевих форумів стійкості (див.: попередній розділ).

¹⁴⁵ Прикладом подібної практики формалізації діяльності з питань стійкості енергозабезпечення є досвід США (див.: попередній розділ).

¹⁴⁶ Local Mitigation Planning Policy Guide. FEMA. FP 206-21-0002. Released April 19, 2022. URL: https://www.fema.gov/sites/default/files/documents/fema_local-mitigation-planning-policy-guide_042022.pdf

пропонується використовувати і в Україні для розроблення планів стійкості функціонування КІ та надання ЖВФ. Методичні нароби також представлені на рівні планування стійкості інфраструктури.

У Рекомендаціях із планування стійкості будівель та інфраструктурних систем (Community Resilience Planning Guide for Buildings and Infrastructure Systems) пропонується наведена нижче послідовність дій, якої варто дотримуватися під час планування стійкості КІ та надання ЖВФ на рівні громад¹⁴⁷.

1. Створення організаційної структури планування стійкості громади:

- визначення лідера (суб'єкта) забезпечення стійкості для громади (або іншої сфери управління);
- формалізація групи спільного планування: визначення членів цієї групи, їхніх функцій та обов'язків;
- визначення ключових державних і приватних зацікавлених сторін для всіх етапів планування та впровадження.

2. Усвідомлення важливих аспектів та особливостей забезпечення стійкості громади:

- визначення особливостей сфери управління (усвідомлення важливих соціально-економічних, ресурсних, технологічних характеристик життєдіяльності громади); уточнення переліку ЖВФ, встановлення взаємозалежностей між функціями; усвідомлення вразливостей та ризиків для громади при порушенні надання функцій / послуг;
- ідентифікація КІ, яка забезпечує надання ЖВФ (інфраструктурні системи, будівлі, конструкції тощо, у т. ч. стан, розташування та залежності між інфраструктурними системами);
- визначення ключових контактів / представників для оцінювання, координації та прийняття рішень з питань забезпечення стійкості життєдіяльності громади;
- ідентифікація існуючих поточних планів, які мають бути скоординовані (ураховані, модернізовані) з планом забезпечення стійкості громади.

3. Визначення цілей і завдань планування стійкості громади:

- визначення довгострокових цілей громади (або іншої сфери управління) в аспекті перспективного розвитку з врахуванням інтересів громади;

¹⁴⁷ Community Resilience Planning Guide for Buildings and Infrastructure Systems. Volume I. NIST Special Publication 1190. URL: <http://dx.doi.org/10.6028/NIST.SP.1190v1> <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1190v1.pdf>

- встановлення цілей щодо ефективності заходів забезпечення стійкості життєдіяльності громади на основі потреб громади, а також залежностей і каскадних ефектів між системами;

- ідентифікація загроз (небезпек) громаді (іншій сфері управління), рівні їхнього впливу та визначення наслідків впливу загроз на життєдіяльність громади (рівні надання ЖВФ, функціонування КІ, економічні збитки тощо);

- визначення рівнів очікуваного падіння ефективності надання життєво важливих функцій / послуг та необхідних рівнів для підтримки життєдіяльності громади на основі потреб громади.

4. Розроблення плану стійкості:

- визначення розбіжностей між наявними та необхідними рівнями надання ЖВФ та існуючими спроможностями КІ за умов реалізації визначених сценаріїв впливу загроз;

- розроблення рішень задля усунення розбіжностей між потребами та існуючими спроможностями з урахуванням адміністративно-організаційних, економічних та будівельних варіантів;

- визначення пріоритетів під час застосування розроблених рішень (на основі техніко-економічних оцінок), підготовка стратегії їх упровадження.

5. Підготовка, перегляд і затвердження плану:

- формалізація та затвердження плану стійкості громади (або іншої сфери управління);

- публічне обговорення в межах громади, отримання відгуків від зацікавлених сторін і спільноти та уточнення плану з врахуванням результатів обговорення;

- затвердження плану стійкості.

6. Реалізація та підтримка плану стійкості громади:

- виконання затверджених рішень, реалізація проєктів;

- комунікація з громадою та зацікавленими сторонами щодо реалізації плану;

- періодичне оцінювання стану виконання та оновлення плану.

До процесу розроблення плану стійкості громади треба залучати максимальну кількість усіх зацікавлених осіб. Ураховуючи важливість забезпечення стійкості життєдіяльності громади та складність імплементації плану стійкості, необхідно переконатися, що громада загалом знає та розуміє цей план. Важливо також, щоб потенційні стейкхолдери були максимально готові долучитись до виконання завдань, визначених планом стійкості громади в різних аспектах діяльності. По завершенні роботи проєкт розробленого плану

стійкості доцільно представити громаді для обговорення та врахування додаткових пропозицій.

Підготовка планів стійкості дає можливість сформувати у громаді спроможності, властиві самодостатній системі. Йдеться, зокрема, про формування ефективного лідера громади (суб'єкта управління); удосконалення готовності й реагування на загрози життєдіяльності громади та її розвитку; налагодження співпраці між усіма членами громади, усвідомлення ними внутрішніх і зовнішніх залежностей; створення системи управління ризиками, забезпечення безперервності бізнесу тощо.

3.2. Зміст етапів підготовки плану стійкості

Організація та завдання планування

Під час розроблення плану стійкості задля узгодження завдань і цілей та координації діяльності стейкхолдерів формується *Група планування*. До її складу залучають різних учасників з боку державного та приватного сектору, громадських організацій, працівників наукових установ, представників жителів громади та ін.

Зазвичай у рамках діяльності Групи планування створюються окремі робочі групи для опрацювання окремих (технологічних, фінансових, ресурсних, комунікаційних) аспектів планування, які допомагають докладно та обґрунтовано визначити цільові параметри забезпечення стійкості надання ЖВФ та функціонування КІ.

При розробленні плану стійкості Група планування:

- визначає чіткі межі сфери планування, передусім щодо критично необхідних для життєдіяльності громади ЖВФ, інфраструктури та ланцюжків постачання, котрі забезпечують надання послуг кінцевим споживачам, географічних особливостей і територіальних меж планування;

- зважає на соціально-економічні особливості життєдіяльності громади (наприклад, бере до уваги місце й види господарської діяльності, чисельність і склад населення, обсяги транспортування вантажів і людей з(до) громади, місце та час найбільшого скупчення людей, рівень самозабезпеченості громади енергією, водою, продовольством тощо);

- ураховує взаємозалежності функцій / послуг та/чи КІ (наприклад, залежність одних функцій від інших у межах громади (за межами громади); імовірність виникнення різного виду потенційних каскадних ефектів впливу

загроз; можливість виникнення чинників, що перешкоджатимуть / сприятимуть швидкому відновленню; здатності до заміщення тощо);

– визначає критичні загрози та здійснює оцінювання ризиків їх реалізації, що впливатиме на життєдіяльність громад (наприклад, опрацьовує перелік критичних загроз, вплив яких необхідно знизити; встановлює правдоподібність та рівні критичності впливу цих загроз); оцінює наслідки впливу загроз (зниження рівня надання функцій / послуг чи порушення / руйнування КІ, економічні втрати, втрата робочих місць, необхідність переміщення людей тощо);

– встановлює цільові параметри надання функцій / послуг та/чи функціонування КІ (наприклад, час та рівні відновлення функціонування КІ, рівні самозабезпечення громади за окремими функціями / послугами (на випадок руйнування проєктної КІ), резервування обладнання й ресурсів тощо);

– узгоджує довгострокові цілі розвитку громади із завданнями забезпечення її стійкості, працює над розробленням конкретних заходів забезпечення стійкості за всіма етапами циклу кризового реагування;

– розроблює механізми об'єднання зусиль усіх стейкхолдерів для забезпечення стійкості громади.

Сфера (межі) планування

Під час розроблення плану стійкості насамперед потрібно визначити сфери планування стійкості та суб'єкта планування. Загалом пропонована методологія розроблення планів стійкості може застосовуватись для різних рівнів управління (країна, галузь, територіальна громада, підприємство).

У цьому дослідженні сферою планування обрано громаду. Термін уживаємо в значенні визначеному Законом України «Про місцеве самоврядування»: територіальна громада – жителі, об'єднані постійним проживанням у межах села, селища, міста, що є самостійними адміністративно-територіальними одиницями, або добровільне об'єднання жителів кількох сіл, селищ, міст, що мають єдиний адміністративний центр (суб'єкт управління. – *Авт.*).

Саме наявність спільної юрисдикції (або сфери формування й реалізації політики) та управлінської структури дозволяє забезпечити координацію дій інших стейкхолдерів, які можуть бути залучені до підготовки й реалізації плану стійкості. Отже, територіально-адміністративний устрій (сфери реалізації політики) є одним із чинників, що визначає сферу планування, про яке йдеться.

Іншим чинником, що визначає межі планувальної діяльності, можуть бути типи загроз, наприклад природні, технологічні, соціальні, воєнні тощо.

При визначенні відповідальності у різних суб'єктів реагування на різні типи загроз цей чинник може обмежити сферу планування. Наприклад, під час планування стійкості громад до уваги можуть братися лише загрози природного чи соціального характеру, а воєнні загрози перебуватимуть поза межами розроблення плану стійкості громади.

У дослідженні зважаємо на те, що порушення життєдіяльності громад може статись унаслідок впливу загроз будь-якого типу, а тому план забезпечення стійкості має охоплювати всі типи загроз. Своєю чергою, особливості реагування на загрози різних типів будуть ураховуватися при формуванні заходів реагування, що визначатиме, які суб'єкти системи реагування відповідно до визначених законодавством країни завдань та повноважень залучатимуться до реалізації цих рішень.

Плануючи стійкість життєдіяльності громади, найкраще брати за основу результати аналізу довгострокових цілей розвитку громади та цільові параметри важливих функцій / послуг, необхідних для життєдіяльності й розвитку громади. Саме надання ЖВФ є пріоритетом забезпечення стійкості громади.

Забезпечення надання визначених ЖВФ здійснюється завдяки інфраструктурним системам, як-от: енергетика, зв'язок, водопостачання та водовідведення, транспорт тощо, а також будівлям. Якщо ці системи виходять з ладу або пошкоджені, надання основних послуг може перерватися, що критично вплине на життєдіяльність громади.

Таким чином, визначення ЖВФ для конкретної сфери управління (громад відповідного рівня, галузей, функцій / послуг), цільових параметрів забезпечення стійкості життєдіяльності та забезпечувальних інфраструктурних систем є першим кроком у розробленні плану стійкості.

Зразок виконання попереднього аналізу пріоритетів забезпечення стійкості на визначених рівнях управління наведено в *табл. 5*.

Загалом розбудова системи планів стійкості передбачає формування горизонтальної (секторальної та міжсекторальної) та вертикальної (громада, область, країна) ієрархії. У такій структурі планів вищий рівень плану елемент більшої системи включає у себе плани нижчого рівня як ресурс чи інструмент. Закон України «Про критичну інфраструктуру» визначає необхідність забезпечення стійкості функціонування КІ за різними рівнями державного управління (загальнодержавним, регіональним та галузевим, місцевим, об'єктовим) та визначеного набору ЖВФ, стійкість яких він має забезпечити¹⁴⁸.

¹⁴⁸ Закон України «Про критичну інфраструктуру» визначає 17 життєво важливих функцій (відображають секторальну спрямованість), які постановою Кабінету Міністрів України «Деякі питання об'єктів критичної інфраструктури» від 09 жовтня 2020 р. № 1109 деталізуються у цілий набір основних послуг за секторальним розподілом (станом на лютий 2024 р. – 138 типів основних послуг).

Таблиця 5. Приклад примірного розподілу завдань суб'єкта управління щодо забезпечення стійкості надання життєво важливих функцій / послуг

Параметри планування	Зміст діяльності та завдання щодо забезпечення стійкості надання ЖВФ			
	Рівень громад ¹⁴⁹ (село, кілька сіл)	Рівень районів ¹⁵⁰ (кілька громад)	Рівень областей ¹⁵¹	Загальнодержавний рівень
Розмежування завдань забезпечення стійкості надання ЖВФ на відповідному рівні управління	Забезпечити короткострокове підтримання життєдіяльності територіальної громади	Забезпечити середньострокове підтримання життєдіяльності громад району	Забезпечити тривале підтримання визначеного набору функцій / послуг регіонального значення	Забезпечити безперервність функцій / послуг, важливих для забезпечення національної безпеки та урядування
Функції / послуги та межі планування				
Зв'язок	Зв'язок кожного населеного пункту із центром територіальної громади (мінімальний рівень – одна точка зв'язку з доступом для всіх жителів села (у сільраді, будинку культури))	Зв'язок усіх сіл із центром територіальної громади (традиційна система зв'язку та система дублювальна); зв'язок із об'єктами КІ та органами владних повноважень; зв'язок із обласним центром	Зв'язок із центрами територіальних громад та органами державної влади загальнодержавного рівня (традиційна система зв'язку та система дублювальна); зв'язок із Операторами КІ обласного рівня; Силами безпеки і оборони, розміщеними на території області	Зв'язок із органами державної влади обласного та загальнодержавного рівня (традиційна система зв'язку та система дублювальна); зв'язок із Операторами КІ; Силами безпеки і оборони

¹⁴⁹ На рівні територіальної громади зазвичай наявні такі інфраструктурні об'єкти: будівлі органів самоврядування, будинок культури, бібліотека, фельдшерський пункт, поштове відділення, школа, продовольчий магазин, фермерські господарства, централізоване водопостачання та газопостачання (щонайменше у частини громади), централізоване електропостачання всіх споживачів від районних мереж (на території села понижувальні трансформатори низької напруги 10 кВ/380 В), транспортне сполучення із центром громади.

¹⁵⁰ На рівні району: ЦНАП, органи самоврядування, поліклініка, банківські відділення, бази (нафтопродуктів, продовольства, матеріалів тощо), транспортні підприємства, що здійснюють пасажирські та вантажні перевезення, велика середня школа / гімназія, залізнична платформа та склад, вузол зв'язку, торговельний центр (ринок, магазини), завод по переробці (агропродуктів, молока, м'яса), окремі підрозділи органів державної влади тощо.

¹⁵¹ У рівні відповідальності області зазвичай наявні: органи влади (місцеві та центральні органи), вузлова залізнична станція, річковий порт, великі промислові підприємства, електростанція, котельні, водоканали, централізована система теплопостачання, магістральні та розподільчі мережі, заклади вищої освіти, лікарні, театри, будинки культури, торгові центри, військові частини тощо.

Параметри планування	Зміст діяльності та завдання щодо забезпечення стійкості надання ЖВФ			
	Рівень громад ¹⁴⁹ (село, кілька сіл)	Рівень районів ¹⁵⁰ (кілька громад)	Рівень областей ¹⁵¹	Загальнодержавний рівень
Транспортування	Забезпечення транспортного сполучення: підвезення хворих у районний медзаклад, працівників органів влади та кризового управління, постачання продовольства тощо	Визначений рівень транспортного сполучення (рівень пасажирських та вантажних перевезень між громадами, районним та обласним центром, транспортування хворих до спеціалізованих лікарень, продовольче забезпечення тощо)	50 % усіх послуг транспортного забезпечення надання життєво важливих функцій / послуг на обласному рівні (критичний рівень пасажирських та вантажних перевезень у межах області); 70 % транспортування ресурсів та сил реагування на кризову ситуацію	70 % усіх послуг транспортного забезпечення сектору безпеки і оборони
Електро-постачання	Мінімальний рівень електропостачання: сільрада, будинки культури, насосні станції, продовольчий магазин, живлення зв'язку, автозаправних станцій	Визначені мінімальні потреби територіальних громад району, потреби місцевих об'єктів інфраструктури, потреби громад району в адміністративних послугах, медичному обслуговуванні, місцевих виробництв	40 % потреб енергозабезпечення області на базі місцевих енергетичних ресурсів, джерел енергії, виробничих потужностей та накопичених місцевих запасів кризового реагування	100 % потреб енергозабезпечення сектору урядування загальнодержавного рівня; 70 % енергозабезпечення потреб сектору безпеки і оборони; 60 % енергозабезпечення потреб об'єктів КІ
Теплопостачання	Мінімально необхідний рівень забезпечення теплом населення громад: медичні заклади, навчальні установи, заклади, які надають адміністративні послуги	Визначений рівень забезпечення теплом працівників медичних закладів, освітніх установ, органів влади, установ, що надають адміністративні послуги населенню	70 % усіх потреб медичних закладів, освітніх установ; потреб органів влади, установ з надання адміністративних послуг населенню	100 % потреб органів влади, установ із надання адміністративних послуг населенню, загальнодержавних сервісів; медичних закладів загальнодержавного рівня
Урядування (реагування на кризові ситуації)	Забезпечення інформування населення громад та надання допомоги у кризовій ситуації	Забезпечення надання адміністративних послуг населенню району, підтримання виробничої активності підприємств	Забезпечення функціонування органів влади, підтримання громадського порядку, надання адміністративних послуг, функціонування	Забезпечення безперервності урядування, підтримання громадського порядку та безпеки, функціонування економіки, захист національних інтересів,

Параметри планування	Зміст діяльності та завдання щодо забезпечення стійкості надання ЖВФ			
	Рівень громад ¹⁴⁹ (село, кілька сіл)	Рівень районів ¹⁵⁰ (кілька громад)	Рівень областей ¹⁵¹	Загальнодержавний рівень
		району та спроможності реагувати на надзвичайні ситуації місцевого рівня	об'єктів критичної інфраструктури та виробничої діяльності підприємств області, реагування на надзвичайні ситуації місцевого рівня	реагування на кризові та ситуації загальнодержавного рівня тощо
Визначення потреб в енергоресурсах та джерелах енергії на відповідних рівнях управління для забезпечення стійкості надання життєво важливих функцій / послуг				
Мінімально необхідний рівень енергозабезпечення (максимальний рівень зниження функціональності)	<i>Транспорт</i> – запас палива для транспортних засобів, забезпечення мінімального рівня послуг на 1 добу. <i>Електроенергія</i> – резервна потужність для живлення мінімальних потреб (надання адміністративних послуг, зв'язку; насосних станцій, пунктів надання медичної допомоги, автозаправних станцій), наприклад, 20–30 % від проектних потреб за вибраними послугами. <i>Паливо</i> – запас для установок опалення (30 % від потреби установки на сезон) з можливістю використання місцевого палива	<i>Транспорт</i> – запас палива на три дні для забезпечення визначених мінімальних транспортних потреб району. <i>Електроенергія</i> – місцева (резервна) потужність для заживлення потреб (зокрема, це органи влади, ЦНАП, системи зв'язку, об'єкти КІ, медичні установи та ін.). <i>Паливо</i> – запас для мінімального забезпечення установок опалення (30 % від потреб району на сезон), роботи об'єктів КІ з можливістю використання місцевого палива	<i>Транспорт</i> – тижневий запас палива для забезпечення потреб області відповідно до рівня надання послуг. <i>Електроенергія</i> – наявні місцеві потужності (з врахуванням резервних потужностей) для заживлення потреб області відповідно до визначеного рівня надання послуг. <i>Паливо</i> – запас для мінімального забезпечення систем теплопостачання та роботи об'єктів КІ (на один місяць споживання)	Мінімальний рівень запасів енергоресурсів на випадок кризового реагування визначається відповідно до вимог законодавства та стратегічних документів у сфері національної безпеки
Час реагування	<i>Аварійне реагування</i> (припинення впливу загрози) та <i>стабілізація</i>	<i>Аварійне реагування</i> (припинення впливу загрози) та <i>стабілізація</i> ситуації	<i>Аварійне реагування</i> (припинення впливу загрози) та <i>стабілізація</i> ситуації	<i>Аварійне реагування</i> (припинення впливу загрози) та <i>стабілізація</i> ситуації (фіксація надання послуги)

Параметри планування	Зміст діяльності та завдання щодо забезпечення стійкості надання ЖВФ			
	Рівень громад ¹⁴⁹ (село, кілька сіл)	Рівень районів ¹⁵⁰ (кілька громад)	Рівень областей ¹⁵¹	Загальнодержавний рівень
	ситуації (фіксація надання послуги на визначеному рівні) – одна година	(фіксація надання послуги на визначеному рівні) – три години	(фіксація надання послуги на визначеному рівні) – шість годин	на визначеному рівні) – дванадцять годин
Час на відновлення інфраструктури до рівня проектного способу надання послуги	<i>Тривалість</i> «використання» спроможностей громади (або <i>час відновлення</i> проектного способу надання послуги) – 24 години	<i>Тривалість</i> «використання» спроможностей району до функціонування у кризовій ситуації – 48 годин	<i>Тривалість</i> «використання» спроможностей області до функціонування у кризовій ситуації або час відновлення проектного способу надання послуги (наприклад, 86 годин)	Встановлюється вимога щодо накопичення матеріалів, ресурсів, обладнання та організаційних можливостей, необхідних для відновлення надання мінімального рівня надання життєво важливих функцій / послуг (забезпечення відновлення у термін до п'яти днів (120 годин)

Джерело: розроблено автором.

Суб'єкт планування та залучені стейкхолдери

Наступним етапом у плануванні має стати визначення суб'єкта розроблення планів стійкості відповідно до ієрархії управління та набору ЖВФ, стійкість яких необхідно забезпечити.

Суб'єкт, який здійснює законодавчо визначені владні повноваження на визначеній географічній території (село, район, область, загальнодержавний або галузевий рівень) чи формування й реалізацію політики у визначеній сфері (секторальні органи влади у сфері захисту КІ), є відповідальним за планування та координацію всіх аспектів забезпечення стійкості у відповідній сфері управління та забезпеченні того, щоб усі стейкхолдери, які відіграють важливу роль у наданні функції / послуги (відповідно до ланцюжка постачання), були залучені до процесу планування й реалізації визначених заходів.

З метою забезпечення стійкості надання ЖВФ для вибраної сфери управління визначають інших потенційних стейкхолдерів, які можуть бути залучені до виконання всіх етапів циклу кризового реагування (у всіх режимах функціонування КІ).

Для того, щоб визначити роль окремого учасника взаємодії, треба враховувати:

- вимоги законодавства, яке зумовлює обов'язковість залучення до кризового реагування;
- наявність визначеної ролі у потенційному залученні ресурсів / персоналу до кризового реагування;
- наявність визначеної ролі у формуванні політики або розробленні законодавства у відповідній сфері;
- участь відповідного учасника взаємодії у наданні чи забезпеченні надання визначеної функції / послуги;
- можливості залучення до кризового реагування недержавного сектору та населення.

Для різних етапів циклу кризового реагування здійснюється огляд доцільності залучення окремих учасників до забезпечення стійкості надання функцій / послуг, орієнтовний приклад якого подано в *табл. 6*. Зазначимо, що перелік суб'єктів, наведених у таблиці, не є вичерпним і формується залежно від конкретної сфери планування та умов життєдіяльності громад і особливостей функціонування критичної інфраструктури.

Таблиця 6. **Визначення ролі та завдань учасників забезпечення стійкості функціонування КІ**

Стейкхолдери	Оцінювання, запобігання / уникнення	Захист, пом'якшення	Реагування	Відновлення	Вивчення уроків, адаптація
Центральні органи державної влади (або територіальні підрозділи у громадах)	+	+	+	+	+
Місцеві органи державної влади, місцевого самоврядування	+	+	+	+	+
Власники / Оператори КІ та надання функцій / послуг	+	+	+	+	+
Постачальники («провайдери») послуг для Операторів функцій / послуг та КІ			+	+	+
Інвестори	+	+		+	
Виробники обладнання, проєктанти	+			+	+
Громадські організації, професійні асоціації тощо	+		+	+	
Дослідницькі та наукові установи	+			+	+
Споживачі послуг (виробництво, адміністративні будівлі, торгіві, медичні, освітні заклади та ін.)	+		+	+	+
Населення (домогосподарства)			+	+	

Джерело: розроблено автором.

Задля детальнішого визначення потреб щодо залучення різних стейкхолдерів до забезпечення життєдіяльності громади, стійкості надання ЖВФ необхідно проаналізувати взаємозалежності між різними функціями / послугами, секторами КІ та взаємодією стейкхолдерів, аби спромогтися забезпечувати надання визначених послуг / функцій залежно від конкретної сфери планування під час розроблення плану стійкості.

Соціально-економічні аспекти життєдіяльності громад

Усвідомлення соціально-економічних, географічних, ресурсних, технологічних аспектів життєдіяльності громад є основоположним під час визначення переліку життєво важливих функцій, необхідних для забезпечення стійкості життєдіяльності громади.

Перелік таких функцій / послуг для різних громад може бути різним. Це залежить від соціально-економічних (наявність виробничих підприємств або сфери послуг / розваг, демографічний склад громади) особливостей та географічного розміщення громади, транспортної інфраструктури, ресурсних можливостей, технологічного забезпечення життєдіяльності громади тощо.

На початковому етапі розроблення плану стійкості громади (розроблення першого подібного плану) варто зосередитися на найбільш поширених послугах / функціях, які необхідні для забезпечення прийняттого рівня життєдіяльності людей у будь-якій громаді (Community Lifelines)¹⁵². Для забезпечення практичних цілей суб'єкта планування особливості надання вибраних ЖВФ потрібно визначати разом з ідентифікацією інфраструктури, яка забезпечує надання цих конкретних послуг кінцевим споживачам (табл. 7).

Такий порядок дій допоможе визначити перелік ЖВФ (припускаємо, що вони однаково важливі для всіх малих територіальних громад України), ідентифікувати КІ (у цій публікації – енергетичну інфраструктуру), яка забезпечує надання цих послуг, осмислити ланцюжок постачання та потенційні наслідки на життєдіяльність громади.

Таблиця 7. Визначення життєво важливих функцій / послуг та критичної інфраструктури, що важливі для громади

Життєво важливі для громади функції / послуги	Необхідні інфраструктурні об'єкти		Потенційні наслідки порушення функціонування КІ
	на території громади	за межами громади	
Електро-забезпечення	Електропідстанція низької напруги та мережі громади	Електропідстанція високої напруги, мережі електропостачання	<i>Безпосередні:</i> неможливість надавати інші функції; економічні збитки. <i>Опосередковані:</i> втрата робочих місць; необхідність евакуації людей
	Енергообладнання (споживаюче або генеруюче) виробничих підприємств, бюджетних установ	Мережі електропостачання	
	Будинки з енергообладнанням (споживаючим або генеруючим)	Мережі електропостачання	

¹⁵² Такі базові життєво важливі функції / послуги, що мають бути надані будь-якій громаді, називають *послугами життєзабезпечення (lifelines)*. Це, зокрема, найважливіші послуги для людини, які, коли вони надаються стабільно, дають змогу функціонувати всім іншим аспектам суспільства. Найчастіше це, наприклад, продовольче та медичне забезпечення, водо- та енергозабезпечення, зв'язок, транспортування, урядування (див.: FEMA Community Lifelines. URL: <https://www.fema.gov/emergency-managers/practitioners/lifelines>).

Життєво важливі для громади функції / послуги	Необхідні інфраструктурні об'єкти		Потенційні наслідки порушення функціонування КІ
	на території громади	за межами громади	
Теплозабезпечення	Котельня, насосні установки	Склади твердого палива, компресорна станція, мережі газопостачання, мережі електропостачання	<i>Безпосередні:</i> неможливість забезпечити функцію; економічні збитки. <i>Опосередковані:</i> необхідність евакуації людей
Водозабезпечення	Насосна станція, мережі живлення	Мережі електропостачання	<i>Безпосередні:</i> неможливість забезпечити функцію; економічні збитки. <i>Опосередковані:</i> збитки для довкілля, потенційна необхідність припинення надання інших функцій
Пошта та зв'язок	Будівля пошти та пункту зв'язку з енергоспоживальним обладнанням	Логістичні центри; інформаційно-комунікаційні мережі	<i>Безпосередні:</i> неможливість забезпечити функцію; економічні збитки. <i>Опосередковані:</i> потенційне порушення забезпечення інших функцій
Медичні послуги	Будівля поліклініки з енергоспоживальним обладнанням; автомобіль швидкої (екстреної) медичної допомоги	Лікарня, склади медикаментів, станція машин швидкої (екстреної) медичної допомоги	<i>Безпосередні:</i> неможливість забезпечити функцію; смертельні випадки. <i>Опосередковані:</i> необхідність евакуації людей; економічні збитки
Адміністративні послуги та владні функції	Адміністративно-офісна будівля з енергоспоживальним обладнанням	Органи вищого рівня управління; інформаційні бази даних	<i>Безпосередні:</i> неможливість забезпечити функцію. <i>Опосередковані:</i> потенційне порушення забезпечення інших функцій
Продовольче забезпечення	Торговий центр з енергоспоживальним обладнанням	Логістичні центри	<i>Безпосередні:</i> неможливість забезпечити функцію; економічні збитки. <i>Опосередковані:</i> потенційне порушення забезпечення інших функцій

Життєво важливі для громади функції / послуги	Необхідні інфраструктурні об'єкти		Потенційні наслідки порушення функціонування КІ
	на території громади	за межами громади	
Транспортування вантажів та пасажирів	Автозаправна станція та склад паливно-мастильних матеріалів	Нафтобази, термінали, трубопроводи	<i>Безпосередні:</i> неможливість виконувати певну функцію та негативний вплив на інші функції; економічні збитки. <i>Опосередковані:</i> втрата робочих місць
	Гараж транспортного підприємства з енергоспоживальним обладнанням	Логістичні центри; інформаційно-комунікаційні мережі	
	Будівля автостанції з енергоспоживальним обладнанням	Інформаційно-комунікаційні мережі	
	Дороги в межах громади	Дороги до громади; логістичні центри; автопарки	

Джерело: розроблено автором.

Послуги / функції забезпечення життєдіяльності громад часто взаємопов'язані. Що більше важливих функцій / послуг залежить від окремої послуги (наприклад, енергозабезпечення), то більшого пріоритету вона набуває у забезпеченні швидкого відновлення її проектних параметрів. Саме тому функція / послуга енергозабезпечення здебільшого входить до критеріїв оцінки ризиків у багатьох країнах.

Взаємозалежності функцій / послуг та критичної інфраструктури

Після ідентифікації ЖВФ та КІ у відповідній сфері планування здійснюється аналіз їх взаємозалежностей. Це важливий етап планування стійкості, під час якого можна точніше визначити потенційних стейкхолдерів плану стійкості, негативні наслідки впливу загроз та сформувавши плани заходів реагування.

Взаємозалежність відображає ступінь залежності однієї інфраструктури від іншої для виконання її функціонального призначення (забезпечення ЖВФ). Наприклад, електростанція, що працює на вугіллі, залежить від належного функціонування транспортної інфраструктури (транспортування вугілля залізницею або водним транспортом). Порушення електроенергетичної (електростанція) чи транспортної (залізнична колія чи порт) інфраструктури може призвести до скорочення виробництва електроенергії та зниження рівня задоволення відповідних потреб споживачів. У свою чергу, втрата електроживлення може призвести до зупинки роботи шахти, де вугілля видобувають.

Окрім того, більшість секторів інфраструктури (промисловості) критично залежать від постачання в повному обсязі потрібної для їхньої роботи електроенергії. Збої в наданні цієї послуги можуть спричинити пошкодження обладнання, а це, своєю чергою, здатне вплинути на виробництво продукції, необхідної в інших секторах (наприклад, надання медичних послуг, водозабезпечення, продовольче забезпечення тощо).

Загалом існують різні типи взаємозалежностей інфраструктурних систем, деякі з них обов'язково треба брати до уваги під час планування. Це, зокрема, взаємозалежності:

- фізичні (наприклад, входи та виходи однієї інфраструктури використовуються іншою (система постачання газу забезпечує електростанцію паливом, а електроенергію, своєю чергою, використовує для транспортування газу));

- кібернетичні (електронні, управлінські, інформаційні зв'язки), у широкому сенсі – це взаємозалежність інфраструктур та їх операторів від інформації та її якості (цілісності, скомпрометованості);

- географічні (розміщення на одній / суміжній території; спільний маршрут ланцюжків постачання вхідних ресурсів / виробленої продукції);

- функціональні (наприклад, робота однієї інфраструктури допомагає працювати іншій, хоча не відображається у фізичній залежності (навчання та підготовка персоналу для Операторів систем енергозабезпечення, інвестиції для енергетики завдяки роботі фінансових ринків)).

Можемо зазначити, що нині не існує єдиної узгодженої методології аналізу взаємозалежностей та метрики їх вимірювання. Кожний суб'єкт планування формує свій підхід до такого аналізу. Проте вже розроблено низку моделей представлення взаємозалежностей (графічна, таблична, текстова, структурно-функціональна та ін.), що допомагає іншим учасникам проаналізувати та осмислити процес планування. Добір того чи того способу визначається практичними потребами тих, хто здійснює планування. Окремі приклади представлення взаємозалежностей наведено у *додатку 3*.

Профіль громади з надання життєво важливих функцій / послуг (Енергетичний профіль громади)

Профіль громади з надання ЖВФ потрібен суб'єкту планування, щоб узгодити особливості (географічні, ресурсні та соціально-економічні) забезпечення життєдіяльності громади, наявну інфраструктуру функціонування

громади¹⁵³ та моделі споживання¹⁵⁴. Тому його розроблення є конче важливим. Саме профіль громади дає змогу усвідомити важливість ланцюжка забезпечення ЖВФ (за всіма вибраними функціями / послугами), особливості (ресурсні, логістичні, технологічні та ін.) функціонування цього ланцюжка, визначити всіх залучених до цього процесу стейкхолдерів.

Наприклад, для функції «Енергозабезпечення» Енергетичний профіль громади уможлиблює провести оцінювання вразливості КІ та надання послуг з енергозабезпечення¹⁵⁵, а також оцінити ризики, що можуть бути завдані громаді внаслідок порушення функції енергозабезпечення, досягнути вимоги¹⁵⁶ щодо забезпечення стійкості життєдіяльності громади.

Мета Енергетичного профілю громади – сприяти:

- визначенню споживачів та конкретних об'єктів, які повинні бути забезпечені енергією, що необхідно для підтримання мінімально необхідного рівня життєдіяльності громади;

- усвідомленню особливостей роботи інфраструктури життєзабезпечення на території відповідної громади (конкретних режимів енергоспоживання та параметрів обладнання, яке використовується);

- з'ясуванню власних спроможностей громади підтримувати визначений рівень життєдіяльності при перериванні ланцюжка постачання зовні (обсягів енергії, доступної громаді для підтримання рівня надання послуг кінцевим споживачам);

- визначенню стейкхолдерів, які потенційно можуть брати участь у забезпеченні стійкості життєдіяльності громади в кризовій ситуації.

Для уточнення потенційних стейкхолдерів та усвідомлення можливих механізмів їх залучення до забезпечення стійкості громади суб'єкту планування стійкості необхідно зібрати детальну інформацію про особливості надання вибраних життєво важливих функцій.

Як приклад наведемо перелік інформації, яку обробляють суб'єкти планування стійкості громад в енергетичній сфері. Досвід США з розроблення

¹⁵³ *Енергетичний профіль* – це опис інфраструктурних та ресурсних можливостей на рівні громади за джерелами енергії для задоволення потреб споживачів у нормальному режимі та на випадок кризової ситуації, з урахуванням уразливостей, зумовлених ресурсними та географічними особливостями.

Для сфери енергетики CESER розробив рекомендації з підготовки «Енергетичного профілю штату» (див.: CESER Guidance on Developing a State Energy Profile. URL: https://www.energy.gov/sites/default/files/2022-08/DOE%20CESER%20Guidance_State%20Energy%20Profile%20Outline_FINAL_508_0.pdf).

¹⁵⁴ Деякі з факторів, що визначають модель споживання енергії у громаді: чисельність населення та його соціальна структура; домогосподарства та енергоспоживальне обладнання домогосподарств; зайнятість населення та географія пересування; виробництва, обсяги та графіки споживання енергії; кліматичні та географічні умови.

¹⁵⁵ У подальшому аналіз заходів забезпечення стійкості життєво важливих функцій / послуг буде зосереджуватися на послугах енергозабезпечення громади.

¹⁵⁶ Для визначення вимог щодо забезпечення стійкості життєдіяльності громади або стійкості надання життєво важливих функцій / послуг варто скористатися Моделлю кризового реагування для забезпечення стійкості цільової функції (рис. 2).

місцевих планів стійкості енергозабезпечення засвідчує, що, аналізуючи енергетичний профіль та модель споживання громади, доцільно враховувати:

– необхідні обсяги споживання за категоріями споживачів, графіки навантаження, наявну можливість зниження енергоспоживання з централізованих мереж;

– наявну та необхідну потужність, виробництво, передачу / розподіл, кінцеве споживання та ціни на види енергії / енергоресурсів: електроенергії, природного газу, нафтопродуктів, інших основних видів, важливих для громади;

– наявність компаній із виробництва та постачання електроенергії, серед яких: комунальні підприємства; приватні підприємства; державні підприємства; регіональні оператори передачі; незалежні оператори локальних систем; енергетичні кооперативи; підприємства-постачальники;

– наявність компаній – виробників нафтопродуктів, постачальників, дистриб'юторів (наприклад, автозаправні станції);

– наявність органів місцевого самоврядування та місцевих підрозділів органів державної влади, які надають основні державні послуги (поліція, служба реагування на надзвичайні ситуації, екстрена медична допомога тощо);

– інших зацікавлених стейкхолдерів, які підтримують життєдіяльність громади, зокрема у сфері надання визначених ЖВФ.

Стосовно стейкхолдерів надання ЖВФ бажано мати інформацію про те, хто є власником, яка форма власності; місцезрештування й територію (райони), які обслуговує; чи має стейкхолдер плани, наприклад, план Оператора КІ на випадок порушення енергопостачання, включно угоди про взаємодопомогу та пріоритети відновлення; кому і як повідомляє про кризову ситуацію; які заходи передбачені, щоб запобігти та/або пом'якшити втрату енергозабезпечення та збій інфраструктури; чи є законодавство, котре регулює реагування; чи визначена типова послідовність відновлення у громадах відповідного рівня (територіальна громада, місто тощо).

Також необхідно зібрати інформацію, що сприятиме розробленню заходів забезпечення стійкості громади, у якій містяться відомості про:

- території обслуговування;
- кількість побутових, комерційних, промислових клієнтів;
- доступні сховища та запаси (для евакуації на випадок кризи, для накопичення ресурсів), їхні обсяги;
- плани на випадок надзвичайних ситуацій, якщо такі є;
- обсяги виробництва /постачання продукції (за визначений період часу), які можуть бути втрачені;

- транспортну та мережну інфраструктуру, що буде використовуватись (дороги, мости, тунелі трубопроводи, мережі (електричні, газові) тощо);
- компанії, які можна найняти для надання послуг «заміщення» замість втрачених (послуг транспортування, електро- та водозабезпечення, продовольчого забезпечення тощо).

Критичні загрози та ризики їх реалізації

Наступним етапом розроблення плану стійкості має стати оцінювання ризиків функціонування КІ та надання визначених ЖВФ. Систематичне проведення ідентифікації актуальних загроз та оцінки наслідків їх впливу дає змогу суб'єктам управління краще розуміти явища та чинники, що здатні порушити функціонування КІ, усвідомити вразливості та планувати заходи забезпечення безпеки і стійкості.

Аналіз безпекового середовища, ідентифікації загроз та оцінювання наслідків впливу загроз (ризиків)¹⁵⁷ є передумовою розроблення планів захисту відповідної інфраструктури від визначених загроз¹⁵⁸, а також заходів пом'якшення негативного впливу їх реалізації і швидкого відновлення штатного режиму надання послуг.

Оцінювання ризиків передбачає оцінку потенційних прямих і непрямих наслідків впливу окремих загроз. Нині у світовій практиці вже досить широко здійснюється оцінювання ризиків¹⁵⁹, хоча універсального підходу не існує¹⁶⁰.

У сфері стійкості надання окремих послуг застосовують підходи, які відображають специфіку функціонування критичної інфраструктури. Наприклад, Міністерство енергетики США¹⁶¹ при оцінці ризиків рекомендує враховувати такі критерії:

- як загрози різного типу впливають на різні енергетичні системи;
- вплив загроз на кінцевих споживачів енергії (наприклад, перебої в електропостачанні виробничих підприємств та домогосподарств, відключення роздрібних автозаправних станцій), величину та очікувану тривалість впливу (тобто рівні й тривалість порушення цільових параметрів функцій / послуг);
- як загрози впливають на спроможність громад реагувати на кризові ситуації (дії системи цивільного захисту в надзвичайних ситуаціях);

¹⁵⁷ Risk Assessment Methodologies. URL: [https://www.cisa.gov/sites/default/files/publications/Risk % 20Assessment % 20Methodologies.pdf](https://www.cisa.gov/sites/default/files/publications/Risk%20Assessment%20Methodologies.pdf)

¹⁵⁸ Див.: підрозділ 2.1.

¹⁵⁹ Див.: ДСТУ ІЕС/ISO 31010:2013 «Керування ризиками. Методи загального оцінювання ризиків».

¹⁶⁰ Див.: підрозділ 1.3.

¹⁶¹ Див.: URL: <https://www.energy.gov/ceser/articles/doe-energy-emergency-response-playbook-states-and-territories>

- вплив загроз на найбільш важливі вибрані функції / послуги життєзабезпечення громад (Community lifelines¹⁶²).

У процесі оцінювання ризиків часто розробляють сценарії реалізації загроз для точнішого відпрацювання плану реагування. Обираючи такий сценарій, необхідно враховувати особливості (технологічні, соціальні, природні, географічні тощо) функціонування відповідного об'єкта. Тобто сценарій має відображати події, які є найбільш вірогідними для визначеної сфери управління (країни, громади) та справлятимуть найбільший вплив на її функціонування¹⁶³.

Загалом, надаючи конкретну специфіку сценарію, у його описі потрібно зважати на низку чинників, як-от час, місце та умови реалізації загрози. Урахування таких деталей при аналізі сценарію допоможе визначити наслідки реалізації для різних інфраструктурних систем та чіткіше усвідомити пріоритетність заходів реагування¹⁶⁴.

Приклад опису Сценарію реалізації загрози

У зимовий період протягом тижня спостерігалася плюсова температура повітря та опади у вигляді дощу. Проте у *четвер*¹⁶⁵ розпочалося різке похолодання¹⁶⁶. До *17 години*¹⁶⁷ температура знизилась до -20 °С, з перспективою до подальшого зниження протягом ночі. Споживання електроенергії на території громади почало різко зростати, що спричинило перевантаження єдиного трансформатора та його загоряння о 21 годині¹⁶⁸. Врешті електрозабезпечення втратили всі споживачі громади. Наслідком реалізації такого сценарію є припинення електропостачання споживачів громади (100 % зниження цільових параметрів функції електрозабезпечення) від централізованої мережі.

Критеріями оцінки сукупних наслідків можуть, серед іншого, бути визначені:

- втрати систем обігріву споживачів (домогосподарств, лікарень, шкіл та ін.);
- смертельні випадки (у лікарні – через зупинку роботи обладнання; на дорогах – через аварії);

¹⁶² Див.: URL: <https://www.fema.gov/emergency-managers/practitioners/lifelines>

¹⁶³ Саме тому є необхідним для кожної громади (кожної сфери управління) розробляти свій профіль загроз та ризиків.

¹⁶⁴ Наприклад, уночі більшу наповненість мають житлові будинки, а вдень – школи, офісні та виробничі будівлі. Відповідно, аварійні роботи та пошуково-рятувальні місії будуть проводитися в різних місцях залежно від часу доби, коли відбувається сценарій.

¹⁶⁵ Четвер і п'ятниця – робочі дні, після них будуть вихідні, що зумовлює необхідність звернути увагу як на побутові, так і виробничі аспекти наслідків реалізації такого сценарію. Необхідно також урегулювати ситуацію до настання вихідних, поки всі потенційні стейкхолдери знаходяться в робочому режимі функціонування (персонал перебуває на робочих місцях).

¹⁶⁶ Відлига та дощ, із подальшим різким похолоданням, зумовлять не тільки зростання споживання електроенергії, а й призведуть до обледеніння на дорогах, будівельних конструкціях та лініях електропередачі, що потенційно може спричинити пошкодження інфраструктури в межах громади та на лініях постачання до громади, підвищити аварійність на дорогах тощо.

¹⁶⁷ Пікове зниження температури припало на початок зростання електроспоживання у вечірні години (увімкнено освітлення, побутові прилади, системи нагрівання), що безальтернативно призведе до різкого зростання енергоспоживання у громаді.

¹⁶⁸ Перевантаження трансформатора порушило централізоване електропостачання для споживачів усієї громади о 21 годині, на початку нічного періоду з підвищеним рівнем потреб у електроенергії (зокрема, для опалювання) та з перспективою до подальшого пониження температури.

- необхідність евакуації визначеної кількості людей (з лікарень; громадян, які належать до вразливих категорій);
- економічні збитки через пошкодження інфраструктури (обрив дротів, аварії на дорогах, перевантаження чи вихід із строю трансформатора, заміну обладнання);
- економічні збитки через припинення виробничої діяльності;
- екологічна шкода (припинення роботи систем очистки на виробництві та вилив шкідливих речовин у річку);
- втрата (відсоток) інших життєво важливих функцій / послуг (зв'язку, медичного та продовольчого забезпечення, урядування тощо);
- інше.

Формувати сценарій реалізації загрози доцільно на основі «обґрунтовано найгіршого сценарію», що може статись найближчими роками. При цьому можна скористатися рекомендаціями THIRA/SPR¹⁶⁹ щодо усвідомлення контексту реалізації сценарію (табл. 8) та чіткішого розуміння можливих наслідків.

Таблиця 8. Питання, які доцільно розглянути при розробленні контексту сценарію реалізації загрози

Питання для розгляду	Приклад на практиці
Як час інциденту вплине на здатність громади впоратися з ним? Який час доби та яка пора року будуть найвірогіднішими при реалізації загрози або матимуть найбільший вплив на надання життєво важливих функцій та послуг?	<i>Громада А</i> є дуже популярним літнім туристичним напрямком. Торнадо о 19:00 у червні може мати найбільший вплив, оскільки велика кількість туристів перебуватиме на дорогах, повертаючись до своїх готелів
Як місце події вплине на здатність громади впоратися із загрозою? Які місця при реалізації загрози або матимуть найбільший вплив на надання життєво важливих функцій та послуг (наприклад, населені пункти, прибережні зони, промислові чи житлові райони)?	<i>Громада В</i> має високу щільність населення на півночі та дуже низьку – на півдні. Пандемія може спричинити найбільший вплив на півночі, де хвороба може поширюватися серед населення швидше
Які інші умови чи обставини викликають особливе занепокоєння, що пов'язано із загрозою чи небезпекою (наприклад, атмосферні умови, як-от швидкість / напрямок вітру та відносна	У <i>Громаді С</i> стався викид небезпечних речовин. Найгірший вплив може виникнути вдень із посиленням швидкості вітру, який дме в бік густонаселених житлових районів громади

¹⁶⁹ Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide Comprehensive Preparedness Guide (CPG) 201. URL: <https://www.fema.gov/sites/default/files/2020-04/CPG201Final20180525.pdf>

вологість або кілька інцидентів, котрі відбуваються одночасно)?	
Яка соціальна або фізична вразливість викликає особливе занепокоєння при реалізації загрози чи небезпеки (наприклад, зони, що можуть зазнати затоплення; населення з обмеженою здатністю до евакуації або без неї)?	<i>Громада D</i> розташована в гірському регіоні, її населення розподілене між приміськими районами у передгір'ях та сільськими гірськими громадами. Лісова пожежа може призвести до тяжчих наслідків у гірських громадах, де обмежена кількість доріг, якими населення може евакуюватись. Відповідно, це утруднює можливості надання порятунку працівникам служб реагування, оскільки до цих громад складніше дістатися

Джерело: Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide Comprehensive Preparedness Guide (CPG).

При розгляді сценаріїв реалізації загроз та розроблені плану забезпечення стійкості суб'єкт планування має враховувати:

- інформацію про минулі інциденти, яка демонструє, як подібні загрози вплинули на системи КІ в минулому, що дозволить краще спрогнозувати ефективність пропонованих заходів реагування;
- місцевий досвід учасників планування, особливо Операторів КІ, а також тих, хто володіє знаннями про вразливість активів і систем до визначених загроз, що дозволить запропонувати ефективніші заходи реагування;
- попередній аналіз досвіду інших громад у реагуванні на подібні сценарії, що дозволить уникнути помилок.

Зрозуміло, що створення єдиної процедури оцінювання ризиків реалізації загроз будь-якого типу поки що є проблематичним. Але загальні принципи дають змогу визначити основні етапи аналізу ризиків КІ, а саме: 1) ідентифікувати загрози функціонуванню КІ; 2) визначити вірогідність того, що така загроза може бути реалізована; 3) оцінити можливі наслідки реалізації визначених загроз з точки зору цілей сфери управління (громади).

У рамках розроблення плану стійкості Група із планування, залучаючи представників експертного середовища, узагальнює зібрану інформацію та формує перелік потенційних загроз наданню ЖВФ громади, а також оцінює ймовірні наслідки, яких загрози, у разі їх реалізації, можуть завдати функціонуванню відповідної інфраструктури.

Приклад попередньої ідентифікації загроз енергетичній інфраструктурі та можливих наслідків для її функціонування уміщено в *додатку 4*.

Детальне оцінювання наслідків реалізації визначених загроз здійснюється за низкою визначених критеріїв, які пов'язані із цілями сфери управління або безпосередньо з цільовими параметрами функціонування КІ та надання ЖВФ.

Зазначимо, що на різних рівнях управлінської діяльності (Оператор КІ, село, район, область, сектор чи загалом країна) та стосовно різних послуг / функцій такі критерії можуть суттєво різнитися.

Тому для спрощення оцінки суб'єкт планування стійкості обирає важливі, з точки зору його практичних потреб (або ж цілей визначеної сфери управління), критерії. У *додатку 5* подано набір критеріїв, дібраних автором цього дослідження, для використання на різних рівнях управління з огляду на завдання забезпечення стійкості функціонування КІ та надання ЖВФ.

Оцінювання впливу загроз може здійснюватися за допомогою різних методів якісного та кількісного характеру, зокрема методів, наведених у ДСТУ ІЕС/ISO 31010:2013 «Керування ризиками. Методи загального оцінювання ризиків». Кількісне оцінювання загроз може бути утруднене через відсутність чітких математичних моделей, що пов'язує загрози з наслідками їх впливу (ризиками), або через недостатність інформації. Тому часто застосовують спрощені методи оцінювання, які використовують методи експертних оцінок. Прикладом застосування такої методології може слугувати дослідження автора щодо оцінювання загроз енергетичній безпеці України¹⁷⁰.

Для цілей аналізу ризиків функціонування КІ та життєдіяльності громад на поточному етапі розвитку національної системи захисту критичної інфраструктури пропонується використовувати спрощений алгоритм оцінювання впливу загроз, де вірогідність загрози та наслідки її впливу оцінюються у балах від 1 до 5. Деталізація алгоритму наведена в *додатку 5*.

Підкреслимо, що оцінювання ризиків має стати обов'язковим щорічним елементом процесу планування стійкості. Наприклад, Керівництво з оцінки ризиків та спроможності громад США (THIRA/SPR)¹⁷¹ вимагає від громад здійснювати відповідне оцінювання ризиків кожні три роки та використовувати отримані дані для оцінювання своїх спроможностей щодо кризового реагування¹⁷². Це фактично безперервний, періодичний цикл, оскільки дає громадам змогу оцінювати щорічні тенденції щодо змін їхніх спроможностей, водночас періодично переглядаючи цілі планування стійкості, щоб не втратити їхньої актуальності в поточних умовах безпекового середовища.

¹⁷⁰ Див.: URL: <http://niss.gov.ua/publikatsiyi/analitichni-dopovidi/otsinyuvannya-zahroz-enerhetychniy-bezpetsi>

¹⁷¹ Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide Comprehensive Preparedness Guide (CPG) 201. URL: <https://www.fema.gov/sites/default/files/2020-04/CPG201Final20180525.pdf>

¹⁷² Громади визначають ризики, що потенційно можуть поставити під сумнів їхні можливості та виявити сфери, у яких спільнота не настільки спроможна, як того б хотілося. Ці області або прогалини в можливостях створюють бар'єри в здатності спільноти запобігати, захищати, пом'якшувати, реагувати на загрозу чи небезпеку та відновлюватися після неї. Розуміння ризиків, з якими громади стикаються, полегшить визначення рівня потенціалу, який громади повинні планувати створити та підтримувати.

Громади використовують інформацію, отриману під час оцінювання ризиків, щоб відповісти на п'ять ключових стратегічних запитань, що стосуються їхньої спроможності забезпечити стійкість життєдіяльності, а саме:

До чого має бути готова громада?

Який рівень спроможностей має бути у громади?

Які поточні спроможності громади?

Які прогалини у спроможностях громади існують?

Яким чином громада може усунути ці прогалини?

Оскільки забезпечення стійкості є спільною відповідальністю всіх членів громади, необхідно, щоб усі стейкхолдери, а не лише державні інституції, брали участь у розвитку необхідних громаді спроможностей. Отже, потрібно, щоб усі стейкхолдери були залучені протягом усього процесу планування стійкості громади, а відповідні плани відображали їхні ролі та обов'язки. Залучення зацікавлених сторін на початку та протягом усього процесу аналізу ризиків та планування стійкості допомагає громаді не помилятися з оцінками. Крім того, це можливість сформулювати орієнтири щодо визначення власних пріоритетів та інвестицій у своїх організаціях.

Цільові параметри стійкості функцій / послуг та функціонування критичної інфраструктури

Щоб підвищити власний рівень стійкості, громади визначають рівень своєї спроможності для подолання наслідків реалізації найбільш актуальних для них загроз. На додаток до ризиків, пов'язаних із загрозами, громади також мають визначити необхідні ресурси, знання, компетенції та інші фактори, які допоможуть досягнути бажаного рівня спроможності. Ідентифікація необхідних спроможностей і визначатиме довгострокові цілі розвитку громад.

Визначення довгострокових цілей у сфері планування стійкості

Довгострокові цілі розвитку сфери управління (громади) визначають бажані цілі планування у сфері стійкості забезпечення ЖВФ, пріоритетні напрями реагування на ідентифіковані загрози, необхідні ресурси.

Наприклад, цілями забезпечення стійкості громади можуть бути:

- вимоги щодо функціонування інфраструктури забезпечення життєдіяльності громади (наприклад, наявність інфраструктури для забезпечення визначеного рівня потреб, ресурси та матеріали для потенційного зростання потреб, вимоги щодо рівнів захисту КІ, надійності інфраструктури до впливу загроз тощо);
- спроможності забезпечити стійкість життєзабезпечення громади власними силами (резервування інфраструктури та ресурсів забезпечення

надання ЖВФ, диверсифікованість надання функцій / послуг, наявність місцевих джерел енергії тощо);

- готовність членів громади до виникнення кризової ситуації (наприклад, спроможності кінцевих споживачів протягом деякого часу зменшити свої потреби або забезпечувати їх власними силами, наявність сил кризового реагування, спроможність швидко відновити втрачені ЖВФ тощо).

Приклади таких довгострокових цілей наведені в *табл. 5*, де зазначено мінімальний рівень енергозабезпечення; час аварійного реагування, час відновлення тощо. Водночас для підготовки плану стійкості довгострокові цільові параметри мають бути розроблені для всіх вибраних ЖВФ та інфраструктурних систем.

Встановлення бажаних цілей у процесі планування

Встановлення бажаних цілей ефективності плану стійкості залежить від визначення двох основних чинників: 1) прийнятний рівень шкоди для певного рівня загрози; 2) час, необхідний для відновлення нормального режиму функціонування КІ, рівня надання функцій / послуг.

Прийнятний рівень шкоди фактично визначається на етапі проектування та будівництва відповідної інфраструктури через застосування вимог законодавства щодо надійності функціонування інфраструктури (стандарту надійності, будівельні норми та правила тощо).

Іншим чинником, що визначає прийнятний рівень шкоди, є цільові потреби сфери управління, для якої розробляється план стійкості, зокрема прийняті припущення щодо рівня толерантності до зниження рівня надання функцій / послуг визначеними інфраструктурними об'єктами (наприклад, тривалість періоду відключення електроенергії, що є допустимим для лікарні). Бажаний час для відновлення нормального рівня надання функцій / послуг (цільових параметрів функціонування КІ) та працездатності КІ на визначеному рівні (протягом часу необхідного для відновлення) фактично встановлює пріоритети щодо ремонту та зусилля з реконструкції.

Варто зазначити, що бажані цілі встановлюються з огляду на практичні потреби (інтереси) суб'єкта відповідної сфери управління (громади), а не визначаються конкретними загрозами.

Визначення пріоритетних напрямів та бажаних цілей реагування

Прикладом формалізації виконання такого завдання для сфери управління на місцевому рівні можуть бути Методичні рекомендації з планування стійкості громад¹⁷³, розроблені Національним інститутом стандартів та технологій

¹⁷³ NIST Community Resilience Planning Guide. URL: <https://www.nist.gov/community-resilience/planning-guide>

(National Institute of Standards and Technology, NIST) США. Запропонований підхід може бути представлений у вигляді такого алгоритму:

1. Формулюють бажані цілі реагування на визначені сценарії реалізації загроз для конкретних інфраструктурних об'єктів та енергоспоживального обладнання.

2. Формується розуміння (заздалегідь встановлюються завдання щодо розвитку спроможності) про те, як можна зберегти можливість надання ЖВФ, навіть за умови, коли робота критичної інфраструктури порушена.

3. Залежно від рівня впливу загроз (сценарію) визначають очікувані терміни й результати реагування на загрози (визначають терміни відновлення рівнів функціональності КІ, ліквідації наслідків загрози, заміщення втрачених спроможностей).

Проведений таким чином аналіз дає змогу усвідомити необхідні й очікувані параметри функціонування КІ та надання послуг, визначити пріоритети відновлення до проектного режиму за відповідний період часу.

Приклад адаптації пропонованого підходу до планування стійкості життєдіяльності громади на випадок порушення централізованого забезпечення громади електроенергією наведено у *табл. 9*.

Прогалини у спроможностях забезпечення стійкості

Розроблення конкретного плану стійкості потребує чіткого усвідомлення дій стейкхолдерів у кризовій ситуації з метою забезпечення функціональної спроможності КІ завдяки реалізації заходів реагування¹⁷⁴.

Для спрощення процесу формалізації плану стійкості відповідні оцінки щодо необхідного та очікуваного рівня забезпечення надання життєво важливих функцій / послуг доцільно представити в зручній для порівняльного аналізу формі (*табл. 10*).

¹⁷⁴ CISA використовує методологію CRPG, де для цілей спрощення аналізу формуються три рівні критичності впливу загроз (три рівні ризиків) – звичайний (routine), проектний (design), екстремальний (extreme), залежно від сценарію реалізації загрози встановлюються бажані / необхідні вимоги щодо рівня функціональності й термінів забезпечення такої функціональності. Такі орієнтири є завданнями для окремих груп планування заходів забезпечення стійкості (конструктивні рішення, логістичні, організаційні, технічні). План стійкості громади повинен базуватися на проектному рівні впливу загроз, але необхідно також оцінити звичайний та екстремальний рівні, щоб зрозуміти ефективність пропонованих рішень, наслідки та потреби у відновленні за різних рівнів небезпеки.

Таблиця 9. Планування стійкості життєдіяльності громади на випадок порушення централізованого забезпечення електроенергією

Потреби громади (послуги / функція енергозабезпечення)	Мінімальний рівень потреб громади	Власні резервні можливості (реалізація – до 30 хв, тривалість використання – до 24 год)	Допомога «ззовні» (реалізація – до 2 год, тривалість використання – до одного тижня)	Відновлення роботи у штатному режимі схеми (до 48 год)	Адаптація до нових умов (довгострокова перспектива – цілі розвитку громади)
Приміщення органу місцевого самоврядування	20 % від проєктного режиму – робота одного офісу та обладнання, забезпечення аварійного освітлення, насосних, вентиляційних систем	20 % – резервний пересувний генератор	Переведення частини персоналу органів влади до інших будівель (до ЦНАПу)	70 % від проєктного режиму	Встановлення систем електрозабезпечення на основі відновлюваної енергетики (ВДЕ) – сонячних та вітрових електростанцій потужністю 50 %, які здатні працювати в автономному режимі
Пункт надання адміністративних послуг (ЦНАП)	40 % від проєктного режиму – робота щонайменше одного офісу та обладнання	20 % – резервний стаціонарний генератор	30 % – постачання генераторів з «резервного фонду громади» на випадок кризових ситуацій	50 % від проєктного режиму	
Продовольчий магазин	40 % від проєктного режиму – забезпечення освітлення аварійного та торгового місця, холодильного обладнання, сигналізації	30 % – резервний пересувний генератор; 20 % – закриття окремих торгових відділів (обладнання)	20 % – постачання від виробничих підприємств	70 % від проєктного режиму	Встановлення систем електрозабезпечення на основі ВДЕ потужністю 30 %, що здатні працювати в автономному режимі
Насосна станція водопостачання та водовідведення	70 % від проєктного режиму – забезпечення роботи насосних та вентиляційних установок, аварійного освітлення	40 % – резервний стаціонарний генератор	30 % – постачання з резервного фонду гарантованих потужностей для кризових ситуацій	70 % від проєктного режиму	Встановлення систем електрозабезпечення на основі ВДЕ потужністю 40 %, що здатні працювати в автономному режимі
Автозаправна	50 % від проєктного	40 % – резервний		70 % від	Встановлення систем

Потреби громади (послуги / функція енергозабезпечення)	Мінімальний рівень потреб громади	Власні резервні можливості (реалізація – до 30 хв, тривалість використання – до 24 год)	Допомога «ззовні» (реалізація – до 2 год, тривалість використання – до одного тижня)	Відновлення роботи у штатному режимі схеми (до 48 год)	Адаптація до нових умов (довгострокова перспектива – цілі розвитку громади)
станція	режиму – забезпечення роботи насосного та вентиляційного обладнання, освітлення робочих місць та обладнання	стаціонарний генератор (робота з обмеженою кількістю заправних постів)		проектного режиму	електрозабезпечення на основі ВДЕ потужністю 50 %, що здатні працювати в автономному режимі
Пункт зв'язку	30 % від проектного – забезпечення освітлення робочого місця та обладнання зв'язку	20 % – резервний пересувний генератор	10 % – економія завдяки зміні системи комунікацій	50 % від проектного режиму	Встановлення нових систем зв'язку із живленням від ВДЕ
Лікарня	70 % від проектного режиму – забезпечення роботи насосного та вентиляційного обладнання, освітлення робочих місць та обладнання	40 % – резервний стаціонарний генератор; 10 % – обмеження постачання	20 % – постачання від фермерського господарства	100 % від проектного режиму	Встановлення систем електрозабезпечення на основі ВДЕ потужністю 50 %, що здатні працювати в автономному режимі
Фермерське господарство	30 % від проектного режиму – насосне обладнання, освітлення робочих місць	30 % – резервний стаціонарний генератор; 20 % – власна сонячна електростанція	20 % – постачання лікарні	50 % від проектного режиму	Встановлення систем електрозабезпечення на основі ВДЕ потужністю 50 %, що здатні працювати в автономному режимі
Усього:	30 % від сукупних потреб громади (проектного режиму споживання електроенергії)	Наявні 30 % потужностей для забезпечення потреб: 10 % – резервні потужності системи Оператора КІ; 10 % – власні стаціонарні генеруючі потужності споживачів; 10 % – аварійні резервні	Наявні 40 %: 20 % – резервні потужності системи Оператора КІ; 15 % – власні стаціонарні генеруючі потужності споживачів; 5 % – аварійні резервні	Наявні 50 %: 25 % – резервні потужності системи Оператора КІ; 20 % – власні стаціонарні генеруючі	Наявні 100 %: 65 % – потужності системи Оператора КІ; 25 % – власні стаціонарні генеруючі потужності споживачів; 10 % – оптимізація споживання

Потреби громади (послуги / функція енергозабезпечення)	Мінімальний рівень потреб громади	Власні резервні можливості (реалізація – до 30 хв, тривалість використання – до 24 год)	Допомога «ззовні» (реалізація – до 2 год, тривалість використання – до одного тижня)	Відновлення роботи у штатному режимі схеми (до 48 год)	Адаптація до нових умов (довгострокова перспектива – цілі розвитку громади)
		<p>потужності споживачів. Для додаткового зниження потреб на 5 % застосовано заходи обмеження споживання</p>	<p>потужності. Заходи оптимізації споживання знизили потреби на 10 %</p>	<p>потужності споживачів; 5 % – аварійні резервні потужності. Заходи оптимізації споживання знизили потреби на 20 %</p>	

Джерело: розроблено автором.

Таблиця 10. Визначення впливу загроз на функціонування КІ та ідентифікація прогалин у забезпеченні стійкості

Пріоритетні інфраструктурні системи (функції / послуги)	Необхідна підтримка під час реагування	Заходи								
		короткотермінові			середньострокові			довготривалі		
		0–1 год	до 24 год	до 72 год	до 7 днів	2-3 тижні	до 8 тижнів	3–6 міс.	6–12 міс.	Більше року
Інфраструктура забезпечення споживачів електроенергією (<i>Інфраструктура система 1</i> , електропідстанція та розподільчі мережі)	Д, МВ, О, ЗС	70 % 30 %	90 % 40 %					90 %		Проектний рівень
Система водопостачання та водовідведення (<i>Інфраструктура система 2</i> , насосна станція, трубопровідні мережі, водозабір, фільтраційна станція)	МВ, О	30 %	90 % 30 %		70 %		90 %	Проектний рівень		
Інфраструктура постачання палива (<i>Інфраструктура система 3</i> , нафтобаза та АЗС)	О, ЗС			30 % 30 %	70 % 70 %			90 % 90 %	Проектний рівень	
..... інші системи										
Інфраструктурна система транспортування (<i>Інфраструктура система – N-1</i> , дороги, мости, гараж, автостанція)	МВ, О, ЗС		30 %	70 % 30 %		70 % 70 %			90 % 90 %	Проектний рівень
Будівлі (<i>Інфраструктура система – N</i> , адміністративні будівлі, поліклініка, школа, житлові багатоповерхові та приватні будинки)	Д, МВ, О, ЗС	70 %	90 % 30 %		70 %			90 %		

Примітка: Д – державні органи влади загальнодержавного рівня (центральні органи виконавчої влади та їх регіональні підрозділи); МВ – місцеві органи влади (місцеві органи виконавчої влади, органи місцевого самоврядування); О – Оператори КІ, надання функцій / послуг; ЗС – залучені суб'єкти кризового реагування (інші суб'єкти).

Джерело: розроблено автором.

Зазначимо, що представлені в *табл. 10* параметри необхідного та очікуваного рівнів надання послуг (функціонування КІ) сформовані відповідно до Моделі кризового реагування для забезпечення стійкості цільової функції (*рис. 2*) і мають, відповідно, такі показники:

- 30 % операційної спроможності КІ (зниження рівня надання функцій / послуг на 70 % від цільових параметрів), що дозволяє забезпечити мінімально можливий рівень функціонування інфраструктурних систем та підтримання життєдіяльності громади на короткий проміжок часу (протягом цього часу споживачі мають бути готові забезпечити надання ЖВФ частково за рахунок власних сил і ресурсів або відмовитися від отримання послуг)¹⁷⁵;

- 70 % операційної спроможності КІ (зниження рівня надання функцій / послуг на 30 % від цільових параметрів), що дозволяє забезпечити допустимий рівень функціонування інфраструктурних систем та підтримання життєдіяльності громади протягом тривалого часу;

- 90 % операційної спроможності КІ (відхилення рівня надання функцій / послуг на 10 % від цільових параметрів), що забезпечує проєктні рівні функціонування інфраструктурних систем;

- проєктний рівень – повна операційна спроможність КІ (повне відновлення після впливу загроз).

У *табл. 9* використано різні за накресленням шрифти та кольори у позначенні відсотків: чорним кольором (жирний шрифт) позначено вимоги щодо необхідного рівня спроможності; зеленим (шрифт курсив) – випадки, коли необхідний та очікуваний рівні збігаються; червоним (шрифт курсив) – очікувані рівні відновлення операційної спроможності КІ, які не забезпечують необхідний для громади рівень у визначені терміни. Літерами синього кольору позначено встановлений термін повного відновлення операційної спроможності КІ з огляду на реалізовані інженерно-технічні та конструктивні рішення, у яких ураховано вивчені уроки, щоб не допустити подібної ситуації в майбутньому (відновитися на кращому рівні чи адаптуватися до нових умов життєдіяльності).

Представлені в наочній формі результати аналізу впливу загроз і наявних можливостей забезпечення стійкості життєдіяльності громади дають змогу визначити прогалини в чинних планах та пріоритетні напрями розвитку спроможностей громади.

Прогалини у забезпеченні стійкості визначаються розходженням між бажаними / необхідними та очікуваними рівнями функціонування КІ та/чи

¹⁷⁵ Точне визначення цього рівня залежить від конкретної ситуації на місці та має враховувати потреби забезпечення процесу відновлення до нормального режиму. Цей рівень може бути узгоджений із потребами гарантованого функціонування КІ громади.

забезпечення ЖВФ. Очікувані рівні визначають залежно від конкретної загрози та сценарію її реалізації за результатами аналізу ризиків.

Пріоритетні напрями розвитку спроможностей рекомендується визначати з урахуванням бажаних цілей забезпечення стійкості визначеної КІ, а також зважаючи на величину розходження між бажаними / необхідними та очікуваними рівнями й термінами відновлення функціональності КІ. Тобто, що більший розрив між необхідними та очікуваними параметрами, то вищий пріоритет має захід із подолання цього розриву.

На основі визначених прогалів можна планувати реалізацію окремих управлінських рішень (проектів), які би сприяли підвищенню стійкості надання відповідних ЖВФ громаді. Наприклад, може бути прийнято рішення щодо розвитку власних спроможностей громади забезпечувати визначений рівень енергозабезпечення з опорою на місцеві види енергоресурсів чи відновлювані джерела енергії¹⁷⁶.

Варто зазначити, що в Україні потенціал відновлюваних джерел енергії є досить значимим¹⁷⁷, а розвиток сучасних енергетичних технологій уможливує їх повноцінне використання.¹⁷⁸ Результати наукових фундаментальних і прикладних досліджень, зокрема Інституту відновлюваної енергетики НАН України, підтверджують факт значного потенціалу відновлюваної енергетики¹⁷⁹ для забезпечення енергетичних потреб суспільства та високий рівень готовності технічних рішень щодо запровадження комбінованих систем енергопостачання¹⁸⁰ для задоволення потреб громад навіть в умовах руйнування КІ¹⁸¹. Детальніша інформація про потенціал ВДЕ та приклади реалізації проектів енергозабезпечення територіальних громад України на основі використання місцевих ресурсів наведені в *додатках 6, 7* відповідно.

Важливо, що в Україні поступово формується законодавча та нормативно-правова база для розширення частки місцевих і відновлюваних джерел енергії в енергетичному балансі територіальних громад і стимулювання розвитку розосереджених джерел енергії та «розумних» мереж (smart-grids). Закон України «Про внесення змін до деяких законів України щодо

¹⁷⁶ Сприяння енергетичній безпеці та сталому розвитку місцевих громад в Україні. ГО АВЕ. URL: <https://rea.org.ua/library/844/>; <https://rea.org.ua/wp-content/uploads/2021/10/handbook-promoting-energy-security.pdf>

¹⁷⁷ Атлас енергетичного потенціалу відновлюваних джерел енергії України / за заг. ред. С. О. Кудрі. Київ : Ін-т відновлюваної енергетики НАН України, 2020. 82 с.

¹⁷⁸ Новітні енергетичні технології та їх вплив на функціонування систем енергопостачання : аналіт. доп. / О. М. Суходоля. Київ : НІСД, 2022. 36 с. URL: <https://doi.org/10.53679/NISS-analytrep.2022.17>

¹⁷⁹ Відновлювані джерела енергії / за заг. ред. С. О. Кудрі. Київ : Ін-т відновлюваної енергетики НАН України, ТОВ «НВП «Інтерсервіс», 2020. 392 с.

¹⁸⁰ Особливості комбінованих енергосистем з відновлюваними джерелами енергії / М. П. Кузнецов. Київ : ІВЕ. 2004. 152 с.

¹⁸¹ Домбровський О. Як запустити розподілену генерацію в Україні. Як відновлювати електростанції таким чином, щоб вони були не цікавими для російських ракетних атак? 2024. 11 квіт. URL: <https://www.epravda.com.ua/columns/2024/04/11/712293/>

відновлення та «зеленої» трансформації енергетичної системи України» від 30 червня 2023 р. № 3220-IX¹⁸² дозволяє запровадити ринкові механізми стимулювання розвитку ВДЕ (зокрема, механізм самовиробництва¹⁸³ для задоволення власних потреб в електроенергії через стимулювання роботи активних споживачів (просьюмерів)¹⁸⁴). У Законі уточнюються алгоритми роботи механізму агрегації ресурсів різних джерел енергії і споживачів (агрегація¹⁸⁵), розвитку малих розподільчих систем (діяльність оператора малих розподільчих систем¹⁸⁶ та енергетичних кооперативів¹⁸⁷), які покликані забезпечити управління енергозабезпеченням окремих локальних груп споживачів і громад.

Розвиток енергетичного законодавства та енергетичних технологій дає змогу реалізувати в Україні стратегічну переорієнтацію енергетичних систем. Розвиток розосередженої генерації в сучасних безпекових умовах дозволяє не тільки забезпечити енергетичну безпеку країни, стійкість надання послуг з енергозабезпечення кінцевим споживачам, а й зміцнювати національну економіку¹⁸⁸.

Визначення заходів забезпечення стійкості

Після того як прогалини оцінені та визначені пріоритети щодо цілей громади, можна вдатися до розроблення стратегічних рішень щодо зниження рівня вразливостей та підвищення стійкості громади.

Пропоновані заходи мають узгоджуватися з іншими планами розвитку відповідної сфери управління. Загалом процес планування підвищення стійкості життєдіяльності громади повинен узгоджуватися з планами дій у

¹⁸² Див.: URL: <https://zakon.rada.gov.ua/laws/show/3220-20#Text>

¹⁸³ Механізм самовиробництва – схема підтримки активних споживачів, призначена для власного споживання електричної енергії, за якою відбувається взаєморозрахунок вартості обсягу відпуску електричної енергії в електричну мережу генеруючими установками таких споживачів та вартості обсягу відбору ними електричної енергії з електричної мережі.

¹⁸⁴ Активний споживач – споживач, у т. ч. приватне домогосподарство, енергетичний кооператив та споживач, який є замовником енергосервісу, що споживає і виробляє електричну енергію, та/або здійснює діяльність із зберігання енергії, та/або продає надлишки виробленої та/або збереженої електричної енергії, або бере участь у заходах з енергоефективності та управління попитом.

¹⁸⁵ Агрегатор – учасник ринку електроенергії, який здійснює діяльність з агрегації (діяльність, що пов'язана з об'єднанням електроустановок, призначених для виробництва та/або споживання, та/або зберігання електричної енергії з метою купівлі-продажу електричної енергії, надання допоміжних послуг та/або послуг з балансування на ринку електричної енергії).

¹⁸⁶ Оператор малої системи розподілу – суб'єкт господарювання, що відповідає за безпечну, надійну та ефективну експлуатацію, технічне обслуговування малої системи розподілу і забезпечення спроможності малої системи розподілу щодо задоволення обґрунтованого попиту на розподіл електричної енергії її користувачам.

¹⁸⁷ Енергетичний кооператив – юридична особа, створена для здійснення господарської діяльності з виробництва, заготівлі або транспортування паливно-енергетичних ресурсів та зберігання енергії, для надання інших послуг з метою задоволення потреб його членів або територіальної громади, а також з метою отримання прибутку відповідно до законодавства.

¹⁸⁸ Розподілена генерація – це безпека зараз, і економіка під час війни і після війни. UABIO. 2024. 16 квіт. URL: <https://uabio.org/news/15978/>

суміжних сферах. Нерідко в методичному аспекті плани забезпечення стійкості громад узгоджуються із діяльністю щодо пом'якшення наслідків надзвичайних ситуацій на місцевому рівні¹⁸⁹. Також важливо, щоб ті, хто здійснює планування, не забували про необхідність урахування визначених у програмах соціально-економічного розвитку громади пріоритетів, а, крім того, у випадку стійкості енергозабезпечення – зважали на стратегічні плани розвитку енергетики¹⁹⁰ на території громади.

Група з планування, яка розробляє план стійкості, ураховуючи результати аналізу ситуації в громаді, формує набір практичних адміністративних заходів, технічних чи будівельних проєктів, рішень з перспективного соціально-економічного чи технологічного розвитку. Вибір заходів реагування здійснюється на основі оцінки ризиків громади від порушення функціонування визначеної КІ. При цьому неабияке значення має рівень підготовки учасників Групи та розуміння ними важливості аналізу ризиків порушення ЖВФ. Прикладом такого аналізу є оцінки ризиків громади від порушення функції енергозабезпечення¹⁹¹.

Перелік заходів реагування формується на основі:

- конкретної ситуації (особливості громади, вибрані ЖВФ, наявна інфраструктура, конкретний тип загроз);
- власних знань і досвіду суб'єктів планування стійкості життєдіяльності громади, зокрема вивчених уроки попереднього реагування;
- опрацювання кращого світового досвіду (публікації та аналіз за відповідними секторами КІ¹⁹² й типами загроз¹⁹³).

Розглянемо приклад планування заходів із забезпечення стійкості функції енергозабезпечення на національному рівні, розроблених у Великій Британії на випадок реалізації загрози «виникнення дефіциту газу на європейському ринку» через припинення постачання газу Росією в 2022–2023 рр.

На фоні повідомлень про загрози припинення постачання російського природного газу трубопроводами регулятор енергетичного ринку Великої Британії провів оцінку ризику виникнення дефіциту природного газу в країні.

¹⁸⁹ Local Mitigation Planning Handbook. FEMA. URL: https://www.fema.gov/sites/default/files/2020-06/fema-local-mitigation-planning-handbook_03-2013.pdf

¹⁹⁰ В Україні поширюється практика розроблення місцевих енергетичних планів, які мають бути документом стратегічного планування на період 10 років, що визначає довгострокові цілі сталого енергетичного розвитку певної території та об'єктів у межах такої території.

¹⁹¹ Mutani G., Santantonio S., Brunetta G., et al. An energy community for territorial resilience: Measurement of the risk of an energy supply blackout. *Energy and Buildings*. Vol. 240. 2021. 01 June. <https://doi.org/10.1016/j.enbuild.2021.110906>

¹⁹² DOE CESER SESP Drop-in_Risk Mitigation Measures. URL: https://www.energy.gov/sites/default/files/2022-06/DOE%20CESER%20SESP%20Drop-in_Risk%20Mitigation%20Measures_FINAL_508.pdf

¹⁹³ Mitigation Ideas. A Resource for Reducing Risk to Natural Hazards. FEMA URL: https://www.fema.gov/sites/default/files/2020-06/fema-mitigation-ideas_02-13-2013.pdf

За результатами оцінювання, регулятор звернувся до Операторів систем електропостачання та газопостачання, а також уряду Великої Британії з проханням розробити заходи на випадок виникнення дефіциту газу на ринку, враховуючи різні сценарії утворення такого дефіциту¹⁹⁴.

Уряд провів необхідне оцінювання й підготував план реагування¹⁹⁵ на випадок реалізації обґрунтовано найгіршого сценарію, який передбачав можливість відключення електроенергії тривалістю до семи днів¹⁹⁶. Під час розроблення плану було оцінено вплив загрози (відключення електроенергії на тлі дефіциту газу) на різні сектори КІ та надання ЖВФ (з урахуванням роботи транспорту, комунікацій та енергетики, постачання продовольства та води), які можуть бути серйозно порушені в цей період.

Згодом уряд Великої Британії спільно з Операторами КІ та компаніями, які працюють на ринку, підготували заходи щодо:

- інформування суспільства на випадок відключення електроенергії¹⁹⁷;
- забезпечення постачання газу з інших джерел та підвищення власного видобутку;
- скорочення споживання (програми заохочення споживачів до скорочення енергоспоживання чи зміщення графіка споживання)¹⁹⁸;
- підготовки промислових споживачів до обмеження постачання газу (обмеження споживання електростанціями для забезпечення постачання населення)¹⁹⁹;
- підготовки до можливого включення у роботу електрогенеруючих потужностей на інших видах палива (вугільної генерації)²⁰⁰.

Оператор системи електропередачі Великої Британії надіслав повідомлення визначеним стейкхолдерам щодо плану дій на випадок кризи з постачання газу напередодні зимового періоду 2022/2023 років²⁰¹.

¹⁹⁴ Government tests energy blackout emergency plans as supply fears grow. URL: <https://www.theguardian.com/business/2022/nov/01/government-tests-energy-blackout-emergency-plans-as-supply-fears-grow>

¹⁹⁵ Цей план розроблявся у форматі «військової гри» на майданчику урядового ситуаційно-кризового центру.

¹⁹⁶ Britain at 'significant risk' of gas shortages this winter, says regulator. Monday 3 October 2022. URL: <https://www.reuters.com/business/energy/britain-significant-risk-gas-shortages-this-winter-says-regulator-report-2022-10-03/>

¹⁹⁷ BBC prepares secret scripts for possible use in winter blackouts. URL:

<https://www.theguardian.com/media/2022/oct/18/bbc-prepares-secret-scripts-for-possible-use-in-winter-blackouts>

¹⁹⁸ Britain's biggest suppliers to offer discounts for off-peak electricity usage. URL: <https://www.theguardian.com/business/2022/nov/04/britains-biggest-suppliers-to-offer-discounts-for-off-peak-electricity-usage>

¹⁹⁹ Ofgem 'prepared for all scenarios' after leaked letter suggests UK could face a gas shortage. URL: <https://www.itv.com/news/2022-10-03/ofgem-prepared-for-all-scenarios-after-leaked-letter-warns-of-gas-shortage>

²⁰⁰ Ofgem admits Britain is at risk of 'gas supply emergency'. URL: <https://www.ft.com/content/f737a827-a069-41c4-8141-73b8f9f56fae>

²⁰¹ Homes could face three-hour power cuts this winter, warns National Grid. URL: <https://www.theguardian.com/business/2022/oct/06/national-grid-warns-households-could-face-three-hour-power-cuts-this-winter>

Згодом, за результатами проведених заходів і моніторингу ситуації, Оператор системи електропередачі повідомив про зниження рівня ризику до прийняттого рівня та скасував плани запровадження надзвичайних заходів²⁰².

Яскравим прикладом вивчення власного досвіду є зусилля українських стейкхолдерів щодо збереження можливості доставити електроенергію споживачам під час цілеспрямованого руйнування армією РФ енергетичної інфраструктури України (генерації та електромереж) протягом осінньо-зимового періоду 2022/2024 років. Зусилля всіх стейкхолдерів, залучених до забезпечення надання функції енергозабезпечення споживачів, спрямовувались на реалізацію дуже широкого кола завдань (*додаток 8*).

Висвітлений у *додатку 8* перелік заходів реагування не є повним відображенням усіх зусиль залучених учасників, і він не був формалізований у вигляді окремого, затвердженого Кабінетом Міністрів України плану реагування. Проте фактично реалізований Україною набір заходів із забезпечення спроможності країни забезпечувати споживачів електроенергією в 2022–2024 рр. може слугувати прообразом змісту Плану енергетичної стійкості України, який уряд повинен розробити відповідно до рішення Ради національної безпеки і оборони України.

Зауважимо, проте, що на окремих етапах циклу кризового реагування вжиті заходи були недостатніми. Так, напередодні широкомасштабного російського воєнного вторгнення (тоді енергетична система України функціонувала в штатному режимі) не було виконано належної роботи з аналізу безпекового середовища, зокрема ідентифікації критичних загроз її функціонування. Не було також проведено оцінювання ризиків порушення функціонування критичної енергетичної інфраструктури. Врешті, як наслідок, не були підготовлені відповідні плани реагування на загрози масштабного збройного вторгнення. Заходи щодо захисту об'єктів КІ у сфері енергетики фактично розроблялись та застосовувались уже в поточному режимі як заходи аварійного реагування.

Водночас у цей період до заходів з відновлення функціональності енергетичної системи України та забезпечення постачання електроенергії споживачам було залучено широке коло найрізноманітніших стейкхолдерів. Узагальнення цього вітчизняного досвіду дає змогу виокремити дві групи заходів реагування на порушення функціонування КІ, що доцільно врахувати під час розроблення планів стійкості:

1) *заходи аварійного реагування*²⁰³ – це заходи першочергового реагування для припинення негативного впливу загроз;

²⁰² National Grid cancels plans to start emergency winter scheme. URL: <https://www.theguardian.com/business/2022/nov/28/national-grid-emergency-winter-plan-energy-prices>

2) заходи пом'якшення впливу загроз на рівень функціональності КІ та надання / споживання послуг²⁰⁴, до яких належать:

- зниження потреб у послугах;
- застосування резервних можливостей підвищення обсягів надання послуги;
- зміщення у часі пікових потреб у послугах;
- заходи скорочення термінів падіння / погіршення проєктних параметрів надання послуг;
- заміщення одних послуг іншими (заміщення інфраструктурних способів надання функцій / послуг).

Розробляючи заходи плану стійкості, варто також урахувувати той факт, що конкретні заходи на визначених об'єктах КІ (побудова захисних стін, ремонт обладнання тощо) безпосередньо не сприяють розвиткові спроможності громади забезпечувати стійкість життєдіяльності у майбутньому, адже такі заходи розроблялися для конкретної загрози та умов її реалізації.

Стійкість – це властивість системи (громади), яка формується внаслідок взаємодії різних елементів системи (складових частин громади, стейкхолдерів) та змінюється в процесі життєдіяльності й розвитку системи. А тому до плану стійкості громади потрібно уводити й інші аспекти діяльності, як-от: стратегічне планування розвитку громади та інвестування, планування заходів кризового реагування та взаємодії залучених стейкхолдерів, аналіз та обмін інформацією, навчання й тренування тощо.

Загалом необхідне формування заходів забезпечення стійкості за всіма етапами циклу реагування²⁰⁵, з урахуванням завдань різного типу. Орієнтовна

²⁰³ Заходи реагування здійснювались за трьома схемами:

тимчасова / аварійна (години) – відновлення функціонування окремих об'єктів чи елементів системи за тимчасовими схемами, доступними матеріалами на основі існуючої інфраструктури (зварювання, шунтування, бандажі, заміна незначних деталей тощо);

короткострокова (дні / тижні) – проведення ремонту після детального обстеження всього об'єкта (енергоблоків, електропідстанцій, газових розподільчих станцій) чи мереж енергопостачання (електричні, теплові чи газової мережі) шляхом заміни пошкоджених елементів на нові або налагодження тимчасових альтернативних систем енергозабезпечення;

довгострокова (місяці) – встановлення нового обладнання, будівництво нових систем та схем енергозабезпечення.

²⁰⁴ Застосування зазначених заходів доцільно розмежувати за виконавцями (відповідальними) за зменшення рівня дисбалансів між наявними можливостями надання та потребами отримання ЖВП, а саме: заходи Оператора КІ (надання послуг); заходи споживачів послуг (суб'єкти господарювання, установи, населення); заходи інших учасників ланцюжка забезпечення виробництва та надання послуг (постачальники ресурсів, обладнання тощо).

²⁰⁵ **Штатний режим функціонування** – аналіз загроз і планування умов функціонування КІ та заходів реагування відповідно до визначених загроз та рівнів критичності їх впливу.

Готовність та запобігання – застосування заходів, які дозволяють уникнути впливу загроз або пом'якшити наслідки їх впливу (наприклад, заходи захисту).

Реагування – заходи реагування на подію (загрозу) з метою повернення до проєктних параметрів функціонування КІ та надання послуг.

Відновлення – заходи відновлення штатного функціонування КІ та надання послуг з урахуванням вивчених

структура конкретного переліку заходів плану стійкості життєдіяльності громади подана в *табл. 11*.

Безумовно, формування планів стійкості громад потребує конкретизації з огляду на особливості функціонування сфери управління (життєдіяльності конкретних громад, сектору КІ чи окремої функції).

У короткостроковій перспективі заходи забезпечення стійкості визначатимуться вимогами щодо безпеки функціонування КІ, аварійного реагування та стабілізації ситуації, що значною мірою залежить від умов реалізації розроблених сценаріїв впливу загроз.

Таблиця 11. Формування заходів забезпечення стійкості за етапами циклу реагування

Етап циклу реагування	Приклади заходів
Штатний режим (підготовка)	
Аналіз та планування	Планування та реалізація заходів захист КІ відповідно до визначеного рівня загроз / небезпек; розроблення планів взаємодії залучених суб'єктів та планів реагування; налагодження обміну інформацією про кращі практики; аналіз безпекової ситуації та оцінка ризиків
Тренінг та підготовка	Навчання та підвищення кваліфікації персоналу; проведення регулярних практичних тренінгів
Пом'якшення / запобігання	
Інфраструктурні рішення	Реалізація інженерно-технічних рішень щодо захисту КІ; модернізація об'єктів КІ та оновлення обладнання відповідно до визначених ризиків; резервування систем, накопичення запасів
Організаційні рішення	Застосування заходів запобігання впливу загроз (захист КІ) та пом'якшення наслідків їхнього впливу (заміщення пошкодженого обладнання, втрачених ресурсів чи функцій іншими активами); аналіз ситуації та координація реагування
Реагування	
Аварійне реагування	Застосування «проектних» сил та ресурсів (сил Операторів КІ, громади, споживачів) відповідно до визначених планів реагування на визначені типи загроз; застосування «термінових» рішень для заміщення втраченого обладнання, ресурсів чи функцій; аналіз ситуації та координація реагування
Стабілізація ситуації	Заміна / ремонт КІ, будівель, обладнання; залучення «додаткових» місцевих сил та ресурсів;

Етап циклу реагування	Приклади заходів
	застосування «середньострокових» та «альтернативних» рішень для відновлення втрачених функцій / послуг; аналіз ситуації та координація реагування
Відновлення	
Відновлення та модернізація	Заміна / ремонт КІ, будівель, обладнання; рішення з відновлення повноцінного функціонування з врахуванням нових технологічних можливостей та необхідності підвищення стійкості у майбутньому
Вивчення уроків та адаптація	Аналіз дій з реагування й поширення кращого досвіду; уточнення процедур підготовки та реагування; внесення змін до законодавства; уточнення пріоритетів довгострокового стратегічного розвитку сфери управління

Джерело: складено автором.

У довгостроковій перспективі добір конкретних заходів довгострокового характеру здійснюється з урахуванням стратегічних цілей громади та планів її соціально-економічного розвитку на основі техніко-економічного аналізу реалізації заходів підвищення стійкості (наявності ресурсів та організаційно-інституційної спроможності громади в майбутньому експлуатувати нову інфраструктуру).

Саме тому при визначенні переліку заходів необхідно враховувати:

– *наявність ресурсів.* Функціонування та життєздатність КІ є обов'язковими до, під час та після кризи, тому необхідно спланувати й створити відповідні ресурси для підтримки потреб. Термін «ресурси» треба розуміти у широкому сенсі: від фінансових ресурсів до людських і професійних та інформаційних через матеріально-технічні засоби;

– *можливості розбудови потенціалу та спроможності до реагування на кризові ситуації.* Цей аспект є одним із ключових для забезпечення безпеки та стійкості КІ й надання функцій / послуг. Спроможності всіх потенційних стейкхолдерів мають бути розвинені до рівня готовності впоратися з викликами поточного безпекового середовища, запобігати та пом'якшувати вплив ідентифікованих загроз;

– *технології та інновації.* Технологічний розвиток є однією з основних особливостей сучасного підходу до створення стійкості КІ. При розробленні заходів захисту, пом'якшення чи відновлення функціонування КІ необхідно завжди враховувати нові можливості, які можуть бути надані завдяки використанню новітніх технологій. Також треба враховувати особливості формування готовності суб'єктів забезпечення функціонування КІ до експлуатації нових технологій, що потребуватиме відображення у плані таких

чинників: можливі механізми фінансування, доступ до спеціалізованих ресурсів (сили та засоби сил сектору безпеки та оборони тощо), підготовка персоналу (місцевих органів влади, операторів КІ та інших стейкхолдерів) тощо.

Отже, планування стійкості функціонування КІ та надання ЖВФ має здійснюватися на основі перспективних інфраструктурних систем, що спрямовуються на випереджувальну стійкість, орієнтовану на майбутній контекст функціонування КІ, нові технології та знання²⁰⁶. Це допоможе виконати одне з основних завдань забезпечення стійкості – адаптуватися до нових умов та відновитися на кращому рівні.

²⁰⁶ Новітні енергетичні технології та їх вплив на функціонування систем енергопостачання : аналіт. доп. / О. М. Суходоля. Київ : НІСД, 2022. 36 с. <https://doi.org/10.53679/NISS-analytrep.2022.17>

Розділ 4. РОЗРОБЛЕННЯ ПЛАНУ СТІЙКОСТІ

4.1. Загальні засади планування стійкості функціонування критичної інфраструктури та надання життєво важливої функції / послуги

За результатами огляду етапів забезпечення стійкості надання функції / послуги можна сформуванати загальні базові принципи, які мають бути покладені в основу процесу планування стійкості.

План стійкості ЖВФ розробляє суб'єкт управління, який відповідає за надання цієї послуги / функції чи реалізацію політики в цій сфері. Це міністерство, агентство, виконавчий орган територіальних громад.

На кожному рівні управління відповідний суб'єкт розробляє план стійкості ЖВФ, який базується на забезпеченні стійкості функціонування інфраструктури надання функцій / послуг у всьому ланцюжку постачання, наприклад: «водопостачання» (насосна станція, мережа, споживачі), «енергопостачання» (джерело енергії, енергомережа, споживачі), «освіта» (освітній заклад, персонал, учні), «адмінпослуги» (органи влади, документи, зв'язок, споживачі).

Суб'єкт, який здійснює планування, не обов'язково володіє інфраструктурою, що забезпечує надання визначених ЖВФ, може не бути відповідальним за ресурсне, фінансове чи технічне забезпечення таких послуг, але зобов'язаний підготувати план стійкості надання цієї функції в межах своєї сфери управління.

План стійкості у своїй структурі повинен містити такі складники: аналіз потреб (загальні потреби та мінімальний рівень споживання відповідно до рівня відповідального суб'єкта), можливостей (наявні ресурси, технології та потреби зовнішньої допомоги), загроз (перелік чинників, які можуть призвести до порушення функції, і рівень готовності до реагування на їх вплив, яку суб'єкт узяв на себе) та заходів забезпечення стійкості ЖВФ (щодо реалізації власних спроможностей (ресурсних, організаційних); допомоги, наданої з-за меж сфери управління (суб'єкти та ресурси більшої сфери управління); механізмів взаємодії залучених стейкхолдерів).

Суб'єкт планування стійкості, залучивши стейкхолдерів, повинен координувати їхні дії, передусім тих, хто бере участь у функціонуванні всього ланцюжка надання ЖВФ (Оператори КІ, які забезпечують надання послуги, а також надавачі допоміжних послуг (у сферах зв'язку, транспорту), інвестори (у сферах фінансів, ресурсів, знань) тощо).

Затвердження плану стійкості має здійснюватися рішенням суб'єкта планування у формах зобов'язального для всіх залучених учасників документа (відповідно до рівня та сфери відповідальності) або спільного узгодженого рішення (протоколу, меморандуму, угоди), за яким учасники самостійно беруть на себе зобов'язання.

Задля того, щоб координувати дії різних учасників, варто постійно використовувати механізм узгодження позицій та інтересів різних стейкхолдерів і вироблення рішень, які будуть підтримувати їхню прихильність до реалізації затвердженого плану стійкості. Таким формальним механізмом найчастіше є спеціально створені дорадчі групи (експертні, консультативні, робочі), до складу яких залучаються стейкхолдери забезпечення надання функції / послуги. Іноді, у період кризового реагування, створюється група антикризового реагування, яка зосереджує свою діяльність на пошуку оперативних рішень щодо усунення кризи (такій групі на час її роботи делегуються повноваження оперативного керівництва діями учасників).

4.2. Базові вимоги до розроблення плану стійкості

На основі проведеного аналізу можна сформувати набір базових параметрів, які необхідно враховувати в планах стійкості надання ЖВФ чи функціонування критичної інфраструктури.

План стійкості, складений на будь-якому рівні управлінської вертикалі, повинен сприяти вирішенню питань, що стосуються:

- залучення широкого кола стейкхолдерів як в частині реагування (безпосередньої діяльності) на загрози виникнення кризової ситуації, так і залучення ресурсів та можливостей, що виходять за межі можливостей Оператора КІ;

- визначення актуальних загроз у відповідній сфері планування (країна, галузь, територіальна громада, підприємство) та оцінювання наслідків їх реалізації (ризиків) з точки зору впливу на рівень надання функцій / послуг; на інші, суміжні послуги / функції, соціально-економічні аспекти, на реалізацію національних інтересів тощо;

- забезпечення обміну інформацією між усіма стейкхолдерами та координованості їхніх дій, розроблення учасниками процедур та планів взаємодії за всіма етапами розвитку кризової ситуації;

- встановлення цільових параметрів реагування, зокрема щодо часових рамок реагування, допустимих та мінімальних рівнів надання послуг / функцій, термінів відновлення проєктних параметрів функціонування КІ;

- розроблення заходів реагування та забезпечення стійкості надання послуг / функцій, навіть в умовах порушення функціонування КІ;
- забезпечення інформування споживачів послуг про розвиток ситуації та заходи реагування, які вже були ухвалені, забезпечення альтернативних способів задоволення потреб споживачів до моменту відновлення проєктних способів;
- вивчення уроків та адаптації процесів надання функцій / послуг відповідно до нових реалій.

4.3. Зміст плану стійкості за етапами циклу кризового реагування

Результати аналізу можливостей і завдань забезпечення стійкості надання ЖВФ формалізуються в плані стійкості, де визначають стейкхолдерів, їхні завдання, доцільні заходи за всіма етапами циклу кризового реагування.

1. Оцінювання та запобігання:

- визначення переліку актуальних загроз життєдіяльності громади, важливих критичних загроз;
- визначення КІ та ЖВФ, які забезпечують життєдіяльність громади, усвідомлення можливих наслідків реалізації загроз (ризиків життєдіяльності громади);
- визначення переліку суб'єктів забезпечення стійкості надання ЖВФ та заходів реагування.

2. Захист і пом'якшення:

- оцінка власних ресурсів відповідального за надання ЖВФ суб'єкта та усвідомлення потреб залучення додаткових, зовнішніх ресурсів;
- планування заходів захисту КІ та пом'якшення впливу загроз на надання ЖВФ, життєдіяльності громади на випадок реалізації загрози;
- розроблення плану взаємодії та обміну інформацією між усіма залученими суб'єктами реагування на визначений перелік загроз.

3. Готовність та запобігання:

- формалізація порядку та обсягів залучення зовнішньої допомоги;
- урегулювання порядку надання зовнішньої допомоги громаді (наприклад, ресурси держави чи сусідньої територіальної громади, комерційні механізми);
- активація планів захисту та взаємодії суб'єктів реагування на випадок реалізації критичного впливу загрози;

– інформування залучених стейкхолдерів (громади) у випадку ідентифікації реальної критичної загрози.

4. Реагування:

- застосування заходів плану реагування для усунення впливу загрози;
- оперативна координація зусиль всіх залучених стейкхолдерів для забезпечення функцій / послуг в умовах кризи;
- залучення зовнішніх ресурсів та можливостей (за потреби), використання власних резервів на випадок кризи;
- застосування надзвичайних заходів (за потреби – відключення від послуг, тимчасове заміщення, евакуація).

5. Відновлення:

- координація зусиль суб'єктів з відновлення надання функцій / послуг (життєдіяльності громади);
- ліквідація наслідків реалізації загрози;
- залучення нових можливостей і технологій до забезпечення стійкості надання ЖВФ;
- адаптація системи, інфраструктури, життєдіяльності громади до нових умов середовища (внутрішнього та зовнішнього).

6. Вивчення уроків та розвиток спроможності:

- розуміння напрямів розвитку власної спроможності щодо забезпечення життєдіяльності громади (наприклад, для енергозабезпечення територіальної громади це може бути: електростанція на території громади, резервне обладнання для енергозабезпечення (школи, сільської ради, будинку культури), альтернативні маршрути та види транспорту тощо).

Етап реагування у кризовій ситуації потребує особливої уваги як стосовно підготовки заходів реагування, так і планування узгодженої діяльності всіх залучених стейкхолдерів.

Загалом у період кризової ситуації, тобто з моменту початку впливу загрози на цільові параметри функції / послуги чи КІ до моменту відновлення нормального режиму роботи (рис. 2), практичні дії²⁰⁷ (з фізичної точки зору) суб'єктів плану стійкості можуть містити заходи щодо:

- запобігання впливу загроз (недопущення погіршення цільових параметрів, що виходять за межі допустимого діапазону):
 - аварійного реагування (припинення впливу загрози та фіксація стану);
 - стабілізації ситуації (забезпечення часткового відновлення рівня надання послуг та/чи функціональності КІ);

²⁰⁷ У цьому контексті маємо на увазі дії, які відображаються у фізичному середовищі (матеріалах, ресурсах, обладнанні, мережах, маршрутах постачання, способах надання послуг тощо), наприклад: застосування сил та засобів захисту, зміна режимів функціонування КІ, ремонт обладнання, будівництво нової інфраструктури тощо.

- відновлення (забезпечення повноцінного відновлення рівня надання послуг та/чи функціонування КІ з урахуванням адаптації до нових безпекових умов).

Приклад формалізації заходів плану стійкості та завдань суб'єктів реагування для випадку порушення постачання електроенергії наведено в *табл. 12*.

Деталізація завдань для окремих суб'єктів може стати додатком до загального плану стійкості. Зокрема, такий додаток може містити конкретні плани (технічні, організаційні, комунікаційні), які допомагатимуть будувати стійкість життєдіяльності громад у довгостроковій перспективі²⁰⁸. Однак і плани для окремих учасників реагування мають відображати всі етапи циклу кризового реагування.

Пропонований підхід щодо забезпечення стійкості надання ЖВФ та/чи функціонування КІ дає можливість підготуватися до стратегічного довгострокового планування розвитку громад (як і будь-якої іншої сфери управління), чітко усвідомлювати та імплементувати аспект стійкості в цей процес. Рішення про пріоритети інвестицій у соціально-економічний розвиток громади, розвиток інфраструктури життєдіяльності та формування механізмів державно-приватного партнерства ухвалюватимуться з врахуванням головної мети – забезпечити стійкість надання ЖВФ для потреб усієї громади.

Наприклад, під час планування соціально-економічного розвитку, що здійснюється на основі аналізу ризиків стійкості життєдіяльності громади, суб'єкт управління може заздалегідь розробляти заходи для забезпечення «резерву» спроможностей (наприклад, автономне енергозабезпечення). Для Операторів КІ та надання ЖВФ вимоги щодо накопичення «резерву» можуть бути визначені законодавством (переважно регулюється ліцензійними вимогами, рішеннями органів влади, власника Оператора КІ).

²⁰⁸ Приклади реалізації проєктів підвищення рівня стійкості надання послуг з енергозабезпечення (на основі локальних рішень) наведено в *додатку 7*.

**Таблиця 12. Визначення заходів плану стійкості та завдань суб'єктів реагування
(на прикладі порушення функції «постачання електроенергії»)**

Штатний режим (оцінки загроз)		Режим готовності та запобігання реалізації загроз		Режим реагування на виникнення кризової ситуації (на прикладі порушення функції «постачання електроенергії»)				Режим відновлення енергозабезпечення	
Заходи підготовки	Суб'єкти	Заходи запобігання	Суб'єкт	Аварійне реагування	Суб'єкт	Стабілізація	Суб'єкт	Заходи відновлення та розвитку	Суб'єкт
Визначення загроз, оцінювання ризиків; інформуван- ня; планування; навчання і тренування	Оператор КІ;	Накопичення ресурсів: - палива; - обладнання; - персоналу	Оператор КІ; органи влади; суб'єкти господарювання	Аварійні джерела енергії бюджетних установ (10 % від потреби)	Органи влади (бюджетні установи)	Аварійні джерела енергії бюджетних установ (5 % від потреби)	Оператор КІ; органи влади; суб'єкти господарювання	Додаткові локальні джерела енергії (5 % від потреби)	Оператор КІ; органи влади
	органи влади;	Перевірка готовності: - планів реагування; - техніки; - персоналу	Оператор КІ; органи влади; суб'єкти господарювання; суб'єкти системи захисту КІ	Резервні джерела енергії оператора (10 %)	Оператор КІ; органи влади, що регламентують його діяльність	ВДЕ оператора (25 %)	Оператор КІ; органи влади; суб'єкти господарювання; населення	ВДЕ оператора (65 %)	Оператор КІ; органи влади; суб'єкти господарюван- ня; населення
	компанії- споживачі;								
	компанії- постачаль- ники;								
	інші залучені стейкхол- дери;								
населення	Встановлення: - спостережного обладнання; - захисних конструкцій та обладнання	Оператор КІ; органи влади; суб'єкти системи захисту КІ	Джерела компаній та населення (10 %)	Суб'єкти господарювання; населення	Джерела компаній та населення (20 %)	Суб'єкти господарювання; населення	Джерела компаній та населення (20 %)	Оператор КІ; органи влади; суб'єкти господарюван- ня; населення	
	Активізація заходів готовності; посилення заходів захисту	Оператор КІ; органи влади; суб'єкти господарювання суб'єкти системи захисту КІ	Самостійне зменшення споживання з боку споживачів (20 %)	Органи влади (бюджетні установи); суб'єкти господарювання; населення	Управління споживанням (20 %)	Суб'єкти господарювання; населення	Управління споживанням (10 %)	Оператор КІ; органи влади; суб'єкти господарюван- ня; населення	
	Інструктаж персоналу та населення	Оператор КІ; органи влади; суб'єкти господарювання	Обмеження споживачів (50 %)	Оператор КІ; суб'єкти господарювання; населення	Обмеження споживачів (30 %)	Оператор КІ; суб'єкти господарювання; населення			

Завдання плану стійкості

<i>Перелік заходів</i>	<i>Залучені стейкхолдери</i>	<i>Перелік заходів</i>	<i>Залучені стейкхолдери</i>	<i>1. Перелік заходів. 2. Індикатори: - наявність енергії; - 30 % від потреб (резервні джерела)</i>	<i>Залучені стейкхолдери</i>	<i>1. Перелік заходів 2. Індикатори: 50–70 % від потреб (відновлення та локальні джерела)</i>	<i>Залучені стейкхолдери</i>	<i>1. Перелік заходів. 2. Індикатори: 90 % від потреб</i>	<i>Залучені стейкхолдери</i>

Джерело: складено автором.

Для інших учасників процесу надання ЖВФ, зокрема кінцевих споживачів, «резерв» може бути сформовано на основі добровільного рішення (коли відомі та усвідомлюються ризики від порушення ЖВФ) або завдяки застосуванню заходів стимулювання (економічних механізмів або законодавчих зобов'язань).

Отже, зусилля всіх стейкхолдерів ще на етапі планування можуть забезпечити очікуваний рівень надання важливих для життєдіяльності громад функцій та послуг (рис. 3).

Варто пам'ятати: завдання щодо забезпечення стійкості енергозабезпечення громад може поєднуватися з розробленням місцевих енергетичних планів, вимогу щодо розроблення яких встановлено Законом України «Про енергоефективність»²⁰⁹. Передбачається, що такий план має стати документом стратегічного планування на період 10 років, що визначає довгострокові цілі сталого енергетичного розвитку певної території та об'єктів у межах цієї території²¹⁰.

Однією з цілей такого плану є усвідомлення громадою наявного енергетичного потенціалу, власних потреб у ресурсах та необхідних інвестиціях для забезпечення життєдіяльності громади і нормальної роботи інфраструктури²¹¹. Пропонується складати різнорівневі плани, а саме: муніципальний енергетичний план (спрямований на сталий енергетичний розвиток територіальної громади, охоплює об'єкти (системи), які розташовані на території територіальної громади) та регіональний енергетичний план (спрямований на сталий енергетичний розвиток області, охоплює об'єкти (системи), які розташовані на території області).

4.4. Орієнтовний зміст і структура плану стійкості

Нижче орієнтовно наводимо елементи структури та змісту плану стійкості щодо функції / послуги «електрозабезпечення».

1. Цілі розвитку громади – визначення цілей розвитку громади; оцінювання соціально-економічної ситуації; активів, що є на території громади.

2. Пріоритети забезпечення стійкості життєдіяльності громади – визначення переліку ЖВФ, які потребують енергозабезпечення.

²⁰⁹ Див.: URL: <https://zakon.rada.gov.ua/laws/show/1818-20#Text>

²¹⁰ Про затвердження Методики розроблення місцевих енергетичних планів: Наказ Міністерства розвитку громад, територій та інфраструктури України від 21.12.2023 № 1163. URL: <https://zakon.rada.gov.ua/laws/show/z0245-24#Text>

²¹¹ Муніципальний енергетичний план м. Івано-Франківська. URL: <https://www.mvk.if.ua/uploads/files/ee080811.pdf>

3. Профіль громади – (Енергетичний профіль громади) – оцінка енергетичної ситуації у громаді з урахуванням таких чинників: наявні види місцевих енергетичних ресурсів; джерела генерації енергії, що є в громаді; обсяги споживання, категорії споживачів; види ресурсів; інфраструктури; способи та маршрути енергозабезпечення з-за меж громади.

4. Суб'єкти забезпечення стійкості – визначення суб'єктів кризового реагування (усіх потенційних стейкхолдерів).

5. Оцінювання загроз та ризиків – визначення загроз, аналіз ризиків порушення енергозабезпечення громади.

6. Розвиток спроможності громади – посилення спроможності громади до реагування у кризовій ситуації із визначенням:

- процедури взаємодії між суб'єктами реагування;
- контактних осіб, способів та протоколів обміну інформацією;
- тематики, графіків (термінів) навчань і тренінгів для суб'єктів реагування.

7. Забезпечення стійкості – визначення заходів із забезпечення стійкості в наданні послуги енергозабезпечення щодо:

- запобігання впливу загроз (захист інфраструктури);
- пом'якшення наслідків реалізації загрози (резервування, заміщення);
- відновлення (ремонт, будівництво нового, переміщення споживання).

8. Пріоритети розвитку – вивчення уроків та розроблення довгострокових планів розвитку інфраструктури громади.

ВИСНОВКИ

В Україні прийнято законодавчі акти, де визначені завдання щодо забезпечення національної стійкості чи стійкості окремої сфери управління, які має вирішувати система державного управління. Водночас ці завдання стали суттєвим викликом для органів державної влади загальнодержавного та місцевого рівня.

Пропонована аналітична доповідь зорієнтована на те, щоб допомогти суб'єктам, які визначені відповідальними за окремі сфери управління, чіткіше усвідомити основні засади концепту стійкості, мету і зміст управлінських дій, а, крім того, надати необхідний інструментарій для формалізації такої діяльності.

У публікації міститься огляд методологічних підходів до визначення мети, завдань та змісту діяльності стосовно безпеки і стійкості критичної інфраструктури, яка забезпечує стійкість життєдіяльності громад. Підготовлено огляд вимог законодавства різних країн з питань стійкості функціонування критичної інфраструктури та надання життєво важливих послуг.

Проаналізовано підходи щодо обґрунтування змісту діяльності із забезпечення стійкості за етапами циклу кризового реагування. Узагальнено досвід реагування України на порушення функції «постачання електроенергії», що сталися внаслідок руйнування військами РФ енергетичної інфраструктури України в осінньо-зимовий період 2022–2023 рр.

Запропоновано модель формалізації діяльності із забезпечення стійкості надання життєво важливих функцій та послуг і функціонування КІ. Розроблена концептуальна модель фактично є практичним інструментарієм формалізації етапів кризового реагування, визначення змісту діяльності та заходів забезпечення стійкості для всіх залучених суб'єктів управління.

Сформовано методологію визначення цільових параметрів діяльності суб'єктів, що беруть участь у процесі планування стійкості, а також необхідних та можливих рівнів надання життєво важливих функцій та послуг.

Запропоновано принципи визначення суб'єкта планування, структури та змісту планів стійкості. Розроблення плану стійкості громади – дуже важливий процес, адже такий документ створює заздалегідь підготовлену та обґрунтовану основу для забезпечення потреб споживачів громади під час кризової ситуації та швидкого відновлення нормальних умов життєдіяльності.

Уміщені в дослідженні методологічні засади регламентації діяльності у сфері забезпечення стійкості, використані в практичній роботі, сприятимуть створенню комплексу механізмів щодо забезпечення стійкості різних сфер управління, розроблення проєктів необхідних законодавчих актів, методичних

та інструктивних матеріалів для суб'єктів управління різних рівнів та сфер управління.

Оприлюднені в доповіді результати досліджень стануть у пригоді суб'єктам управління для того, щоб розпочати практичну роботу із забезпечення стійкості функціонування визначених сфер управління, стійкості надання важливих для життєдіяльності суспільства послуг.

ДОДАТКИ

Додаток 1. Групи загроз / небезпек, що увійшли до Стратегічної національної оцінки ризику США

Типи загроз / небезпек	Опис загрози, яка приймається для подальшого оцінювання (на національному рівні)
Природні	
Спалах хвороби тварин	Ненавмисне занесення вірусу ящуру в домашню худобу в штаті США
Землетрус	Землетрус на території США, що призводить до прямих економічних збитків понад 100 млн дол.
Повінь	Повінь у США, яка призвела до прямих економічних збитків понад 100 млн дол.
Спалах пандемії людини	Серйозний спалах пандемічного грипу із загальним рівнем клінічних випадків у 25 % поширюється серед населення США
Ураган	Тропічний шторм або ураган вражає територію США, що призводить до прямих економічних збитків на суму понад 100 млн дол. США
Космічна погода	Сонце випромінює спалахи електромагнітного випромінювання та частинок енергії, що спричиняє збої в комунальному господарстві та пошкодження інфраструктури
Цунамі	Цунамі з хвилею, висота якої приблизно 15 м, ударило по Тихоокеанському узбережжю США
Виверження вулкану	Вулкан на північному заході Тихого океану вивергається, вражаючи потоками лави й попелу прилеглі території, а також димом і попелом – області на сході
Лісова пожежа	У США сталася лісова пожежа, яка призвела до прямих економічних збитків понад 100 млн дол. США
Технологічні (ненавмисні)	
Біологічне забруднення їжі	Випадкові умови, коли введення біологічного агента (наприклад, сальмонели, кишкової палички, токсину ботулінічного) у їжу призводить до 100 госпіталізацій або більше та реакції кількох штатів
Розлив або викид хімічної речовини	Аварійні умови, коли викид великого об'єму хімічної речовини, яка є гостро токсичною для людини, з хімічного заводу, сховища чи способу транспортування призводить до одного чи кількох смертельних випадків за межами об'єкта або одного чи кількох смертельних випадків (на місці або за його межами) з евакуацією за межі об'єкта / укриття
Прорив дамби водосховища	Аварійні умови, коли прорив дамби та затоплення призводять до одного або більше смертельних випадків
Викид радіоактивної речовини	Аварійні умови, коли пошкодження активної зони ядерного реактора спричиняє викид радіації

Типи загроз / небезпек	Опис загрози, яка приймається для подальшого оцінювання (на національному рівні)
Зловмисні (створені людиною)	
Літак як зброя	Ворожий недержавний суб'єкт(и) розбиває(ють) комерційний літак або літак авіації загального призначення на фізичну ціль у межах США
Збройний напад	Ворожі недержавні суб'єкти використовують тактику нападу для нанесення ударів по вразливих цілях у США, що призводить до смерті або поранення щонайменше однієї людини
Біологічна терористична атака (непродовольча)	Ворожий недержавний суб'єкт(и) отримує(ють) біологічний агент, перетворює(ють) його на зброю та застосовує(ють) у приміщеннях, ззовні чи стосовно ресурсів води з метою ураження скупчення людей у США
Хімічне / біологічне забруднення харчових продуктів	Ворожий недержавний суб'єкт(и) отримує(ють) біологічний або хімічний агент, перетворює(ють) його на зброю та розповсюджує(ють) його у продовольчих товарах у рамках ланцюга постачань США
Хімічний терористичний напад (непродовольчий)	Ворожий недержавний суб'єкт(и) отримує(ють) біологічний агент, перетворює(ють) його на зброю та застосовує(ють) у приміщеннях, ззовні чи стосовно ресурсів води з метою ураження скупчення людей у США (використовуючи аерозоль, ковтання або через шкіру)
Кібератака на інформацію (бази даних)	Кібератака, яка серйозно порушує цілісність або доступність даних (інформації, що міститься в комп'ютерній системі) або обробки даних, що призводить до економічних збитків у мільярд доларів або більше
Кібератака на фізичну інфраструктуру	Інцидент, у якому кібератака використовується як вектор для досягнення «поза комп'ютером» ефектів (тобто кінетичних чи інших ефектів), що призводить до одного або більше смертельних випадків або економічних збитків у розмірі 100 млн дол. США чи більше
Теракт із застосуванням вибухівки	Ворожі недержавні суб'єкти встановлюють переносний саморобний вибуховий пристрій на автомобілі або судні в США проти скупчення людей та/або структур, таких як важливі комерційні чи державні об'єкти, транспортні об'єкти, об'єкти критичної інфраструктури тощо, що призвело до принаймні одного смертельного результату чи поранення
Атака ядерного тероризму	Ворожий недержавний суб'єкт(и) отримує саморобну ядерну зброю шляхом виготовлення з матеріалів, що розщеплюються, купівлі чи крадіжки, і підриває її у великому населеному пункті США
Радіологічний терористичний напад	Ворожий недержавний суб'єкт(и) отримує(ють) радіологічні матеріали та розсіює(ють) їх за допомогою вибухівки чи інших засобів (наприклад, пристрої для розсіювання радіації) або створює(ють) пристрій радіаційного опромінення

Джерело: ²¹².

²¹² Див.: URL: <https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf>

Додаток 2. Порівняльний аналіз прикладів реагування на загрози й ризики кризової ситуації за етапами циклу кризового реагування

Криза 2014 р. (Україна) ²¹³ (дефіцит палива)	Криза 2022–2023 рр. (Україна) ²¹⁴ (руйнування інфраструктури)	Криза 2021 р. (США) ²¹⁵ (природний катаклізм)	Криза 2021 р. (США) ²¹⁶ (кібератака)
Загрози й ризики кризової ситуації			
<p>Російська агресія 2014 р. призвела до того, що Україна втратила доступ до антрацитового вугілля; було зруйновано маршрути постачання вугілля та частково – енергетичну інфраструктуру. Унаслідок руйнувань інфраструктури та дефіциту вугілля на теплових електростанціях виник ризик обмеження постачання електроенергії на всій території країни</p>	<p>Широкомасштабне російське збройне вторгнення, що розпочалось у лютому 2022 р., постійно супроводжувалося численними ракетними та артилерійськими обстрілами, унаслідок чого зазнала руйнувань вітчизняна енергетична інфраструктура. Зокрема, масована ракетна атака в жовтні 2022 р. спричинила руйнування 30 % енергетичної інфраструктури України, що зумовило ризик припинення постачання електроенергії для всіх споживачів країни</p>	<p>У лютому 2021 р. через різке зниження температури та шквальні вітри в системі електропостачання штату Техас були зафіксовані непроєктні режими в роботі обладнання (обледеніння, замерзання обладнання). Унаслідок того, що обладнання не було підготовлене до роботи в таких умовах, а також через недосконалість системи реагування на таку загрозу сталося часткове знеструмлення Техасу.</p>	<p>У травні 2021 р. було здійснено кібератаку на комп’ютерну мережу оператора системи трубопроводів Colonial Pipeline. Через зупинку роботи системи автоматичного керування технологічним процесом припинилося постачання нафтопродуктів. Кібератака спричинила ризик виникнення дефіциту моторного палива у східній частині США. Оцінки ситуації DOE та DHS засвідчили, що, якби робота Colonial Pipeline не відновилася протягом 10–12 днів, у країні зупинилось би транспортне сполучення Східного узбережжя через відсутність палива</p>

²¹³ Суходоля О. М. Проблеми та пріоритетні напрями забезпечення стійкості роботи енергосистеми України: аналіт. зап. Київ: НІСД, 2017. URL: <https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/problemi-ta-prioritetni-napryami-zabezpechennya-stiykosti-roboti>

²¹⁴ Детальний аналіз застосованих заходів реагування на порушення енергозабезпечення подано в *додатку 4*.

²¹⁵ Суходоля О. М. Техаська зимова енергетична криза 2021: висновки для України: аналіт. зап. Київ: НІСД, 2021. URL: <https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/tekhaska-zymova-enerhetychna-kryza-2021-vysnovky-dlya-ukrayiny>

²¹⁶ Аналіз кібератаки на трубопровідну систему США «Colonial Pipeline» / Оцінка стійкості енергетичної інфраструктури України: аналіт. звіт. ГО «Діксі Груп». 2022. URL: <https://dixigroup.org/wp-content/uploads/2022/05/dixi-energy-resilience-str.pdf>

Криза 2014 р. (Україна) ²¹³ (дефіцит палива)	Криза 2022–2023 рр. (Україна) ²¹⁴ (руйнування інфраструктури)	Криза 2021 р. (США) ²¹⁵ (природний катаклізм)	Криза 2021 р. (США) ²¹⁶ (кібератака)
Етап передбачення та підготовки			
<p>Україна мала можливості видобувати енергетичне вугілля, відповідно, була самодостатньою щодо цього виду палива, навіть експортувала його. Ризик зникнення енергетичного вугілля не оцінювався. Підготовка до реагування на загрози дефіциту такого виду вугілля не здійснювалася</p>	<p>Ризики фізичного руйнування енергетичної інфраструктури внаслідок збройної агресії РФ усвідомлювалися. Деякі енергетичні компанії розробили плани реагування на випадок руйнування окремих об'єктів енергетики.</p>	<p>Випадки різкого похолодання траплялися на цій території США. Водночас, на противагу сусіднім штатам, Техас відмовився від встановлення жорстких зобов'язувальних вимог до операторів енергетичної інфраструктури щодо підготовки до загрози різкого похолодання</p>	<p>Кібератаки на енергетичну інфраструктуру стали однією з основних загроз сталому енергозабезпеченню у США. Для операторів критичної інфраструктури були встановлені вимоги щодо кібербезпеки, проте в різних секторах критичної інфраструктури вони не визначалися як обов'язкові</p>
Етап приготування до реагування			
<p>Сезонне накопичення вугілля на складах електростанцій було неефективним через блокування постачання. Логістика імпорту енергетичного вугілля не опрацьовувалася. Інфраструктура перевалки імпортного вугілля в портах і його транспортування до ТЕС не були заздалегідь підготовлені. Підготовка до відновлення пошкодженої інфраструктури не перевищувала рівня підготовки до природних явищ (наприклад, низьких температур у зимовий період чи ожеледі)</p>	<p>Накопичено мінімальний рівень палива (запаси вугілля, природного газу) для роботи генеруючих потужностей. Опрацьовувалися можливості постачання природного газу та електроенергії з країн Європи. Здійснювалося накопичення ресурсів та обладнання для проведення ремонтних робіт (у рамках підготовки до сезонного зниження температури). Готувалися плани забезпечення альтернативного енергоживлення (із використанням дизель-генераторів, пересувних котельнь, запасів альтернативних видів палива). Здійснювалася підготовка запасних центрів управління роботою енергетичних компаній.</p>	<p>Енергетичний сектор штату Техас загалом, як і оператори системи передачі й розподілу електроенергії, не приділяли належної уваги підготовці заходів реагування на таку загрозу. На рівні штату план реагування на кризові ситуації був розроблений, але без урахування такого рівня втрат генерації. Погодні умови призвели до того, що з експлуатації було виведено близько 40 % генеруючих потужностей штату Техас. Зупинка вугільної генерації була спричинена замерзанням систем подачі вугілля із складів, газової генерації – замерзанням запірної арматури відбору газу з підземних сховищ та постачання</p>	<p>Для електроенергетичного сектору такі вимоги є обов'язковими через формування ефективної системи кібербезпеки. Водночас у транспортному секторі, до якого належить трубопровідний транспорт, такі вимоги мали рекомендаційний характер. Оператор на першому етапі атаки не повідомив про інцидент Агентство з питань кібербезпеки та безпеки інфраструктури (CISA) та не залучав його спеціалістів до розслідування й подолання наслідків кібератаки</p>

Криза 2014 р. (Україна) ²¹³ (дефіцит палива)	Криза 2022–2023 рр. (Україна) ²¹⁴ (руйнування інфраструктури)	Криза 2021 р. (США) ²¹⁵ (природний катаклізм)	Криза 2021 р. (США) ²¹⁶ (кібератака)
	Були створені антикризові центри (галузеві, регіональні) для координації дій. Тривала підготовка (збільшення чисельності) ремонтних бригад	газопроводами	
Етап реагування			
<p>Був створений урядовий антикризовий штаб, який забезпечував оперативне вирішення проблемних питань щодо перевезень вугілля, потреб в енергоресурсах, вчасних розрахунків компаній за постачене вугілля, проведення ремонтних робіт тощо.</p> <p>Застосовувалися заходи задля: зменшення споживання електричної енергії на території України; обмеження експорту електричної енергії; додаткового імпорту електричної енергії; припинення генерації на антрацитових вугільних ТЕС; збільшення генерації на інших потужностях (АЕС); встановлення граничних величини (лімітів) споживання потужності та електроенергії; уведення й активізації графіків відключення споживачів.</p> <p>Через руйнування маршрутів постачання та обмеження</p>	<p>Був створений урядовий антикризовий штаб. Пророблялися різні сценарії розвитку ситуації та відповідного реагування, а також сценарії енергозабезпечення (насамперед тепла) на випадок руйнування централізованої системи.</p> <p>У випадку критичного руйнування (10–11 жовтня 2022 р.) застосовувалося: включення додаткових генеруючих потужностей (аварійних, резервних); перерозподілення потоків потужності та електроенергії (перекомутація) в Об'єднаній енергосистемі України; запровадження графіків аварійного обмеження енергопостачання; спонукання до добровільного скорочення енергоспоживання (заклик до споживачів перемістити споживання на нічні години); переведення на альтернативні джерела, інші види палива</p>	<p>В уряді штату Техас була створена група реагування на кризу. Запроваджувались різні способи збільшення виробництва електроенергії (резервні газові генеруючі потужності, використання резервних джерел живлення – у лікарнях).</p> <p>Уряд штату закликав споживачів скорочувати енергоспоживання.</p> <p>На частині території штату були уведені графіки аварійного обмеження енергопостачання. Були розгорнуті системи локального енергопостачання (переважно для обігріву людей у спортзалах, школах)</p>	<p>Була створена міжвідомча робоча група для підготовки до різних сценаріїв, включно з необхідністю ухвалення додаткових заходів для пом'якшення будь-якого потенційного впливу на постачання пального. В окремих штатах запроваджено режим надзвичайної ситуації, що дає змогу мобілізувати ресурси федерального рівня.</p> <p>З метою забезпечення функції постачання моторного палива було: мобілізовано бензовози для доставки палива споживачам; сформовано нові логістичні маршрути постачання палива (з використанням морського та автомобільного транспорту); спрощено правила регулювання постачання палива дорогами (допуск у прибережні зони для танкерів, допуски у певні години доби та залежно від завантаженості доріг); спрощення умов найму / допуску до роботи</p>

Криза 2014 р. (Україна) ²¹³ (дефіцит палива)	Криза 2022–2023 рр. (Україна) ²¹⁴ (руйнування інфраструктури)	Криза 2021 р. (США) ²¹⁵ (природний катаклізм)	Криза 2021 р. (США) ²¹⁶ (кібератака)
у пунктах пропуску на кордоні було сформовано графік пріоритетного постачання вугілля залізницею	та енергозабезпечення; мобілізація всіх наявних ремонтних спроможностей для відновлення пошкодженої інфраструктури; запровадження тимчасових режимів роботи мереж та обладнання систем енергозабезпечення		водіїв, працівників паливних баз, АЗС; надано тимчасовий дозвіл на використання нестандартного палива для 12 штатів, що знаходяться в зоні надзвичайної ситуації. Щоб запобігти ажіотажу на автомобільне паливо, урядовці зверталися через ЗМІ до бізнесу із закликом діяти відповідально, застерігали від значного підвищення цін на пальне чи необґрунтованого закриття АЗС
Етап відновлення			
Збільшення видобутку вугілля на підприємствах, що залишилися на підконтрольній урядові України території. Налагодження стабільних поставок вугілля за імпортом. Переведення енергоблоків ТЕС із антрацитового вугілля на газове. Запровадження програм управління енергоспоживанням на стороні споживача.	Уряд виділяв ресурси для відновлення зруйнованої внаслідок обстрілів енергетичної інфраструктури. Було досягнуто урядових домовленостей щодо надання міжнародної допомоги (постачання обладнання, комплектуючих і матеріалів) для проведення ремонтних робіт. Проводилася робота з відновлення пошкодженої енергетичної інфраструктури, побудови нових об'єктів генерації, постачання та розподілення енергії. Активізація програм управління енергоспоживанням споживача	Оператор енергосистеми діяв у рамках чинних операційних планів та долучав до збільшення виробництва електроенергії доступні резерви. Основну роль у відновленні енергопостачання зіграло поліпшення погодних умов. З потеплінням оператор енергетичної інфраструктури стабілізував функціонування системи. Фінансові втрати оператора системи, генеруючих компаній і насамперед споживачів були величезними, переважно через економічні втрати унаслідок припинення виробничих процесів та коливання цін	Оператор трубопроводу задля допомоги в подоланні наслідків кібератаки залучив приватну фірму з кібербезпеки FireEye. CISA разом із DHS та FBI надавали допомогу в процесі розслідування інциденту. У сфері кіберзахисту були підготовлені оперативні рекомендації щодо захисту обладнання з ідентифікаторами можливого ураження та заходи з пом'якшення впливу кібератак. Також пропонувалася допомога урядових спеціалізованих структур іншим приватним операторам критичної інфраструктури у сфері кібербезпеки

Криза 2014 р. (Україна) ²¹³ (дефіцит палива)	Криза 2022–2023 рр. (Україна) ²¹⁴ (руйнування інфраструктури)	Криза 2021 р. (США) ²¹⁵ (природний катаклізм)	Криза 2021 р. (США) ²¹⁶ (кібератака)
<i>Етап вивчення уроків та розвиток спроможності</i>			
Усвідомлення ризиків руйнування енергетичної інфраструктури. Здійснювалася підготовка планів реагування на ймовірні кризи (утворення запасного центру управління, складання плану евакуації персоналу із небезпечних територій, накопичення ресурсів та обладнання для ремонтних робіт)	Уточнення ризиків; переоцінка загроз; перегляд планів реагування на ймовірні кризи	Були запропоновано внести зміни в законодавство штату Техас щодо формування обов'язкових до виконання вимог щодо підготовки обладнання до роботи в період низьких температур	За наслідками аналізу подій, президент США підписав розпорядження про вдосконалення федеральної кібербезпеки. Запроваджено обов'язкові вимоги, котрі стосувалися: обміну інформацією про загрози, надання послуг зі сфери кіберзахисту, запровадження жорсткіших стандартів кібербезпеки у федеральному уряді та ін.

Джерело: розроблено автором.

Додаток 3. Взаємозалежності життєво важливих функцій та особливості їх надання

Група спільного планування повинна зібрати інформацію про особливості функціонування КІ, яка забезпечує надання ЖВФ громаді визначеного рівня.

Метою такого аналізу є визначення конкретного енергоспоживального обладнання, що забезпечує надання необхідних для життєдіяльності громади послуг / функцій, а також залежностей одних інфраструктурних систем від інших та способів взаємозаміни втрачених можливостей. Насамперед складають перелік ЖВФ та інфраструктурних систем, що їх забезпечують, аналізують взаємозалежності функцій / послуг. Визначається інфраструктура, яка забезпечує надання функцій / послуг, у всьому ланцюжку постачання (будівлі, устаткування, процеси, інформація тощо) у межах сфери управління.

До аналізу залучаються представники всіх стейкхолдерів, які беруть участь у забезпеченні надання функцій / послуг, вивчається надана ними інформація, передусім та, що надійшла від органів центральної та місцевої державної влади, місцевого самоврядування, провайдерів (постачальників) функцій / послуг та Операторів КІ.

Під час проведення аналізу зазвичай застосовують процедуру опитування за орієнтовним переліком питань:

- Які послуги / функції є критично важливими для підтримання життєдіяльності конкретної громади? *(Можлива відповідь: водопостачання, медичні послуги, електрозабезпечення, урядування тощо.)*

- Визначте критичну інфраструктуру забезпечення життєдіяльності громади *(Можлива відповідь: адміністративні будівлі, лікарні, дороги, мости, порти, трубопроводи, електронідстанції, розподільчі пункти тощо.)*

- Яка інфраструктура може бути пошкоджена при реалізації загроз, визначених для певної громади, унаслідок чого не зможе виконувати своє призначення? *(Можлива відповідь: адміністративні будівлі, міст, електронідстанція тощо.)*

- Як втрата однієї функції / послуги та/або інфраструктури вплине на роботу іншої інфраструктури та надання інших функцій / послуг? *(Можлива відповідь: втрата електрозабезпечення зупинить практично всю виробничу діяльність; унаслідок цього скоротяться можливості надання адміністративних послуг громадянам; виникнуть загрози неможливості постачання води, продовольства, медичних послуг тощо.)*

- Який відсоток втрати основних послуг / функцій очікується, якщо буде порушено функціонування визначеної критичної інфраструктури? Якою буде

частка споживачів, котрі зазнають негативних наслідків? (Можлива відповідь: буде втрачено 70 % потужності джерел енергії для громади та 50 % транспортного сполучення тощо.)

- Скільки часу знадобиться, щоб усунути пошкодження задля відновлення послуг / функцій (години, дні, тижні, місяці, роки)? Яким чином можливо замінити втрачені послуги / функції? (Можлива відповідь: відновлення електропостачання до 100 % потребуватиме заміни трансформатора на електростанції, на що знадобиться п'ять днів; задля забезпечення щонайменше 50 % електропостачання в цей період є можливість: задіяти пересувні резервні генератори, запровадити програму добровільного скорочення споживання електроенергії, використати сонячні та вітрові установки фермерського господарства для живлення продовольчого магазину та лікарні.)

- Як довго громада може підтримувати життєдіяльність без втрачених послуг / функцій (дні, тижні, місяці)? (Можлива відповідь: 30 % потреб в електроенергії громада зможе підтримувати протягом семи днів, 50 % – протягом трьох днів.)

Крім переліку ЖВФ, треба визначити особливості ланцюжка надання послуг, проаналізувати взаємозалежності²¹⁷ та/або взаємозамінності одних послуг (КІ) іншими (див. табл. Д.3.1, рис. Д.3.1 та Д.3.2).

Таблиця Д.3.1

Побудова матриці взаємозалежностей

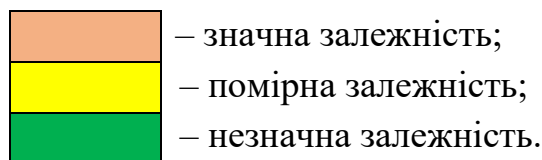
	Електро-забезпечення	Водо-забезпечення	Пошта та зв'язок	Продовольче забезпечення	Медичні послуги	Транспортування
Електро-забезпечення	Розміщення		Функція Відновлення	Відновлення	Відновлення	Відновлення
Водо-забезпечення	Функція Відновлення Розміщення	Розміщення			Відновлення	Відновлення
Пошта та зв'язок	Функція Відновлення		Розміщення	Відновлення		Заміщення
Продовольче забезпечення	Функція Відновлення	Функція Відновлення		Розміщення		Функція Відновлення
Медичні послуги	Функція Відновлення	Функція Відновлення	Заміщення Відновлення	Функція	Розміщення	Функція Відновлення
Транспортування	Функція		Заміщення	Функція	Відновлення	Розміщення

Джерело: адаптовано автором на основі²¹⁸.

²¹⁷ Community Resilience Planning Guide for Buildings and Infrastructure Systems. Vol. II. Dependencies and Cascading Effects. NIST Special Publication 1190. URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1190v2.pdf>

У табл. Д.3.1 представлено, як ЖВФ (стовпець праворуч) залежать від інших функцій (розміщені в рядках).

Рівень взаємозалежностей для підтримання надання функції / послуги чи КІ або її відновлення можна передати за допомогою кольору:



Пояснення термінів:

Функція – порушення однієї функції / послуги чи КІ негативно впливає на виконання іншої.

Відновлення – ця функція / послуга чи КІ визначає можливість і швидкість відновлення іншої.

Розміщення – фізичне руйнування однієї функції / послуги чи КІ через близькість розміщення спричиняє порушення іншої.

Заміщення – одна функція / послуга чи КІ може замінити іншу.

Іншим способом представлення взаємозалежностей функції / послуг чи КІ є графічна форма (рис. Д.3.1), що дає змогу наочно представити (завдяки лініям зв'язку між функціями) та визначити найбільш важливі функції / послуги, стійкість яких необхідно забезпечити громаді.

Продемонструємо цей спосіб на прикладі побудови залежностей, представлених у табл. Д.3.1 функцій забезпечення життєдіяльності громади.



Рис. Д.3.1. Графічний спосіб ідентифікації взаємозалежностей між функціями / послугами
Джерело: розроблено автором.

Стрілками різного спрямування на *рис. Д.3.1* представлено, яка функція у фізичному та/чи функціональному плані підтримує іншу (бере на себе роль у забезпеченні функціонування іншої чи її відновленні). Кількість стрілок (ліній) відображає важливість тієї чи іншої функції / послуги з точки зору забезпечення різних аспектів життєдіяльності громади. Товщина стрілок вказує на вагомість окремої функції у забезпеченні функціонування іншої.

Можливі й інші способи та методи аналізу взаємозалежностей, які допомагають визначити найбільш важливі аспекти забезпечення життєдіяльності громади, життєво важливі функції / послуги та КІ, яка підтримує громаду та забезпечує її розвиток²¹⁹.

Графічне представлення залежності життєдіяльності громади від функції енергозабезпечення (*рис. Д.3.2*) унаочнює аналіз взаємозалежностей та взаємодії між життєво важливими функціями / послугами громади.

²¹⁹ *Див.:* URL: [https://www.energy.gov/sites/default/files/2022-06/DOE %20CESER %20SESP %20Drop-In_Cross-Sector %20Interdependency %20Diagrams_FINAL_508.pdf](https://www.energy.gov/sites/default/files/2022-06/DOE%20CESER%20SESP%20Drop-In_Cross-Sector%20Interdependency%20Diagrams_FINAL_508.pdf)

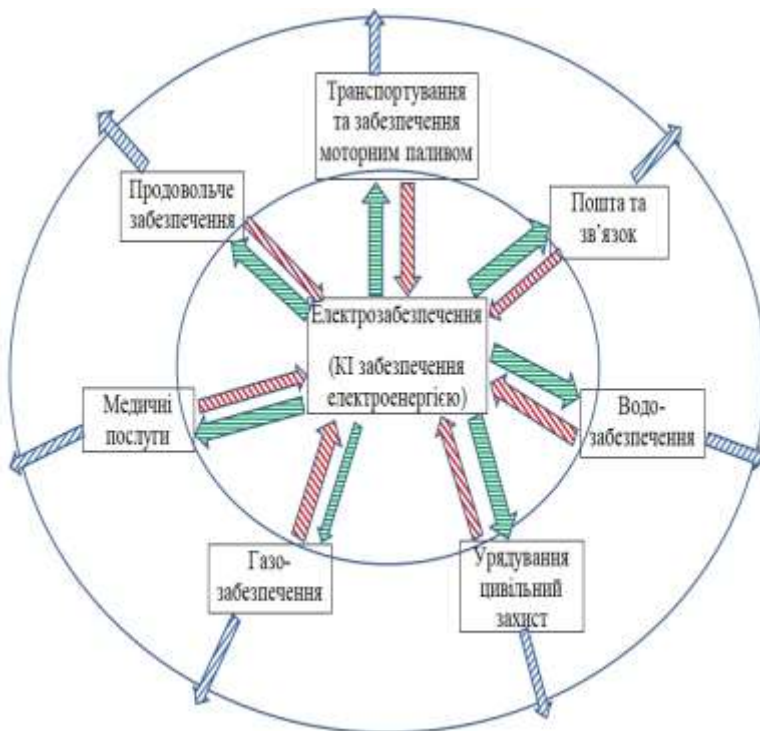


Рис. Д.3.2. Залежність функцій забезпечення життєдіяльності громади від функції енергозабезпечення
Джерело: розроблено автором.

Примітка.

⇒ Функція «Електрозабезпечення» підтримує функції / послуги забезпечення життєдіяльності громади.

⇒ Функція «Електрозабезпечення» залежить від підтримки функцій / послуг із забезпечення життєдіяльності громади.

⇒ Функція «Електрозабезпечення» опосередковано, через вибрані функції забезпечення життєдіяльності громад, підтримує ширше коло функцій / послуг.

Приклад проведення аналізу.

1. Водозабезпечення – забезпечення: водою населення, виробничих процесів, соціальної сфери, роботи каналізації, генерування енергії.

Електроенергія необхідна для здійснення функції водозабезпечення: обладнання очисних споруд та підготовки води, насосних станцій подачі води та водовідведення, забезпечення технологічних процесів на виробництві.

Водозабезпечення необхідне для функціонування енергетичної інфраструктури, зокрема для виробництва електроенергії на електростанціях (у системах охолодження)

2. Пошта та зв'язок – забезпечення: комунікації, передавання інформації, підтримка фінансових і виробничих процесів, торговельної діяльності, доставка посилок, робота систем автоматичного управління (виробничих установок, територіальних систем управління).

Електроенергія необхідна для систем зв'язку: функціонування обладнання систем передачі, обробки та поширення інформації, створення умов, необхідних для підтримки роботи обладнання та персоналу (освітлення, кондиціонування тощо).

Системи зв'язку необхідні для виробництва електроенергії, зокрема для роботи систем автоматичного управління роботою електростанції, роботи систем обліку виробництва та споживання енергії, передачі інформації виробничої діяльності, передачі диспетчерських команд, оповіщення жителів громад та персоналу тощо.

3. Продовольче забезпечення – забезпечення: постачання продовольства, роботи складів, роботи продовольчих магазинів.

Електроенергія необхідна для роботи торговельного обладнання, холодильних установок, створення комфортних умов обслуговування клієнтів (торгові зали, адміністративні приміщення тощо).

Постачання продовольства необхідне для підтримання роботи обслуговуючого персоналу підприємств енергетики та забезпечення життєдіяльності громад

4. Медичні послуги – забезпечення: надання медичної допомоги (консультування, огляд, діагностика, лікувальні та оздоровчі процедури, проведення операцій), ланцюжків доставки медичних препаратів (склади, аптеки), транспортування хворих до лікувальних закладів.

Електроенергія необхідна для роботи медичного обладнання, інформаційних систем, створення умов для надання медичних послуг (освітлення, кондиціонування тощо), забезпечення обігріву чи охолодження приміщень (лікарні та склади) тощо.

Медичне забезпечення необхідне для підтримання роботи обслуговуючого персоналу підприємств енергетики та забезпечення життєдіяльності громад.

5. Транспортування та постачання моторного палива – забезпечення: доставки вантажів (виробничих процесів та побутових споживачів), перевезення пасажирів (транспорт загального користування та спеціалізований транспорт), підтримка виробничих процесів і територіальних систем управління (пожежна охорона, правоохоронна діяльність тощо).

Електроенергія необхідна для доставки палива (бензовози, трубопроводи), роботи місцевих системи постачання палива для транспортних засобів (насосні станції на нафтобазах, АЗС), створення умов, необхідних для підтримки роботи обладнання та персоналу (освітлення, кондиціонування тощо).

Транспорт та паливо необхідні для доставки палива та вантажів для забезпечення роботи електростанції, доставки вантажів та матеріалів, транспортування персоналу тощо.

6. Урядування / цивільний захист – забезпечення: пожежної безпеки, евакуації та прихистку населення під час криз, правоохоронної діяльності, безпеки руху, технологічної безпеки, захисту довкілля тощо.

Електроенергія необхідна для роботи транспортних засобів, створення умов для надання послуг (освітлення, кондиціонування приміщень, робота інформаційних систем), створення умов, необхідних для підтримки роботи обладнання систем безпеки (освітлення, управління рухом, інформування та оповіщення тощо).

Урядування / цивільний захист необхідне / необхідний для підтримання роботи підприємств енергетики та забезпечення життєдіяльності громад, надання інформації для забезпечення роботи підприємств, захисту персоналу в кризових ситуаціях, надання адміністративних послуг персоналу.

7. Газозабезпечення – забезпечення: постачання палива для домогосподарств (приготування їжі та опалення), систем централізованого опалення (роботи котелень), виробничих процесів.

Електроенергія необхідна для роботи компресорних станцій, створення умов, необхідних для підтримки роботи обладнання та персоналу (освітлення, кондиціонування тощо).

Газозабезпечення необхідне для доставки палива для забезпечення роботи електростанції, роботи систем теплозабезпечення.

Джерело: розроблено автором.

Додаток 4. Огляд загроз для енергетичного сектору

Загроза	Можливі негативні наслідки для підсекторів критичної енергетичної інфраструктури		
	Електрозабезпечення	Газозабезпечення	Забезпечення моторним паливом
Кібератака	Можливий вплив на інформаційні технології (ІТ) та системи операційних технологій (ОТ), зокрема компанії, системи обліку, оплати та планування, системи управління		
Посуха	Зменшення виробництва гідроелектроенергії через низький рівень води. Зниження продуктивності роботи електростанцій, якщо існують обмеження на пару або охолодження	Обмеження щодо буріння, якщо немає альтернативного водопостачання	Зниження вологості в ґрунті обмежує утворення біомаси (ріст). Перешкоджання у використанні річок як шляхів транспортування. Обмеження роботи бурових установок та нафтопереробних заводів, якщо немає альтернативного водопостачання
Руйнування дамби	Пошкодження інфраструктури вниз за течією через затоплення та сміття. Виробництво гідроелектроенергії може бути порушено, що також може зменшити можливості аварійного запуску (відновлення енергосистеми)	Пошкодження інфраструктури вниз за течією через затоплення та сміття. Відкопування та розриви трубопроводів	Пошкодження інфраструктури вниз за течією через затоплення та сміття. Відкопування та розриви трубопроводів
Землетрус	Пошкодження інфраструктури. Приклади: об'єкти виробництва електроенергії, опори електропередачі тощо	Розриви трубопроводів, порушення роботи переробних заводів, свердловин, компресорних станцій	
Поломка обладнання	Електрична дуга, стрибки напруги, корозія або волога на обладнанні можуть призвести до несправності обладнання або виходу з мережі	Корозія, пошкодження матеріалу, підвищення тиску або несправність елементів керування можуть спричинити перебої в постачанні	
Висока температура	Підвищений попит на охолодження. Залежно від доступної потужності це може призвести до того, що енергосистема працюватиме нижче від резервних запасів. Підвищені ризики виникнення лісових пожеж від ліній електропередачі		Зниження ефективності нафтопереробних заводів

Загроза	Можливі негативні наслідки для підсекторів критичної енергетичної інфраструктури		
	Електрозабезпечення	Газозабезпечення	Забезпечення моторним паливом
Повені	Пошкодження інфраструктури вниз за течією через затоплення та сміття. Порушення роботи обладнання для виробництва електроенергії, будівлі центру управління, ліній електропередачі	Порушення роботи технологічних установок нафтопереробного заводу, резервуарів підземних трубопроводів	Порушення роботи переробних заводів, терміналів СПГ, підземних трубопроводів
Зсуви порід	Пошкодження сусідньої інфраструктури через уламки або удари фундаменту		
Спланована зловмисна фізична атака	Навмисні фізичні напади на інфраструктуру або захоплення інфраструктури. Людські помилки, що зумовляють роботу обладнання у позапроектних режимах. Лінії електропередачі можуть постраждати від дій людей, які руйнують стовпи електропередачі, зрізають дерева (гілки дерев) або пошкоджують підземні кабелі	Навмисні фізичні напади на інфраструктуру або захоплення інфраструктури	Навмисні фізичні напади на інфраструктуру або захоплення інфраструктури. Атаки на трубопроводи можуть призвести до розриву ліній електропередачі
Епідемія	Зміни в попиті та зменшення кількості працівників		
Літній шторм	Пошкодження інфраструктури внаслідок сильного вітру, сміття та повеней		
	Порушення роботи об'єктів виробництва електроенергії, опор електропередачі тощо	Порушення роботи трубопровідних насосів, резервуарів палива	Порушення роботи трубопровідних насосів, резервуарів
		Виробничі потужності та нафтопереробні заводи можуть зупинитися перед штормом для безпеки персоналу	
Грози з блискавками	Зруйновані трансформатори та повалені дерева можуть вплинути на лінії електропередачі	Перебої в електропостачанні можуть вплинути на роботу деяких електричних компресорів	Перебої в електропостачанні можуть вплинути на роботу нафтопереробного заводу, терміналу або перекачування
Лісові пожежі	Пошкодження ліній електропередачі та об'єктів електроенергетики. Комунальні служби можуть вимкнути електроенергію, щоб запобігти пожежам	Займистий матеріал у разі загоряння може вплинути на роботу наземної інфраструктури	

Загроза	Можливі негативні наслідки для підсекторів критичної енергетичної інфраструктури		
	Електрозабезпечення	Газозабезпечення	Забезпечення моторним паливом
	(наприклад, високим температурам і сильному вітру)		
Зимові шторми та заморозки	Замерзання в градирнях запобігає виробленню електроенергії. Заморожування залізниці впливає на сировину для виробництва електроенергії (наприклад, вугілля). Збільшення попиту на опалення може збільшити навантаження на наявну потужність, спричиняючи зменшення резервних запасів енергосистеми	Замерзання може вплинути на обладнання, яке не піддається погодним умовам, що може призвести до зупинки виробництва. Підвищений попит на опалення може перенавантажити енергорозподільчу систему	Замерзання обладнання, яке не піддається погодним умовам, включно замерзання речовин у системі трубопроводів, несправне обладнання контролю потоку, спалювання на факелі зупинку виробництва. Підвищений попит на резервні джерела енергії (генератор)
Торнадо	Сильний вітер може призвести до пошкодження ліній електропередачі та об'єктів виробництва електроенергії	Сильні вітри можуть завдати шкоди переробним підприємствам, компресорним станціям, вимірювально-регулюючим станціям та іншим наземним спорудам	Сильні вітри можуть завдати шкоди нафтопереробним заводам, терміналам та іншим наземним об'єктам

Джерело: адаптовано автором на основі²²⁰.

²²⁰ Див.: URL: <https://www.energy.gov/ceser/articles/doe-energy-emergency-response-playbook-states-and-territories>

Додаток 5. Загальний алгоритм оцінювання впливу загроз

1. У загальному випадку ризик реалізації загрози (R) визначається як добуток правдоподібності реалізації загрози та настання негативних наслідків:

$$R = LC,$$

де L – правдоподібність реалізації загрози;

C – негативний наслідок реалізації загрози, результат впливу на об'єкт управління.

2. Для цілей визначення загроз²²¹, які потребують першочергового планування заходів реагування (недопущення їх реалізації чи пом'якшення наслідків їх впливу), здійснюється ранжування загроз.

3. Ранжування загроз можна здійснювати за спрощеним алгоритмом оцінювання ризиків окремих загроз R_t , порівнюючи добутки усереднених оцінок загальної вірогідності L_t реалізації загрози (з наперед установленого переліку загроз $t = 1 \dots n$ ²²²) та сукупних негативних наслідків C_h (за переліком вибраних критеріїв оцінки цільових параметрів ЖВФ $h = 1 \dots m$ ²²³):

$$R_t = \sum_{t=1}^n L_t \sum_{h=1}^m C_h .$$

4. Оцінювання ризиків здійснюється шляхом експертного аналізу, тобто вибрані експерти на основі свого досвіду та знань формують власні судження щодо вірогідності реалізації загроз та наслідків їх реалізації.

5. Для оцінок правдоподібностей та наслідків встановлюється така градація (у балах)²²⁴:

- для правдоподібностей: «низька» (1), «помірно низька» (2), «середня» (3), «помірно висока» (4), «висока» (5);

- для наслідків: «незначні» (1), «неістотні» (2), «помірні» (3), «істотні» (4), «катастрофічні» (5).

6. Сукупність наслідків впливу кожної загрози визначається як середньоарифметичне значення оцінки впливу загрози на кожний із вибраних

²²¹ Перелік загроз формується на основі аналізу широкого спектру подій, чинників, явищ, які можуть негативним чином вплинути на функціонування КІ. Зазвичай початковий перелік загроз визначається на основі статистичного аналізу випадків порушення функціонування КІ за визначений період у минулому та аналізу нових тенденцій, що потенційно можуть вплинути на функціонування КІ.

²²² Орієнтовний перелік загроз для первинного аналізу ризиків функціонування енергетичній інфраструктурі наведено в додатку 4.

²²³ Перелік сукупних наслідків формується з огляду на цільові параметри функціонування КІ. Цільові завдання / функції визначаються суб'єктом аналізу ризиків, зважаючи на вимоги законодавства або цілей управлінської діяльності у визначеній сфері аналізу. Приклад визначення переліку ризиків (наслідків впливу загроз) порушення функціонування КІ для різних рівнів управлінської діяльності подано в табл. Д.5.2.

²²⁴ Орієнтовні рекомендації щодо визначення ризиків реалізації загроз у балах подано в табл. Д.5.3.

цілових параметрів функціонування критичної інфраструктури (на кожний із вибраних наслідків C_h)²²⁵.

7. Отриманні результати оцінки загроз можна подати у вигляді таблиці ранжованих за вагомістю впливу ризиків²²⁶ або у графічній формі (рис. Д.5.1).

Графічна форма є поширеною у світовій практиці для представлення результатів оцінок. З цією метою використовується матриця ризику (або карта ризику), у якій представлено залежності наслідків впливу визначених загроз та їх імовірності. Зазвичай використовується матриця розмірністю 5 x 5, у якій наслідки оцінюються від незначних до катастрофічних, а їх імовірність / частість – від дуже низької до високої. Для наглядного представлення рівня ризиків застосовується чотири діапазонна кольорова шкала: низький (зелений колір), середній (жовтий колір), високий (помаранчевий колір) та дуже високий (червоний колір).

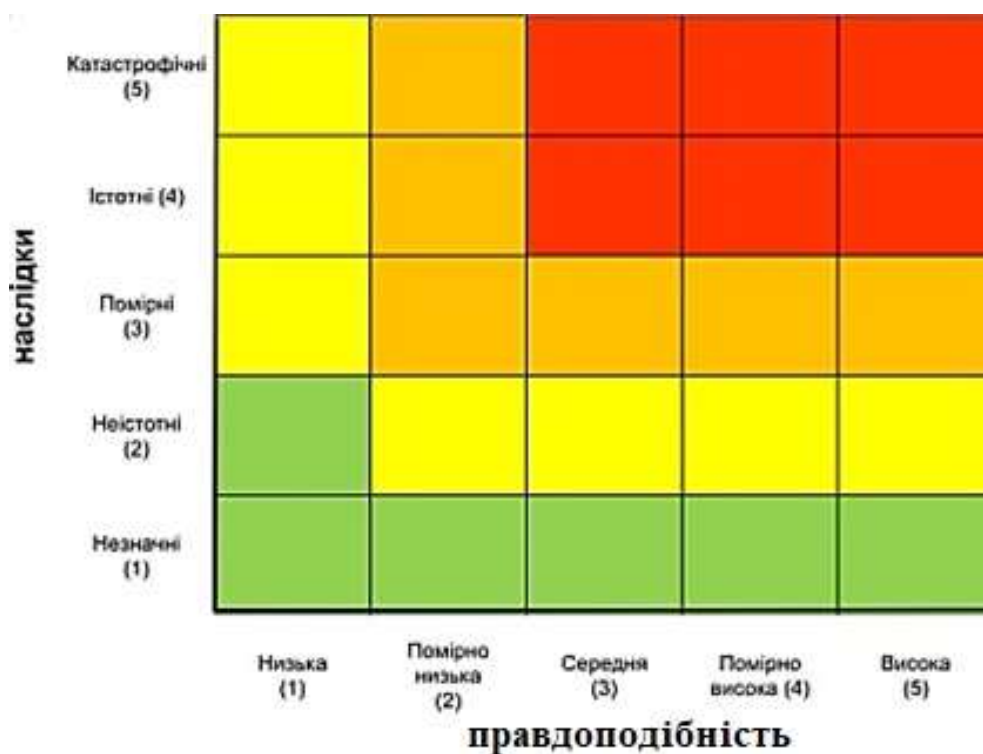


Рис. Д.5.1. Зразок матриці ризику

Джерело: складено автором.

8. Орієнтуючись на результати аналізу, суб'єкт аналізу приймає рішення щодо визначення межі переліку загроз, які будуть обрані для подальшого планування забезпечення стійкості функціонування КІ (планування заходів запобігання, реагування та пом'якшення впливу загроз).

²²⁵ Приклад визначення ризику (насадків впливу загроз) на рівні громади наведено в табл. Д.5.4.

²²⁶ Приклад ранжування загроз наведено в табл. Д.5.5.

Орієнтовні рекомендації щодо оцінки правдоподібності реалізації загрози

Правдоподібність	Визначення
Висока	Максимально можливий сценарій, тому що така загроза вже була реалізована протягом останніх кількох років або наявні вагомі докази щодо можливості, спроможності, намірів та планування здійснення такого сценарію реалізації загрози
Помірно-висока	Загроза ймовірна, тому що наявна інформація про відносно нещодавні приклади її реалізації або докази завчасного планування реалізації загрози
Середня	Значною мірою загроза реальна, тому що наявні дані про можливе виникнення умов реалізації загрози або є відомості про наміри та спроможність реалізувати загрозу
Помірно-низька	Приклади реалізації загрози відсутні на цей момент або подібні інциденти останнім часом не відбувалися, проте наявні деякі дані щодо потенційних намірів (або появи умов) реалізації загрози
Низька	Теоретично можливе виникнення загрози, проте відсутні обґрунтовані приклади чи ознаки, що загроза актуальна за цих умов

Джерело: розроблено автором.

Орієнтовні рекомендації щодо визначення переліку ризиків порушення цільових параметрів функціонування критичної інфраструктури

Орієнтовний перелік наслідків впливу загрози (ризиків реалізації загрози)				
Національні інтереси / безпека	Рівень функціонування критичної інфраструктури			
	загальнодержавний	секторальний	об'єктовий	місцевий (громади)
Економічні збитки	Економічні збитки	Економічні збитки	Економічні збитки (оператора)	Економічні збитки (громад)
Шкода довкіллю	Шкода довкіллю	Шкода довкіллю	Шкода довкіллю (громад)	Шкода довкіллю (громад)
Чисельність ураженого населення (вимушена міграція чи потреба прихистку / допомоги)	Чисельність ураженого населення (вимушена міграція чи потреба прихистку / допомоги)	Чисельність ураженого населення (вимушена міграція чи потреба прихистку / допомоги)	Чисельність ураженого населення (вимушена міграція чи потреба прихистку / допомоги)	Чисельність ураженого населення громад (вимушена міграція чи потреба прихистку / допомоги)
Зниження обороноздатності	Зниження рівня надання життєво важливих функцій / послуг	Зниження рівня надання секторальних життєво важливих функцій / послуг	Зниження рівня виробництва / надання основної послуги (продукції)	Зниження рівня надання життєво важливих послуг громадам
Чисельність населення, що зазнало ризику втрати здоров'я	Чисельність населення, яке зазнало ризику втрати здоров'я	Чисельність населення, яке зазнало ризику втрати здоров'я	Чисельність населення, яке зазнають ризику втрати здоров'я	
Міжнародне співробітництво	Вплив на роботу КІ, транскордонні потоки	Вплив на інші сектори КІ	Вплив на інші сектори КІ	
Публічне сприйняття ситуації, яка спричинена впливом загрози	Публічне сприйняття ситуації, яка спричинена впливом загрози			

Джерело: розроблено автором.

Орієнтовні рекомендації щодо визначення бальної оцінки ризиків (наслідків впливу загроз)

Ризики (цільові параметри)	Критерії оцінювання наслідків впливу загрози				
	1	2	3	4	5
Економічні збитки	Менше 100 млн грн	Від 100 млн до 1 млрд грн	1...10 млрд грн	10...50 млрд грн	Більше 50 млрд грн
Чисельність населення, яке зазнало ризику втрати здоров'я (фатальність)	Менше 10 осіб	10...50 осіб	50...500 осіб	500...1000 осіб	Більше 1000 осіб
Зниження рівня надання життєво важливих функцій / послуг, тривалість зниження рівня	Менше 5 % функцій / послуг, що зазнають порушень; 1...2 дні	5...10 % функцій / послуг, що зазнають порушень; 2...4 дні	10...20 % функцій / послуг, що зазнають порушень; 3...5 днів	20...40 % функцій / послуг, що зазнають порушень; 5...10 днів	Понад 40 % функцій / послуг, які зазнають порушень; понад 10 днів
Шкода довкіллю	Навколо об'єкта критичної інфраструктури, термін до 1 місяця	Територія громади на термін до 1 місяця або навколо будівлі на 1 рік	Територія району на термін до 1 року	Територія області на термін до 1 року	Територія кількох областей (або території з населенням 3 млн осіб) на термін до 1 року
Вплив на інші сектори КІ	Один (свій) сектор КІ	2-3 суміжні сектори КІ	30 % секторів КІ	30...50 % секторів КІ	Понад 50 % секторів КІ
Зниження обороноздатності	Зниження на менше ніж на 5 %	Зниження 5...10 %	Зниження 10...20 %	Зниження 20...30 %	Зниження 30...50 %
Міжнародне співробітництво	Помірне погіршення відносин із будь-якою країною	Серйозне погіршення відносин із будь-якою країною	Помірне погіршення відносин з країнами-партнерами	Серйозне погіршення відносин з країнами-партнерами	Серйозне погіршення відносин з країнами-союзниками
Зниження рівня надання секторальних життєво важливих функцій / послуг	Зниження на 5 % функцій / послуги, що зазнають порушень; 1...3 днів	Зниження 5...10 % функцій / послуг, що зазнають порушень; 2...4 дні	Зниження 10...20 % функцій / послуг, що зазнають порушень; 3...5 днів	Зниження 20...40 % функцій / послуг, що зазнають порушень; 5...10 днів	Зниження на понад 50 % функцій / послуг, що зазнають порушень; понад 10 днів

Ризики (цільові параметри)	Критерії оцінювання наслідків впливу загрози				
	1	2	3	4	5
Зниження рівня виробництва / надання основної послуги (продукції) (електрозабезпечення)	Втрата послуги (електрозабезпечення) для 1 тис. абонентів	Втрата послуги (електрозабезпечення) для понад 50 тис. абонентів	Втрата послуги (електрозабезпечення) для понад 300 тис. абонентів	Втрата послуги (електрозабезпечення) для понад 1 млн. абонентів	Втрата послуги (електрозабезпечення) для понад 3 млн. абонентів
Зниження рівня надання життєво важливих послуг громаді (медичні послуги)	Втрата послуги (медичної підтримки) для 5 % осіб громади на термін до 6 год	Втрата послуги (медичної підтримки) для 10 % осіб громади на термін до 1 доби	Втрата послуги (медичної підтримки) для 25 % осіб громади на термін до 3 днів	Втрата послуги (медичної підтримки) для 50 % осіб громади на термін до 10 днів	Втрат послуги (медичної підтримки) для 60 % осіб громади на термін до 30 днів
Чисельність ураженого населення (вимушена міграція чи потреба прихистку / допомоги)	Вплив на 1 тис. осіб на термін до 24 год	Вплив на 10 тис. осіб на термін до 10 днів	Вплив на 100 тис. осіб на термін до 30 днів	Вплив на 1 млн осіб на термін до 3 місяців	Вплив на понад 3 млн осіб на термін понад 3 місяці
Публічне сприйняття ситуації, спричинене впливом загрози	Занепокоєння відчуває менше 2 % населення	Занепокоєння відчуває 2...5 % населення	Занепокоєння відчуває 5...10 % населення	Сильне занепокоєння відчуває 10...30 % населення	Гостре занепокоєння відчуває понад 30 % населення

Джерело: розроблено автором.

Приклад оцінювання ризиків впливу загроз на життєдіяльність громади, бали

Загроза	Правдо- подібність	Наслідки впливу загрози на цільові параметри життєдіяльності громад						Сумарні наслідки	Ризик
		Економічні збитки	Шкода довкіллю	Чисельність ураженого населення (вимушена міграція)	Зниження рівня надання функцій / послуг (електро- забезпечення)	Зниження рівня надання функцій / послуг (медичні послуги)	Зниження рівня надання функцій / послуг (транспорту- вання)		
Диверсія чи терористичний акт	2	3	1	2	4	2	3	2,5	5
Кібератака	4	2	1	1	2	3	2	1,8	7,2
Епідемія	1	5	2	5	1	3	2	3,0	3
Різке та значне зниження температури	3	3	1	3	3	2	3	2,5	7,5

Джерело: розроблено автором.

Приклад ранжування загроз критичній інфраструктурі, бали

Загроза	Правдоподібність	Наслідки	Ризик
Різка та значне зниження температури	3	2,5	7,5
Кібератака	4	1,8	7,2
Диверсія або терористичний акт	2	2,5	5
Епідемія	1	3,0	3

Джерело: розроблено автором.

Додаток 6. Потенціал відновлюваних джерел енергії України

Наведений нижче потенціал середньорічного виробітку електроенергії відновлюваними джерелами визначений Інститутом відновлюваної енергетики НАН України²²⁷ з урахуванням поточного розвитку енергетичних технологій станом на 2020 рік. Завдяки науково-технічному розвитку, уточненню ресурсної бази та зміні соціально-економічних моделей регулювання енерговикористання кількісні параметри досяжного для використання енергетичного потенціалу відновлюваних джерел енергії на всій території України можуть бути суттєво збільшені (табл. Д.6.1, Д.6.2).

Таблиця Д.6.1

Потенціал встановленої потужності відновлюваних джерел енергії в областях України, МВт

№	Адміністративна одиниця (АРК та області)	Енергія					Усього
		сонця	вітру	малих ГЕС	гео-термальна	біомаси	
1	Автономна Республіка Крим	3603	22 128	1	840	1273	27 844
2	Вінницька	3646	13 393	24	40	6192	23 295
3	Волинська	2770	7184	1	40	2239	12 234
4	Дніпропетровська	4388	38 978	2	120	5128	48 616
5	Донецька	3646	32 387	5	200	2835	39 072
6	Житомирська	4102	10 640	8	50	4575	19 374
7	Закарпатська	1757	1163	132	1400	1209	5661
8	Запорізька	3737	33 196	0	40	3646	40 620
9	Івано-Франківська	1911	2416	59	600	1671	6658
10	Київська	3868	11 983	3	40	4961	20 855
11	Кіровоградська	3381	21 226	15	40	4482	29 144
12	Луганська	3669	32 591	2	80	2042	38 384
13	Львівська	3002	8015	46	1400	2672	15 135
14	Миколаївська	3382	30 043	3	80	3435	36 943
15	Одеська	4580	34 719	1	240	4912	44 453
16	Полтавська	3953	14 522	6	1400	5662	25 544
17	Рівненська	2756	7745	3	40	2594	13 139

²²⁷ Атлас енергетичного потенціалу відновлюваних джерел енергії України / за заг. ред. С. О. Кудрі. Київ : Ін-т відновлюваної енергетики НАН України, 2020. 82 с.

№	Адміністративна одиниця (АРК та області)	Енергія					Усього
		сонця	вітру	малих ГЕС	гео- термальна	біомаси	
18	Сумська	3277	11 096	2	560	5009	19 945
19	Тернопільська	1901	6983	12	80	3019	11 995
20	Харківська	4320	27 119	10	1300	5160	37 908
21	Херсонська	3913	34 761	1	1300	3360	43 335
22	Хмельницька	2839	10 429	8	40	4668	17 984
23	Черкаська	2874	10 558	8	40	4150	17 630
24	Чернівецька	1113	2414	24	40	1252	4843
25	Чернігівська	4381	12 311	1	800	5932	23 425
	Разом	82 768	438 000	376	10 810	92 078	624 033

Джерело: ²²⁸.

Таблиця Д.6.2

**Потенціал середньорічного виробітку електроенергії
відновлюваними джерелами, млн кВт·год/рік**

№	Адміністративна одиниця (АРК та області)	Енергія					Усього
		сонця	вітру	малих ГЕС	гео- термальна	біомаси	
1	Автономна Республіка Крим	4323	60 090	3	5236	6255	75 907
2	Вінницька	4375	36 371	83	298	25 327	66 453
3	Волинська	3324	19 510	4	298	8310	31 446
4	Дніпропетровська	5266	105 849	7	894	20 646	132 662
5	Донецька	4375	87 949	16	1489	11 673	105 502
6	Житомирська	4922	28 893	27	372	16 619	50 834
7	Закарпатська	2108	3157	439	10 424	4180	20 308
8	Запорізька	4485	90 148	1	298	14 089	109 020
9	Івано-Франківська	2294	6562	196	4468	6415	19 935
10	Київська	4642	32 540	11	298	20 116	57 606
11	Кіровоградська	4057	57 641	53	298	17 724	79 773
12	Луганська	4403	88 503	7	596	8032	101 540
13	Львівська	3602	21 766	153	10 424	10 428	46 373

²²⁸ Атлас енергетичного потенціалу відновлюваних джерел енергії України / за заг. ред. С. О. Кудрі. Київ : Ін-т відновлюваної енергетики НАН України, 2020. 82 с.

№	Адміністративна одиниця (АРК та області)	Енергія					Усього
		сонця	вітру	малих ГЕС	гео- термальна	біомаси	
14	Миколаївська	4059	81 584	11	596	13 448	99 697
15	Одеська	5496	94 283	5	1787	19 693	121 264
16	Полтавська	4743	39 437	22	10 424	22 425	77 051
17	Рівненська	3308	21 033	10	298	9396	34 045
18	Сумська	3933	30 133	8	4170	19 445	57 689
19	Тернопільська	2281	18 963	42	596	12 301	34 182
20	Харківська	5183	73 645	33	9680	20 171	108 713
21	Херсонська	4696	94 397	2	9680	13 212	121 987
22	Хмельницька	3406	28 321	29	298	18 719	50 774
23	Черкаська	3449	28 671	28	298	16 964	49 410
24	Чернівецька	1336	6554	80	298	4714	12 982
25	Чернігівська	5258	33 433	2	5957	22 879	67 528
	Разом	99 323	1 189 433	1272	80 494	362 161	1 732 682

Джерело: ²²⁹.

²²⁹ Атлас енергетичного потенціалу відновлюваних джерел енергії України / за заг. ред. С. О. Кудрі. Київ : Ін-т відновлюваної енергетики НАН України, 2020. 82 с.

Додаток 7. Приклади реалізації проєктів енергозабезпечення територіальних громад України на основі використання місцевих ресурсів

Рішення (проєкт)	Загальні параметри запропонованих рішень	Короткий опис рішення (проєкту)	Суб'єкти реалізації	Локація
Комплексне рішення із теплозабезпечення громади на базі власних ресурсів ²³⁰	Побудовано три котельні загальною потужністю 3,4 МВт (0,85, 1,35 та 1,22 МВт відповідно)	Створено енергетичний кластер для місцевої громади. Побудовано три котельні, паливом для яких є деревна тріска з плантацій енергетичної верби, що розташовані в радіусі 20 км. На території громади на 295 га вирощують 5-6 тис. т тріски на рік, це при середньорічному споживанні котелень 2 тис. т. Завдяки реалізації проєкту було проведено реконструкцію газових котелень із встановленням твердопаливних котлів і системи подачі палива, а також прокладено нові теплові мереж. До однієї з котелень підключено нового споживача	Місцеві органи самоврядування, компанії-постачальники обладнання й сировини, установи-споживачі	СМТ Іваничі, Волинська область
Теплозабезпечення окремих об'єктів громади з використанням місцевої агробіомаси ²³¹	Встановлено два котли потужністю 0,4 МВт кожен	У територіальній громаді на 2,2 тис га вирощують зернові культури, відповідно утворюється й залишається солома. Започатковано виробництво брикетів із соломи для спалювання в котлах. Також у котлах спалюють комиш і т. зв. мішанку (комиш, стебло кукурудзи й сіно). У модульній котельні, що працює на солімі та опалює школу, встановлено два котли потужністю 0,4 МВт кожен. За опалювальний період ця школа на 82 % потреб у теплопостачанні забезпечується місцевим ресурсом	Місцеві органи самоврядування, компанії-постачальники обладнання й сировини, установи-споживачі	с. Веселе, Харківська область
Використання сонячної енергії для	Встановлено 144 сонячні панелі	Енергетичний кооператив установив сонячну електростанцію на дахах універмагу, будинку культури	Енергетичний кооператив,	м. Славутич

²³⁰ Трибой О., Радченко С., Зубенко В., Гайдай О. Сприяння енергетичній безпеці та сталому розвитку місцевих громад в Україні. Київ : ГО «Агентство з відновлюваної енергетики», 2021. URL: <https://rea.org.ua/wp-content/uploads/2021/10/handbook-promoting-energy-security.pdf>

²³¹ Там само.

Рішення (проект)	Загальні параметри пропонуваніх рішень	Короткий опис рішення (проекту)	Суб'єкти реалізації	Локація
виробництва електроенергії ²³²	загальною потужністю 200 кВт	та будинку побуту, її загальна площа 4700 м ² Капітальні затрати проекту становили 175 513 євро. Цю суму було поділено на 320 паїв із вартістю одного паю близько 550 євро. З урахуванням дисконтування окупність проекту становить сім років	Комунальне підприємство «Агенція регіонального розвитку», фізичні особи. Було підписало договір оренди трьох дахів до 2049 р.	
Комплексне рішення із теплозабезпечення громади ²³³	Будівництво котельні потужністю 10,5 мВт	У м. Славутичі на Київщині почала працювати найбільша в Україні котельня на біопаливі потужністю 10,5 мВт. Котельня на 40 % забезпечує потреби міста в тепловій енергії та гарячій воді завдяки використанню ВДЕ. Передбачається подальший розвиток енергетичного кластеру навколо м. Славутича. Планується будівництво біоТЕЦ на ВДЕ загальною потужністю 12,5 МВт на годину електричної енергії, яка також вироблятиме 25 ГКал/год теплової енергії. Неподалік міста буде висаджено близько 1500 га енергетичної верби. Це дасть можливість забезпечити котельню та біоТЕЦ деревинною сировиною	Місцеві органи самоврядування, компанії-постачальники обладнання й сировини, установи-споживачі, центральні органи виконавчої влади	м. Славутич, Київська область
Реконструкція та переведення системи централізованого теплозабезпечення міста на використання біомаси ²³⁴	Реконструкція котельнь (встановлення нових десяти котельнь потужністю до 1500 кВт), модернізація системи централізованого теплопостачання	У м. Дубно проживає близько 40 тис. людей, 30 % із них отримують тепло централізовано. Міська система теплопостачання складається з п'яти котельнь і має тепломережі протяжністю 16 км. Місто, модернізуючи систему теплопостачання, до тих газових систем, які були, додатково встановило 9 твердопаливних котлів (1250 та 1500 кВт), а також електрогенератор на 180 кВт, який можна за потреби перевозити з котельні до котельні. Котли можуть переключатися з одного виду палива на інший (використовують також і газ на випадок дуже	Місцеві органи самоврядування, компанії-постачальники обладнання й сировини, установи-споживачі	м. Дубно, Рівненська область

²³² Трибой О., Радченко С., Зубенко В., Гайдай О. Сприяння енергетичній безпеці та сталому розвитку місцевих громад в Україні. Київ : ГО «Агентство з відновлюваної енергетики», 2021. URL: <https://rea.org.ua/wp-content/uploads/2021/10/handbook-promoting-energy-security.pdf>

²³³ У Славутичі на Київщині почала працювати найбільша в Україні котельня на біопаливі потужністю 10,5 мВт. URL: <https://www.epravda.com.ua/news/2017/11/20/631376/>

²³⁴ Як Дубно пережило першу зиму без газу. URL: <https://enefcities.org.ua/novyny/yak-dubno-perejylo-pershu-zymu-bez-gazu/>

Рішення (проект)	Загальні параметри пропонуваніх рішень	Короткий опис рішення (проекту)	Суб'єкти реалізації	Локація
		сильних морозів або зупинки твердопаливних котлів на ремонт або чистку). У якості палива використовуються паливні гранули, торфобрикети, торфокрихту, дрова й тирсу. Паливна гранула йде з відходів підприємств місцевої агропромисловості. Місто планує додатково встановити вітрову електростанцію, а також сонячну на даху місцевих соціальних та освітніх закладів. На випадок надзвичайної ситуації місто має пересувні резервні генератори, що дозволяють забезпечити 80 % потреб у електроенергії		
Теплозабезпечення промислового майданчика та об'єктів громади з використанням місцевої агробіомаси ²³⁵	Встановлено паровий котел, його паропродуктивність 2,5 т/год, потужність 2 МВт	Виробничою аграрною компанією було реалізовано проект власного забезпечення потреб у тепловій енергії. Збудовано парову котельню, яка працює на тюкованій соломі та виробляє технологічну пару для виробничого майданчика, що розміщений на території громади. Солому заготовляють на власних полях місцевого підприємства. Подібні котли були встановлені на всіх дев'яти свинокомплексах підприємства, розміщених в інших громадах	Виробнича аграрна компанія	с. Переяславське, Київська область
Модернізація котелень та будівництво ТЕС на біомасі для часткового заміщення газу	Реконструкція котелень місцевого підприємства теплопостачання	У м. Рівному було прийнято стратегію заміщення використання газу в системі теплопостачання міста ²³⁶ . Місцеве підприємство теплопостачання реалізує стратегію модернізації котелень і системи теплопостачання для пріоритетного використання біомаси та заміщення природного газу у якості палива. Встановлено 30 котлів, що працюватимуть на біомасі, а частина котелень стануть комбінованими: 60–70 % тепла вироблятиметься за допомогою газу, а 30–40 % – за допомогою пелет, брикетів та інших видів біомаси ²³⁷ . Для стабільного	Місцеві органи самоврядування, компанії-постачальники обладнання й сировини, установи-споживачі	м. Рівне, Рівненська область

²³⁵ Трибой О., Радченко С., Зубенко В., Гайдай О. Сприяння енергетичній безпеці та сталому розвитку місцевих громад в Україні. Київ : ГО «Агентство з відновлюваної енергетики», 2021. URL: <https://rea.org.ua/wp-content/uploads/2021/10/handbook-promoting-energy-security.pdf>

²³⁶ Схема теплопостачання м. Рівного. URL: http://rvrada.gov.ua/portalfiles/1/232/11419/Звіт_Рівне__ТОМ_1.pdf

²³⁷ У розвиток ТОВ «Рівнетеплоенерго» буде інвестовано 50 млн євро. URL: <http://rivneteploenergo.com/u-rozvytok-tov-rivneteploenerho-bude-investovano-50-mln-jevro/>

Рішення (проект)	Загальні параметри пропонуваніх рішень	Короткий опис рішення (проекту)	Суб'єкти реалізації	Локація
		забезпечення підприємства біопаливом висаджено плантацію енергетичної верби ²³⁸		
Когенерація в системах теплопостачання	Реконструкція котельнь та встановлення когенераційних установок потужністю до 2 МВт	У м. Хмельницькому використовують 13 когенераційних установок (КГУ) для генерації теплової та електричної енергії. Електрична потужність цих установок становить 6,375 МВт. Теплопостачальні підприємства покривають власні потреби в електричній енергії та продають надлишки в мережу (близько 2,5 МВт), зокрема для забезпечення живлення критичної інфраструктури. КГУ приєднані до електромереж за схемою, яка дозволяє забезпечувати власні потреби в електрозабезпеченні навіть за відсутності енергопостачання з мережі. Крім того, частина об'єктів теплопостачального підприємства заживлені від КГУ шляхом прокладання прямого електричного кабелю. В перспективі керівництво підприємства розглядає можливість заживлення всіх власних об'єктів від КГУ, таким чином забезпечуючи роботу систем теплопостачання навіть за умов блекауту	Місцеві органи самоврядування, компанії-оператори систем теплопостачання, компанії-постачальники обладнання та сировини, установи-споживачі	м. Хмельницький, Хмельницька область
Когенерація в системах теплопостачання	Реконструкція котельнь та встановлення когенераційних установок потужністю до 1 МВт	У м. Старокостянтиніві на місцевому теплопостачальному підприємстві було виведено із експлуатації котел 2,2 МВт, натомість встановлено КГУ потужністю 500 кВт електричної енергії та 720 кВт – теплової. КГУ приєднано до електромережі 0,4 кВ. Сама котельня, на якій встановлено КГУ, споживає 80–100 кВт, надлишок потужностей використовується для живлення інших об'єктів теплопостачальної організації шляхом прокладання електричного кабелю. Так, були приєднані на відстані близько 600 м ЦТП 1 з електричним навантаженням 25–30 кВт та ЦТП 2 – 6 кВт, а також ЦТП 3 з електричним навантаженням 25–30 кВт, що розташоване на відстані 400 м.	Місцеві органи самоврядування, компанії-оператори систем теплопостачання, компанії-постачальники обладнання та сировини, установи-споживачі	м. Старокостянтинів, Хмельницька область

²³⁸ Рівнетеплоенерго висадило плантацію енергетичної верби для котельнь, що працюють без газу. URL: <http://rivneteploenergo.com/rivneteploenerho-vysadylo-plantaciju-enerhetychnoji-verby-dlja-kotelen-scho-pracjijut-bez-hazu/>

Рішення (проект)	Загальні параметри пропонуваніх рішень	Короткий опис рішення (проекту)	Суб'єкти реалізації	Локація
		Передбачається приєднання до КГУ головної каналізаційної насосної станції міста, що належить КП «Водоканал», з електричним навантаженням 120–150 кВт. Для цього необхідно прокласти кабельну трасу довжиною 800 м та встановити комплектну трансформаторну підстанцію (КТП 04/10 потужністю 250 кВт)		
Когенерація в системах теплопостачання	Встановлення когенераційних установок потужністю до 2 МВт	У м. Черкасах теплопостачальне підприємство в 2013 р. встановило три когенераційні установки (одна на 1460 кВт (теплова потужність 1731 кВт), дві – на 1200 кВт (теплова потужність 1293 кВт). Підприємство розробило схему аварійного живлення в режимі «острів» низки котелень, без КГУ, за рахунок генерації електроенергії від когенераційних установок. На випадок надзвичайних ситуацій передбачено аварійне заживлення низки котелень від дизельних генераторів	Місцеві органи самоврядування, компанії-оператори систем теплопостачання, компанії-постачальники обладнання та сировини, установи-споживачі	м. Черкаси, Черкаська область
Комплекс забезпечення соціального поселення електричною й тепловою енергією з використанням ВДЕ (проект) ²³⁹	Комплексна система енергозабезпечення, що забезпечує електричну потужність близько 200 кВт; теплові потреби в зимовий період 700 кВт, або 780 МВт·год за сезон	Проект розроблено Інститутом відновлюваної енергетики (ІВЕ НАН) України. Проект передбачає створення у сільській місцевості (поряд із населеними пунктами) соціального поселення, разом із промислово-виробничим комплексом аграрного спрямування, з використанням маловартісної енергозберігальної будівельної технології та впровадженням комплексної системи енергозабезпечення з використанням ВДЕ (основні джерела), а також електричної мережі обленерго (допоміжне джерело). Передбачено сонячну електростанцію потужність 2,9 МВт, вітроелектростанцію 2 МВт, тепловий насос, біоенергетичні установки 0,5 МВт	ІВЕ НАН України, Громадська організація «Вільна генерація»	с. Городище, Київська область
Енергетичний кластер багатоцільового призначення із	Фотоелектрична потужність 18 кВт; теплові насоси 5,5 кВт «повітря –	Створено демонстраційний проект побудови енергосистем з використанням ВДЕ різних видів для споруд, окремих і групових споживачів, із застосуванням акумулювання теплової та електричної енергії, резервного обладнання,	Комплекс адміністративних та лабораторних приміщень ІВЕ НАН	м. Київ, вул. Метрологічна

²³⁹ Інститут відновлюваної енергетики НАН України. Реєстраційний номер науко-дослідної роботи ДР № 0118U001794. URL: https://www.ive.org.ua/?page_id=6&lang=uk

Рішення (проект)	Загальні параметри пропонуваніх рішень	Короткий опис рішення (проекту)	Суб'єкти реалізації	Локація
забезпечення електричною й тепловою енергією з використанням відновлюваних джерел ²⁴⁰	вода» та 5,5 кВт «вода – вода»; акумулятор теплоти підземних шарів об'ємом 5 м ³	а також теплових насосів. Система енергопостачання передбачає автономну та/або комбіновану форму живлення та завдяки модульному принципу – можливість масштабування генерації енергії відповідно до потреб споживача	України	
Дахова сонячна електрична станція (перша промислова у м. Києві)	Встановлення сонячних панелей потужність 105 кВт	Виробництво електроенергії для забезпечення потреб підприємства та передачі надлишку в мережу	Розроблено ІВЕ НАН України, реалізовано місцевим приватним інвестором	м. Київ, вул. Електротехнічна
Енергонезалежні медичні заклади ²⁴¹	П'ять лікарень із встановленою автономною системою енергозабезпечення: сонячні електростанції встановленою потужністю 70 кВт; резервні накопичувачі електричного живлення потужністю кВт; дизельні генератори потужністю 160 кВт	Спорудження лікарень, які будуть мати автономне енергозабезпечення (проект реалізовано за підтримки Німеччини та ЄС) у п'яти областях. Для кожної лікарні збудовані автономні сонячні електричні станції встановленою потужністю 70 кВт. Вони розраховані на забезпечення безперебійного функціонування всього наявного медичного обладнання у збудованих модулях (без урахування потреб опалення). Сонячні панелі встановлено на модульних блоках, дахах закладів, земельних ділянках поруч із модульною лікарнею – залежно від ситуації. До складу сонячної станції також входять резервні накопичувачі електричного живлення потужністю 50 кВт, установлені в модульних лікарнях, гібридні та мережеві інвертори, програмне забезпечення для роботи станцій у режимі онлайн. Для аварійного енергопостачання п'яти лікарень також встановлені дизельні генератори потужністю 160 кВт разом із резервом палива	Місцеві органи самоврядування, міжнародні організації, установи-споживачі електроенергії, постачальники обладнання	м. Перещепине, Дніпропетровська область смт Широке, Запорізька область селище Березанка, Миколаївська область м. Тростянець, Сумська область м. Чернігів
Енергозабезпечення громади	Побудовано біоТЕС потужністю 5,9 МВт	Поліська ТЕС у м. Овручі є кліматично нейтральною, працює на місцевій сировині – залишках деревини	Місцеві органи самоврядування,	м. Овруч, Житомирська

²⁴⁰ Інститут відновлюваної енергетики НАН України. Реєстраційний номер науко-дослідної роботи ДР № 0123U100830. URL: https://www.ive.org.ua/?page_id=6&lang=uk

²⁴¹ Уряд Німеччини та ЄС профінансував будівництво шести енергонезалежних лікарень. URL: <https://www.epravda.com.ua/news/2023/11/21/706824/>

Рішення (проект)	Загальні параметри пропонуваніх рішень	Короткий опис рішення (проекту)	Суб'єкти реалізації	Локація
з використанням місцевої біомаси ²⁴²		від деревообробної промисловості, санітарного очищення лісів та енергетичній вербі, яку вирощують поруч із ТЕС. Разом із плантаціями енергетичної верби утворює зелений енергетичний кластер – повний цикл: від вирощування палива до виробництва електроенергії. Створено 50 робочих місць і ще 200–300 робочих місць – у сфері заготівлі та доставки тріски деревини. ТЕС здатна забезпечити безперебійну подачу електроенергії в період пікових навантажень і зможе відпускати в енергомережу понад 40 млн кВт·год електроенергії щорічно	приватна компанія, установи-споживачі тепла та електроенергії	область
Будівництво біоТЕС з метою використання місцевих ресурсів для потреб громади	Побудовано біоТЕС потужністю 8,6 МВт ²⁴³	Проект будівництва теплоелектростанції, що використовує місцеву агросировину реалізовувався у м. Токмаку, Запорізької області. Придніпровська БіоТЕС розташована на площі ділянкою 4,10 га в промисловій зоні. Як паливо електростанція використовуватиме лушпиння соняшника та солому. Потужність біоТЕС – 8,6 МВт електроенергії та 24 МВт теплопостачання	Місцеві органи самоврядування, приватні компанії-постачальники обладнання, сировини, технічних рішень, установи-споживачі тепла та електроенергії	м. Токмак, Запорізька область
Будівництво біогазових станцій з метою використання місцевих ресурсів для потреб громади	Встановлення електрогенеруючих установок потужністю 2 МВт ²⁴⁴	Біогазова станція на полігоні твердих побутових відходів у Лівобережному районі м. Маріуполя почала працювати на початку 2020 р. Сумарна встановлена потужність двох черг становить 2 МВт. Того ж року, менше ніж за рік роботи, біогазова станція виробила 2,2 млн кВт·год електроенергії і сплатила місту понад 650 тис. грн за договором про співпрацю, а також близько 100 тис. грн інших податків та зборів	Місцеві органи самоврядування, приватні компанії-постачальники обладнання, сировини, технічних рішень, установи-споживачі тепла та електроенергії	м. Маріуполь, Донецька область
Будівництво біогазових станцій	Встановлення електрогенеруючих	Біогазова станція на Рівненському сміттєзвалищі потужністю 500 кВт розпочала роботу в 2017 р. Збір біогазу	Місцеві органи самоврядування,	м. Дубно, Рівненська область

²⁴² Енергетична децентралізація: в Овручі розпочала роботу теплоелектростанція на біомасі. URL: <http://ukrteplo.ua/novini/energetichna-detsentralizatsiya-v-ovruchi-rozrochala-robotu-teploelektrostantsiya-na-biomasi/>

²⁴³ Придніпровська БіоТЕС. URL: <http://ukrteplo.ua/nashi-proekti/pridniprovska-tes/>

²⁴⁴ У Маріуполі побутові відходи перероблятимуть в електроенергію. URL: <https://mariupolrada.gov.ua/news/u-mariupoli-pobutovi-vidhodi-pererobljatimut-v-elektroenergiju>

Рішення (проект)	Загальні параметри пропонуваніх рішень	Короткий опис рішення (проекту)	Суб'єкти реалізації	Локація
з метою використання місцевих ресурсів для потреб громади	установок потужністю 500 кВт ²⁴⁵	здійснюється свердловинами з полігону твердих побутових відходів. Біогаз газопроводами транспортується на майданчик, де розміщується компресорна станція, готується і очищується. Від компресорної станції біогаз подається на когенераційну установку, де виробляється електроенергія. Вироблена електроенергія передається в загальну електромережу. Станція щороку видобуває 3–4 млн м ³ газу, за допомогою якого виробляється понад 4 млн кВт·год	приватні компанії-постачальники обладнання, сировини, технічних рішень, установи-споживачі тепла та електроенергії	
Будівництво для потреб громади біогазових станцій, що використовують місцеві ресурси	Встановлення електрогенеруючих установок потужністю 500 кВт ²⁴⁶	У м. Кам'янець-Подільському ввели в експлуатацію біогазову установку, яка виробляє електроенергію із сміття. Установка потужністю 500 кВт вироблятиме близько 4 млн кВт·год електроенергії щорічно.	Місцеві органи самоврядування, приватна компанія – розробник проекту, установи-споживачі тепла та електроенергії	М Кам'янець-Подільський, Хмельницька область
Будівництво біогазових станцій з метою використання місцевих ресурсів для потреб громади	Виробництво біогазу обсягом 1,2 тис. м ³ щодня для подальшого використання громадою ²⁴⁷	На Вінниччині приватне молочне підприємство запустило очисні споруди з виробництвом біогазу. Раніше всі стоки та брудні води, що утворювалися під час виробництва молока, а саме під час миття молоковозів чи заводських систем, відправляли у міські стоки. Комплекс дозволяє очищати два мільйони літрів води за добу. Крім очищеної води, очисні споруди виробляють біогаз для власних потреб та мінеральні добрива. Обсяг отриманого біогазу становить близько 1,2 тис. м ³ на день, а мінеральних добрив – 2-3 м ³	Приватні компанії (власник та постачальники), споживачі продукції, місцеві органи самоврядування	м. Іллінка, Вінницька область

²⁴⁵ Біогазова станція у м. Рівному. URL: <http://ukrteplo.ua/nashi-proekti/biogazova-stantsiya-u-m-rivne/>

²⁴⁶ У Кам'янець-Подільському ввели в експлуатацію біогазову установку, яка вироблятиме електроенергію із сміття. URL: <https://web.archive.org/web/20180827142556/http://uprom.info/news/energy/u-kam-yanets-podilskomu-vveli-v-ekspluatatsiyu-biogazovau-ustanovkau-yaka-viroblyatime-elektroenergiyu-iz-smittyu/>

²⁴⁷ Молочне підприємство на Вінниччині запустило очисні споруди з виробництвом біогазу. URL: <https://web.archive.org/web/20191104102139/https://ecotown.com.ua/news/Molochne-pidpriyemstvo-na-Vinnychchini-zapustilo-ochysni-sporudy-z-vyrobnystvom-biohazu/>

Рішення (проект)	Загальні параметри пропонуваніх рішень	Короткий опис рішення (проекту)	Суб'єкти реалізації	Локація
Будівництво малих та міні гідроелектростанцій для потреб споживачів громад	Будівництво міні гідроелектростанції потужністю 180 кВт ²⁴⁸	Міні гідроелектростанцію потужністю 0,18 МВт встановлено на Вінниччині. Обсяг інвестицій становив близько 13 млн грн. Встановлено сучасне обладнання, об'єкт працює в автоматичному режимі. Протягом року така ГЕС виробляє 1,2–1,3 млн кВт·год електричної енергії	Місцеві органи самоврядування, компанія – розробник проекту, установи-споживачі тепла та електроенергії	с. Уладівка, Вінницька область

Джерело: розроблено автором.

²⁴⁸ Міні-ГЕС у с. Уладівка на Вінниччині встановленою потужністю 0,18 МВт. URL: <http://ukrteplo.ua/napryamki-diyalnosti/elektrogeneratsiya/>

Додаток 8. Огляд заходів реагування на порушення функції електропостачання через руйнування РФ енергетичної інфраструктури України в осінньо-зимові періоди 2022–2024 рр.

Типи заходів	Приклади заходів реагування	Короткий опис	Суб'єкт реалізації
Планування готовності у штатному режимі функціонування			
Ідентифікація ризиків	Аналіз загроз та вразливостей	Здійснення перевірки стану енергетичної інфраструктури, систем життєзабезпечення, будівель у рамках підготовки до зимового періоду. Ідентифікація природних і техногенних загроз, загроз зловмисного характеру. У 2023 р. запроваджено щорічне оцінювання ризиків функціонування критичної інфраструктури	Центральні органи виконавчої влади (ЦОВВ), органи місцевої влади, Оператори КІ
Планування процедур	Планування сталості функціонування КІ	Щорічно здійснюється підготовка до проходження зимового періоду, яка стратегічно містить чотири ключові аспекти: запаси газу; запаси вугілля; технічна готовність енергетичної інфраструктури; підготовка до реагування на екстрені ситуації. Уряд щорічно, з урахуванням ситуації, затверджував план підготовки об'єктів житлово-комунального господарства та паливно-енергетичного комплексу до осінньо-зимового періоду та створював координаційний штаб (Антикризовий енергетичний штаб) його з реалізації цього плану. Встановлювався алгоритм взаємодії Операторів КІ, міністерств, Агентства з відновлення та обласних військових адміністрацій	Оператор системи передачі – НЕК «Укренерго» та Оператор ГТС України (ОСП), оператори системи розподілу – місцеві розподільчі мережі (ОСР), органи місцевої влади, Оператори КІ, компанії-виробники, постачальники обладнання
	Розроблення графіків відключення споживачів	Графіки відключення споживачів є стандартним інструментом для забезпечення безпеки роботи енергосистеми, який заздалегідь розробляється за участю ОСР, ОСП та представників місцевої влади. Графіки аварійних відключень вводяться, щоб запобігти автоматичному та неконтрольованому відключенню всіх споживачів на визначеній території	ОСР, ОСП, органи місцевої влади, Оператори КІ
	Накопичення запасів	ОСП, ОСР, компанії виробники та органи влади формували	ОСП, ОСР, органи місцевої

Типи заходів	Приклади заходів реагування	Короткий опис	Суб'єкт реалізації
	резервного обладнання та матеріалів	мінімальні запаси необхідного резервного генеруючого обладнання на випадок повної відсутності газу, електроенергії та централізованого опалення	влади, Оператори КІ, компанії-виробники, обслуговуючі компанії, постачальники обладнання
Удосконалення процедур	Підготовка до реагування на кризову ситуацію	Запроваджено вимогу щодо підготовки органами влади (на різному рівні) та енергетичними компаніями планів забезпечення стійкості функціонування енергетики у надзвичайній ситуації. Урядом було доведено плани реагування на випадок критичних ситуацій	ОСП, ОСР, центральні органи виконавчої влади, органи місцевої влади, оператори КІ
	Уточнення законодавства	Кабінет Міністрів України встановлює правила здійснення експортних та імпорتنних операцій. Зокрема, окремими рішеннями було заборонено експортувати вугілля та паливну деревну	ЦОВВ, органи місцевої влади, Оператори КІ, компанії-постачальники
Готовність та запобігання			
Готовність захисту	Фізичний захист об'єктів КІ	Компанії енергетичної сфери спільно з військовими та правоохоронними організаціями забезпечували захист об'єктів енергетики від фізичних загроз (повітряні атаки та диверсії), щоб не допустити їх руйнування. Здійснювалися заходи з посилення охорони об'єктів, встановлення захисних огорожувальних конструкцій	ОСП, ОСР, ЦОВВ, Сили безпеки і оборони, компанії-виробники
	Захист об'єктів КІ від атак з повітря	Було розгорнуто системи протиповітряної та протиракетної оборони. На об'єктах енергетики побудовано фізичні захисні споруди від прямих ударів з повітря та опосередкованого враження вибуховими хвилями та осколками	ОСП, ОСР, ЦОВВ, Сили безпеки і оборони, компанії-виробники
	Кіберзахист	Енергетичні компанії щільно співпрацювали з органами державної влади та міжнародними партнерами у сфері кіберзахисту, посилюючи ІТ-безпеку країни. Така співпраця дозволила запобігти тисячам кібератак у сфері енергетики	ОСП, ОСР, ЦОВВ, Сили безпеки і оборони, компанії-виробники
	Захист персоналу	Компанії намагалися мінімізувати присутність персоналу на об'єктах енергетики. Управління здійснювалось із віддалених місць. Лише	ОСП, ОСР, ЦОВВ, Оператори КІ,

Типи заходів	Приклади заходів реагування	Короткий опис	Суб'єкт реалізації
		оперативно-технічний персонал залишався на місцях. Було забезпечено місця укриття на випадок обстрілів	компанії-виробники
Готовність (планів, процедур, інституцій)	Підготовка до реагування на кризову ситуацію	Проводилися тренування з реалізації таких планів. Оцінювалася доцільність примусової евакуації мешканців окремих районів (передусім тих, хто живе поряд із об'єктами КІ)	ОСП, ОСР, ЦОВВ органи місцевої влади, оператори КІ
	Координація зусиль	Уряд створив Штаб із підготовки до опалювального періоду 2022/23 років під час воєнного стану. Розроблялися варіанти роботи ОЕС України у разі припинення генерації на окремих станціях, руйнування підстанцій чи ліній електропередачі. При Міненерго діяв Штаб з ліквідації наслідків воєнної надзвичайної ситуації державного рівня в електроенергетичних системах	ОСП, ОСР, ЦОВВ, органи місцевої влади, Оператори КІ, компанії-виробники, постачальники обладнання
	Накопичення матеріалів та обладнання для ремонту	На доповнення до щорічної практики накопичення запасів та резервів для проходження зимового періоду, у 2022 р. додатково було зроблено резервний запас обладнання на випадок пошкодження інфраструктури. Підготовка здійснювалась на загальнодержавному та місцевому рівнях	ОСП, ОСР, ЦОВВ, органи місцевої влади, оператори КІ, компанії-виробники, постачальники обладнання
	Адаптація законодавства до умов кризової ситуації	Уряд звільнив від сплати ввізного мита та ПДВ імпорт обладнання, яке допомагало енергозабезпеченню споживачів в умовах кризи. Спрощено порядок дій ОСР з відновлення електропостачання населених пунктів, знеструмлених унаслідок бойових дій, затверджено Порядок тимчасового приєднання електроустановок до системи розподілу в період дії в Україні воєнного стану. Було визначено завдання формувати плани відновлення з метою безпечного виконання робіт та забезпечення електропостачання споживачів, які критично впливають на забезпечення життєдіяльності регіону	ОСП, ОСР, ЦОВВ, органи місцевої влади, Оператори КІ, компанії-виробники, споживачі

Типи заходів	Приклади заходів реагування	Короткий опис	Суб'єкт реалізації
	Підготовка системи управління технологічним процесом	Найбільшими енергетичними компаніями було підготовлено запасні центри корпоративного і технологічного управління, складено плани переведення операційної діяльності на такі майданчики. Були підготовлені й реалізовані плани евакуації персоналу з небезпечних об'єктів і територій	ОСП, ОСР, компанії-виробники
Пом'якшення наслідків	Альтернативні та децентралізовані джерела живлення	Уряд країни підтримував встановлення альтернативної мобільної генерації з метою пом'якшення впливу загроз. Суб'єкти господарювання почали використовувати резервні стаціонарні й пересувні генератори та накопичувачі енергії для підтримки роботи технологічних процесів (у випадках зникнення електроенергії). Накопичення резервних джерел енергії здійснювали також компанії-споживачі, зокрема компанії, що є Операторами КІ, котрі забезпечують надання основних послуг (зв'язок, водопостачання, транспорт тощо)	ОСП, ОСР, компанії-виробники, компанії-споживачі, компанії-постачальники, населення
	Зменшення рівня енергоспоживання	Реалізовувалися заходи, спрямовані на зменшення споживання енергоресурсів в Україні. На місцевому рівні це стосувалося заходів: переведення теплогенеруючих підприємств на альтернативні види енергії, термомодернізації (житла), скорочення потреб енергоспоживання у бюджетній сфері	ЦОВВ, органи місцевої влади, Оператори КІ, споживачі
	Упереджувальне відключення	Якщо надходило попередження про ракетну атаку, ОСП та ОСР застосовували превентивні відключення споживачів та окремих вузлів мереж для мінімізації ризиків порушення обладнання мереж унаслідок раптових змін режимів роботи через атаки (перевантаження)	ОСП, ОСР, компанії-виробники
Реагування			
Аварійне реагування	Застосування графіків відключення споживачів	Через значні пошкодження енергетичної інфраструктури (генеруючі потужності та мережевої інфраструктури) в Україні в окремі періоди застосовували не лише планові, а й аварійні відключення електроенергії	ОСП, ОСР, органи місцевої влади, Оператори КІ, компанії-виробники

Типи заходів	Приклади заходів реагування	Короткий опис	Суб'єкт реалізації
	Аварійний ремонт	Фактично у безперервному режимі здійснювалися роботи з ремонту пошкодженої інфраструктури. До участі у відновленні долучались місцеві екстрені служби. Підтримка та постачання обладнання від закордонних колег дозволила нам швидко відновлювати живлення та стабілізувати ситуацію в енергосистемі.	ОСП, ОСР, ЦОВВ, органи місцевої влади, Оператори КІ, компанії-виробники, компанії-постачальники
	Взаємодія та координація	На доповнення до координаційної структури на загальнодержавному рівні створювалися також місцеві штаби антикризового реагування	ОСП, ОСР, ЦОВВ, органи місцевої влади, Оператори КІ, компанії-постачальники
	Застосування обмежень на роботу потужних споживачів електроенергії	Здійснювалося обмеження електропостачання промисловим клієнтам. Окремі суб'єкти господарювання (виробничі підприємства) скоротили обсяги виробництва або взагалі його зупинили. Було обмежено зовнішнє освітлення населених пунктів, освітлення офісів, ресторанів, торгових центрів. Для скорочення споживання електроенергії зупинялася робота електротранспорту, частково електротранспорт був замінений автотранспортом	ОСР, органи місцевої влади, Оператори КІ, компанії-виробники, компанії-споживачі
	Застосування процедур відновлення роботи енергосистеми після системної аварії	ОСП застосовував заздалегідь розроблений протокол щодо повернення синхронної роботи всієї енергосистеми після системної аварії. Передусім заживлювались об'єкти КІ: водоканали, теплокомуненерго, системи водовідведення тощо. Поступово до синхронної роботи поверталися насамперед гідро- та теплоелектростанції, згодом – атомна генерація	ОСП, ОСР, органи місцевої влади, Оператори КІ, компанії-виробники
Стабілізація ситуації	Застосування тимчасових схем живлення	В окремих випадках, коли масштаби руйнувань були значні, електропостачання споживачів відновлювалося завдяки оперативному налагодженню резервних схем постачання	ОСП, ОСР, Оператори КІ
	Збільшення кількості ремонтних бригад	Руйнування енергетичної КІ потребувало формування необхідної кількості ремонтних бригад. З початком інтенсивних бойових дій НЕК «Укренерго» та Оператор ГТС України збільшили до 40 од. кількість ремонтних бригад. Подібна тенденція спостерігалась і на	ОСП, ОСР, ЦОВВ, органи місцевої влади, Оператори КІ, компанії-виробники

Типи заходів	Приклади заходів реагування	Короткий опис	Суб'єкт реалізації
		рівні місцевих розподільчих мереж електроенергії та газу (ОСР), особливо в регіонах, де відбувались інтенсивні бої. В Україні цілодобово працювали понад 70 ремонтних бригад. В окремих прифронтових регіонах ОСР мали до 50 ремонтних бригад для оперативного реагування	
	Застосування стабілізаційних графіків відключення споживачів	Застосування стабілізаційних графіків відключення споживачів здійснювалось ОСП та ОСР для забезпечення балансу пропозиції та попиту. Обмеження споживачів необхідні, щоб зменшити навантаження на мережі, забезпечити стає балансуювання енергосистеми та уникнути повторних аварій	ОСП, ОСР, ЦОВВ, органи місцевої влади, Оператори КІ, населення, компанії-виробники, компанії-споживачі
	Зміщення графіка енергоспоживання	Понад 60 % виробничих компаній вимушено змінили графік роботи для зміщення максимального рівня навантаження, 40 % скорочували виробничу діяльність, а 10 % частково або повністю зупинили роботу	ОСР, органи місцевої влади, Оператори КІ, компанії-виробники, компанії-споживачі
	Застосування резервних джерела енергії	Побутові споживачі та бізнес почали адаптуватись до нових умов, забезпечуючи себе альтернативними джерелами живлення. На початок січня 2023 р. 50 % магазинів продуктових мереж були забезпечені генераторами	ОСР, органи місцевої влади, Оператори КІ, постачальники обладнання, галузеві асоціації, населення
	Застосування мобільних джерел генерування енергії	Було реалізовано низку проєктів із встановлення мобільних установок генерування електроенергії (газотурбінні та газопоршневі електростанції 1–50 МВт) і тепла (мобільні котельні)	ОСР, органи місцевої влади, Оператори КІ, постачальники обладнання, компанії-споживачі
	Застосування альтернативних та відновлюваних джерел енергії	Через сприятливі погодні умови та поступове зростання світлового дня збільшилася тривалість роботи електростанцій з ВДЕ, потужності яких працюють переважно у денні години	ОСП, ОСР, компанії-виробники, постачальники обладнання
	Добровільне	Уряд звернувся до всіх громадян з проханням обмежити споживання	ОСР, органи місцевої влади,

Типи заходів	Приклади заходів реагування	Короткий опис	Суб'єкт реалізації
	скорочення рівня енергоспоживання населенням	електроенергії, особливо у вечірні години, на ці кілька днів, поки тривають відновлення й ремонтні роботи. Домогосподарства відреагували на звернення. Наприклад, у понеділок 10 жовтня 2022 р. мешканці Києва та Київської області у вечірні години зменшили споживання електроенергії на 26,5 % порівняно із звичайним осіннім днем	Оператори КІ, населення
	Ремонт обладнання	Унаслідок руйнування енергетичної інфраструктури було пошкоджено більше як 50 % енергетичної інфраструктури. У середньому протягом двох діб після кожного обстрілу відновлювали спроможність системи забезпечувати споживачів на допустимому рівні. У деяких випадках термін ремонтів збільшувався через масштабність руйнувань	ОСП, ОСР, ЦОВВ, органи місцевої влади, компанії-виробники, компанії-споживачі, постачальники обладнання, міжнародні інституції
	Зміна конфігурації мереж	В окремих випадках для відновлення енергозабезпечення змінювалася конфігурація мереж та склад обладнання	ОСП, ОСР, компанії-виробники, компанії-споживачі
	Залучення зовнішніх ресурсів (імпорт електроенергії)	Для покриття дефіциту електроенергії здійснювався імпорт електроенергії з країн ENTSO-E в Україну. У грудні 2022 р. Україна потребувала імпорту електроенергії з Європи до 2 ГВт. У 2023 р. було введено в експлуатацію додаткову лінію, яка з'єднала Україну з мережами країн ЄС напругою 400 КВт. Наприкінці 2023 р. технічна можливість імпорту електроенергії з країн ЄС в Україну становила 1,7 ГВт	ОСП, ОСР, ЦОВВ, компанії-постачальники, споживачі
	Розвиток співпраці з міжнародними партнерами	Створено Фонд енергетичної підтримки України, який об'єднав зусилля різних країн, компаній та інституцій у допомозі Україні з ремонту та відновленні функціональності пошкодженої енергетичної інфраструктури. Від міжнародних партнерів було отримано понад 825 вантажів гуманітарної допомоги з енергетичним обладнанням. Усього допомогу Україні надали країн світу з різних континентів	ОСП, ОСР, ЦОВВ, Оператори КІ; компанії-виробники

Типи заходів	Приклади заходів реагування	Короткий опис	Суб'єкт реалізації
Відновлення			
Розвиток спроможностей	Створення джерел фінансування ліквідації наслідків та відшкодування збитків	Прийнято Закон України про створення Фонду ліквідації наслідків збройної агресії. Зокрема, кошти з Фонду буде спрямовано на будівництво громадських будівель, реконструкцію, капітальний ремонт об'єктів критичної інфраструктури	ЦОВВ, органи місцевої влади
	Управління режимами енергоспоживання	Використання потенціалу енергозбереження з боку споживача (суб'єкти господарювання та домогосподарства) дозволить реалізувати механізм управління енерговикористанням та регулювати рівні енергоспоживання	Органи місцевої влади, компанії-виробники, компанії-споживачі, постачальники обладнання
	Створення запасів енергоресурсів та матеріалів на довгострокову перспективу	Уряд затвердив перелік підземних споруд, де будуть зберігатися акумульовані нафта, газ, інші речовини та матеріали. Створення надійних сховищ реалізує довгострокову стратегію забезпечення стійкості функціонування енергетичного сектору в умовах розширення спектра загроз фізичного характеру	ЦОВВ, органи місцевої влади, компанії-виробники
	Розширення можливостей для імпорту електроенергії	Підготовка технічних можливостей для імпорту електроенергії (до кінця 2023 р. потужність імпорту збільшено до 1,7 ГВт), а також затвердження необхідної законодавчої бази для полегшення імпорту. У 2023 р. прийнято низку рішень, які створили економічні й регуляторні умови забезпечення стабільного імпорту електроенергії	Енергетичний регулятор, ОСП, ОСР, ЦОВВ, компанії-постачальники, споживачі
	Спрощення процедур увезення в Україну критичного обладнання	Уряд спростив завезення в Україну енергетичного обладнання, зокрема генераторів і трансформаторів. Фактично було призупинено дію шести технічних регламентів, які застосовувалися при ввезенні та продажу енергетичного обладнання	ОСП, ОСР, ЦОВВ, компанії-постачальники, споживачі
	Удосконалено законодавчі та організаційні	На національному рівні в 2023 р. утворено Координаційний штаб із оперативного реагування та забезпечення створення нормальних умов життєдіяльності населення під час обмеження та/або	ЦОВВ, органи місцевої влади, компанії-виробники, компанії-споживачі

Типи заходів	Приклади заходів реагування	Короткий опис	Суб'єкт реалізації
	засади реагування на кризові ситуації	припинення постачання електричної енергії. На місцевому рівні у тому ж році започатковано розроблення й затвердження місцевих програм забезпечення безпеки та стійкості критичної інфраструктури, програм підвищення стійкості територіальних громад до кризових ситуацій, спричинених припиненням або погіршенням надання важливих для їхньої життєдіяльності послуг чи для здійснення життєво важливих функцій	
	Удосконалення навичок персоналу	У межах відповідальності окремих місцевих органів влади було проведено перевірку готовності резервного обладнання для забезпечення енергією об'єктів критичної інфраструктури та організовано тренування з оперативного розгортання резервного обладнання. У межах повноважень, за результатами вивчення досвіду реагування, проводилися командно-штабні навчання з питань безпеки та стійкості критичної інфраструктури	ЦОВВ, органи місцевої влади, компанії-виробники, компанії-споживачі
Розвиток КІ	Проведення ремонтних робіт	У період з лютого 2022 до березня 2023 рр. було виведено з ладу понад 50 % енергетичної інфраструктури України. На початок опалювального сезону 2023/2024 років сумарно було відновлено майже 2 ГВт генеруючих потужностей, а функціональність енергетичної системи вдалося відновити до рівня понад 80 % довоєнного рівня. Значна увага була приділена переконфігурації мереж та розбудові розподіленої генерації	ОСП, ОСР, ЦОВВ, органи місцевої влади; компанії-виробники, компанії-споживачі, постачальники обладнання, міжнародні інституції
	Зміна структури генерації та мереж	Одним із ключових пріоритетних завдань з відновлення енергетики країни є розосередження генерації, яка буде встановлена в різних регіонах. Сприятиме цьому розвиток ВДЕ, генеруючих потужностей малої потужності. Доповнюватиме усе це розвиток «розумних» мереж (Smart Grid), які завдяки сучасним технологіям управління режимами роботи мереж та енерговикористання з боку споживача дозволять оптимізувати обсяги споживання енергії	ОСП, ОСР, ЦОВВ, органи місцевої влади, компанії-виробники, компанії-споживачі, постачальники обладнання, міжнародні інституції
	Розвиток систем	Запропоновано, щоб забезпечення генеруючих установок	ОСР, органи місцевої влади,

Типи заходів	Приклади заходів реагування	Короткий опис	Суб'єкт реалізації
	резервного живлення	енергоресурсами здійснювалося з урахуванням диверсифікації видів палива. Якщо раніше резервні паливні господарства базувалися на мазуті та вугіллі, то сьогодні вони можуть працювати на циклічно відновлюваних ресурсах, на відходах сільського господарства, біогазі. Прийнято рішення щодо розбудови спроможності громад, зокрема про те, що їхня критична інфраструктура має бути заживлена автономно. У разі критичних ситуацій в енергосистемі мають працювати водоканали, теплокомуненерго, лікарні та інші підприємства, які забезпечують життєдіяльність населених пунктів. Залежно від потреб місцева влада, державні або приватні компанії можуть закупити станції різної потужності: від 1 МВт до 150 МВт. При цьому визначено пріоритет щодо переведення генеруючих об'єктів на альтернативні низьковуглецеві джерела енергії	компанії-виробники, компанії-споживачі, постачальники обладнання
	Уточнення процедур реагування Операторів КІ	З урахуванням отриманого досвіду зими 2022/2023 рр. оновлено протоколи реагування ОСП та ОСР із місцевими органами влади на випадок надзвичайних подій: яким чином перезаживлювати споживачів, у якій послідовності, як реагувати на екстрені ситуації, можливі нестандартні інженерні рішення, резервні схеми живлення тощо. Уточнено графіки аварійних відключень у співпраці з місцевими органами влади, операторами системи передачі та розподілу	ОСП, ОСР, органи місцевої влади

Джерело: розроблено автором на основі²⁴⁹.

²⁴⁹ Суходоля О. М. Стійкість критичної інфраструктури та життєво важливих функцій і послуг: формалізація завдань та змісту дій суб'єктів забезпечення. *Стратегічна панорама*. 2023. № 2.

Наукове видання

Олександр Михайлович СУХОДОЛЯ

**СТІЙКІСТЬ
КРИТИЧНОЇ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ
ТА ЖИТТЄДІЯЛЬНОСТІ ГРОМАД**

Аналітична доповідь

Відповідальна за випуск *Т. Джига*

Редактор *Т. Карбовнича*

Коректор *Т. Карбовнича*

Видання підготовлено
в Національному інституті стратегічних досліджень
вул. Пирогова, 7-а, м. Київ, 01030
Тел./факс: (044) 234-50-07
e-mail: info-niss@niss.gov.ua
<http://niss.gov.ua>