НАЦІОНАЛЬНИЙ ІНСТИТУТ СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ

ОРГАНІЗАЦІЙНІ ТА ПРАВОВІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ І СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

АНАЛІТИЧНА ДОПОВІДЬ

Київ 2019

УДК 351.862.4:340.13+338.583(477)
О64

За повного або часткового використання матеріалів цієї публікації посилання на видання обов'язкове
Електронна версія: http://www.niss.gov.ua

Автори:

Бобро Д. Г. – підрозділи 3.1, 3.3 – 3.5, 3.7; додатки 1.4 – 1.6, 3, 4;
Іванюта С. П. – підрозділи 3.3, 3,6; додатки 1.5, 4;
Кондратов С. І. – підрозділи 2.1, 2.3 – 2.5; додатки 3, 4;
Суходоля О. М. – підрозділи 1.1, 1.2, 2.2, 3.1 – 3.3, 3,7; додатки 1.1 – 1.6, 2, 3, 4.

За загальною редакцією
доктора наук з державного управління, професора *О. М. Суходолі*

О64 **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. – К. : НІСД, 2019. – 224 с.

ISBN 978-966-554-258-2

У виданні висвітлено теоретичні та нормативно-правові засади створення системи безпеки і стійкості критичної інфраструктури в Україні, запропоновано методологічні засади виокремлення критичної інфраструктури та формалізації діяльності залучених суб'єктів з питань захисту критичної інфраструктури.

Проаналізовано передовий зарубіжний досвід у галузі захисту критичної інфраструктури, ситуацію із запровадженням концепції захисту критичної інфраструктури в Україні, окреслено можливі напрями та інструменти щодо здійснення державної політики у цій сфері, сформульовано низку конкретних рекомендацій і пропозицій.

Розраховано на представників органів державної влади всіх рівнів, працівників правоохоронних органів та спецслужб, представників вітчизняного бізнесу, неурядових організацій, науковців, експертів, а також на широке коло читачів, які цікавляться питаннями національної безпеки, захисту та стійкості критичної інфраструктури.

УДК 351.862.4:340.13+338.583(477)

ISBN 978-966-554-258-2

© Національний інститут стратегічних досліджень, 2019

ЗМІСТ

Передмова 7

Розділ 1. **Система безпеки та стійкості критичної інфраструктури – невід'ємний елемент системи національної безпеки** 11

1.1. Термінологічні особливості формування системи забезпечення безпеки та стійкості критичної інфраструктури 13

1.2. Забезпечення безпеки та стійкості критичної інфраструктури у системі забезпечення національної стійкості 19

Розділ 2. **Світовий досвід створення національних систем забезпечення безпеки та стійкості критичної інфраструктури** 31

2.1. Передовий зарубіжний досвід створення національних/ державних систем забезпечення безпеки та стійкості критичної нфраструктури 31

2.1.1. Система забезпечення безпеки та стійкості критичної інфраструктури в США 33

2.1.2. Система забезпечення безпеки та стійкості критичної інфраструктури у Великій Британії 42

2.1.3. Система забезпечення безпеки та стійкості критичної інфраструктури у Польщі 50

2.1.4. Висновки для України з огляду на зарубіжний досвід щодо державної системи забезпечення безпеки та стійкості критичної інфраструктури 54

2.2. Розвиток законодавства ЄС у сфері безпеки енергопостачання 56

2.3. Планування у забезпеченні безпеки критичної інфраструктури 61
2.3.1. Планування реагування на загрози критичної інфраструктури за умови забезпечення її безпеки та стійкості в США 63
2.3.2. Планування дій у кризових ситуаціях в Україні з точки зору забезпечення безпеки та стійкості критичної інфраструктури 67
2.4. Взаємодія та обмін інформацією 70
2.4.1. Структура системи взаємодії та обміну інформацією 70
2.4.2. Основні підходи до формування архітектури національної мережі ситуаційно-кризових та інформаційно-аналітичних центрів 71
2.5. Огляд форм і форматів навчальних курсів 78
2.5.1. Організація підготовки кадрів і населення на державному рівні та в межах секторів критичної інфраструктури 79
2.5.2. Основні форми та інструменти підготовки кадрів і населення у рамках сектору критичної інфраструктури на прикладі США 83

Розділ 3. **Методологічні та організаційні засади забезпечення діяльності системи забезпечення безпеки та стійкості критичної інфраструктури** 87

3.1. Модель організації взаємодії залучених суб'єктів у рамках державної системи забезпечення безпеки та стійкості критичної інфраструктури 87
3.2. Ситуаційно-кризові центри в системі забезпечення безпеки та стійкості критичної інфраструктури 110
3.3. Ризик-аналіз у системі забезпечення безпеки та стійкості критичної інфраструктури 115
3.4. Методологія віднесення інфраструктурних об'єктів і систем до критичної інфраструктури 125
3.5. Проектна загроза у системі забезпечення безпеки та стійкості критичної інфраструктури 135
3.5.1. Модель порушника та модель загрози протиправних дій . . . 136

3.5.2. Модель загроз та проектна загроза критичній інфраструктурі 140
3.6. Паспорти безпеки об'єктів критичної інфраструктури 145
3.6.1. Нормативно-правові засади формування вимог до захисту об'єктів критичної інфраструктури 145
3.6.2. Основні вимоги до розробки паспортів безпеки об'єктів критичної інфраструктури 148
3.7. Проведення навчань і тренувань 152

Післямова 164

Додатки 167

Додаток 1. Інструменти формалізації діяльності у сфері захисту критичної інфраструктури 167
1.1. План захисту критичної інфраструктури 167
1.2. План реагування на випадок кризової ситуації 169
1.3. Проведення ризик-аналізу 172
1.4. Перелік секторів критичної інфраструктури 174
1.5. Паспорт безпеки об'єкта/системи критичної інфраструктури . . 177
1.6. Проектна загроза критичній інфраструктури 181
Додаток 2. Пропозиції до Національного плану захисту критичної інфраструктури 185
Додаток 3. Пропозиції до проекту Закону України «Про критичну інфраструктуру» 200
Додаток 4. Глосарій 220

Відомості про авторів 223

СПИСОК СКОРОЧЕНЬ

БСКІ	безпека та стійкість критичної інфраструктури
ВОІ	взаємодія та обмін інформацією
ГСЦУ	Головний ситуаційний центр України
ДПП	державно-приватне партнерство
ДСНС України	Державна служба України з надзвичайних ситуацій
ДСФЗ	Державна система фізичного захисту
ЄДСЦЗ	Єдина державна система цивільного захисту
ЄС	Європейський Союз
ЄСЗРПТА	Єдина система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків
ЗКІ	захист критичної інфраструктури
КІ	критична інфраструктура
КМУ	Кабінет Міністрів України
МВБ	Міністерство внутрішньої безпеки США (U. S. Department of Homeland Security, DHS)
МВС України	Міністерство внутрішніх справ України
НМ СКЦ	національна мережа ситуаційно-кризових та інформаційно-аналітичних центрів
НСК	Національна система кібербезпеки
ОКІ	об'єкт критичної інфраструктури
РНБОУ	Рада національної безпеки і оборони України
СБУ	Служба безпеки України
СКЦ	ситуаційно-кризовий центр
ССКЦ	секторальний ситуаційно-кризовий центр
УЦБС	Урядовий центр безпеки і стійкості

ПЕРЕДМОВА

Сьогодні термін «критична інфраструктура» (КІ) усе частіше використовується в різних сферах життєдіяльності суспільства. Ним послуговуються експерти, науковці у своїх публікаціях і коментарях, під час наукових конференцій, семінарів, міжнародних форумів, присвячених питанням розвитку та захисту критичної інфраструктури, цей термін вживають журналісти в засобах масової інформації (ЗМІ).

У багатьох країнах світу цей безпековий напрям визнано пріоритетним у політиці національної безпеки. Відтак у цих країнах активно розбудовуються національні системи із забезпечення захисту (безпеки) та стійкості критичної інфраструктури, ухвалюються законодавчі документи для регламентації діяльності учасників системи, готуються відповідні кадри, налагоджуються партнерські відносини з приватним сектором, здійснюються освітні заходи серед населення тощо.

Звичайно, під впливом низки специфічних для кожної країни чинників національні підходи до створення систем захисту критичної інфраструктури (ЗКІ) можуть відрізнятися за організаційними та правовими засадами, до того ж ці системи можуть перебувати на різних стадіях свого розвитку. Все це зумовило появу низки варіантів створення систем ЗКІ, високу динамічність змін, які спостерігаються на цьому напрямі, у т. ч. в термінологічному забезпеченні цього процесу.

З огляду на це в різних країнах (і навіть в одній, але в різні періоди часу) в офіційних документах можна натрапити на терміни «*критична інфраструктура*», «*національна критична інфраструктура*», «*національна інфраструктура*». Хоча, як правило, йдеться про одне й те саме поняття і маються на увазі аналогічні цілі та завдання

щодо критичної інфраструктури. Але в національному законодавстві одних країн вживається термін «захист критичної інфраструктури», а в інших – питання розглядається в широкому контексті, бо мається на увазі безпека та стійкість критичної інфраструктури, що й позначається відповідним терміном. Ураховуючи це, читачі не повинні дивуватися, коли, наприклад, у національному законодавстві США побачать комбінацію з майже всіх згаданих термінів у назві одного офіційного документа, а саме: чинного Плану захисту національної інфраструктури 2013 «Партнерство заради безпеки та стійкості критичної інфраструктури».

Беручи до уваги викладене вище, у пропонованому виданні висвітлено швидкі зміни, які відбуваються в цьому безпековому напрямі у світі, зокрема й у термінологічному плані, що накладають свій відбиток на процес формування підходів до запровадження концепції захисту критичної інфраструктури в Україні.

Незважаючи на наявність деяких відмінностей у національних системах захисту критичної інфраструктури в розвинутих країнах (для нас найбільший інтерес становлять ті, що входять до НАТО та ЄС), існують загальновизнані цими країнами підходи до побудови систем ЗКІ, які спираються на спільне розуміння базових для цієї сфери термінів і понять.

До таких підходів варто віднести насамперед те, що КІ необхідно системно захищати від усіх видів фізичних загроз і небезпек (природного і техногенного походження, зловмисних дій) та кіберзагроз, виходячи з результатів оцінки ризиків, розвиваючи державно-приватне партнерство та залучаючи до відповідних зусиль і заходів усе суспільство: від окремих сімей та місцевих громад і до вищого політичного керівництва держави. Натомість до числа базових для цієї сфери термінів і понять, без сумніву, слід віднести такі: «критична інфраструктура», «загрози для критичної інфраструктури», «безпека і стійкість критичної інфраструктури».

На основі викладеного вище можна сформулювати деякі фундаментальні умови (висновки) щодо побудови систем захисту критичної інфраструктури, забезпечення її безпеки та стійкості, а саме:

- системність підходів досягається створенням відповідної системи забезпечення безпеки та стійкості критичної інфраструктури (БСКІ);

- масштабність завдань щодо БСКІ зумовлює залучення численних акторів, ефективна діяльність яких неможлива без забезпечення якісно нового рівня координації дій, взаємодії та обміну інформацією між ними;
- розподіл функцій, повноважень та сфер відповідальності між суб'єктами діяльності для забезпечення належного рівня координації дій, взаємодії та обміну інформацією (ВОІ) у цій сфері, а також призначення (створення) на національному рівні органу (органів) для координації дій, сприяння ВОІ суб'єктів відповідної діяльності;
- розвиток партнерських відносин з іншими акторами, включно й із приватними компаніями, планування взаємодії з ними в кризових ситуаціях; здійснення регулярних перевірок відповідних планів і процедур під час навчань, тренувань і в реальному житті;
- підготовка управлінців нового типу, здатних забезпечувати якісно новий рівень управління. З цією метою має бути створена національна система підготовки кадрів для КІ. Іншим наслідком такої вимоги є необхідність у створенні на основі національної мережі інформаційно-аналітичних і ситуаційно-кризових центрів (СКЦ) системи підтримки рішень (у т. ч. політичних) щодо безпеки критичної інфраструктури.

Усі пов'язані з цими завданнями проблеми та виклики певною мірою знайшли своє відображення в цій аналітичній доповіді.

Так, *перший розділ «Система безпеки та стійкості критичної інфраструктури – невід'ємний елемент системи національної безпеки»* присвячений взаємозв'язку та взаємозалежності завдань і цілей забезпечення захисту БСКІ із національною безпекою та національною стійкістю.

У *другому розділі «Світовий досвід створення національних систем безпеки та стійкості критичної інфраструктури»* зроблено огляд зарубіжного досвіду в сфері забезпечення БСКІ у низці країн НАТО та ЄС з точки зору можливості його використання в Україні, опрацьовуються питання налагодження ефективної системи взаємодії та обміну інформацією між залученими суб'єктами, вивчається кращий досвід з організації системи навчання, підготовки та перепідготовки кадрів у цій сфері.

До *третього розділу «Методологічні та організаційні засади забезпечення діяльності системи безпеки та стійкості критичної інфраструктури»* увійшли матеріали, які мають на меті сформувати методологічні та організаційні засади забезпечення безпеки та стійкості критичної інфраструктури в Україні. Зокрема, розглядаються напрями розбудови державної системи забезпечення БСКІ; досліджуються етапи реагування на розвиток кризових ситуацій, визначаються та формалізуються вимоги до діяльності суб'єктів БСКІ на цих етапах; досліджуються та пропонуються організаційні, регулятивні та правові інструменти формалізації діяльності в цій галузі; пропонуються рішення щодо відображення діяльності у сфері ЗКІ в системі забезпечення національної безпеки України, розробляються підходи щодо організації координації дій, взаємодії та обміну інформацією між чинними системами безпеки та кризового реагування в Україні тощо.

У *Додатках*, включених до цього видання, містяться інформаційні матеріали, які представляють собою деталізацію окремих аспектів проблем забезпечення БСКІ. Крім того, пропонуються типові рішення щодо формалізації окремих аспектів реагування на загрози на різних етапах діяльності системи захисту критичної інфраструктури, проекти законодавчих актів, зокрема Національного плану захисту критичної інфраструктури та Закону України «Про критичну інфраструктуру».

Р о з д і л 1

СИСТЕМА БЕЗПЕКИ ТА СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ – НЕВІД'ЄМНИЙ ЕЛЕМЕНТ СИСТЕМИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Національний інститут стратегічних досліджень (НІСД), тривалий час досліджуючи питання забезпечення національної безпеки, сформував цілу низку продуктивних ідей та концепцій щодо вдосконалення системи забезпечення національної безпеки.

Серед таких ідей є й питання забезпечення безпеки та стійкості критичної інфраструктури країни, і загалом національної стійкості, що розглядається крізь призму забезпечення національної безпеки. Зазначені питання останнім часом стали набувати все більшої актуальності не тільки для України, США або країн ЄС, але й загалом для людської цивілізації.

Передові країни, що забезпечують життєдіяльність суспільства, базуючись на принципах демократії та верховенства права, навіть стали визначати стійкість як пріоритетний напрям розвитку політики у сфері національної безпеки.

Зокрема, саме питанням забезпечення стійкості присвячені нові стратегічні документи ЄС, який затвердив *Глобальну стратегію ЄС із зовнішньої політики та політики безпеки* [1], та НАТО, коли глави держав і урядів країн – членів НАТО в липні 2016 р. затвердили завдання щодо забезпечення національної стійкості [2].

Цей напрям в Україні набув розвитку також і завдяки зусиллям науковців НІСД, які тривалий час здійснювали дослідження у сфері

[1] A Global Strategy for the European Union's Foreign And Security Policy. URL: https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

[2] Commitment to enhance resilience. URL: http://www.nato.int/cps/en/natohq/official_texts_133180.htm?selectedLocale=en

захисту критичної інфраструктури. Саме ці напрацювання лягли в основу схваленої Кабінетом Міністрів України (КМУ) наприкінці 2017 р. Концепції створення державної системи захисту критичної інфраструктури [3]. Ця Концепція базується на розробленій НІСД «Зеленій книзі з питань захисту критичної інфраструктури в Україні», де було запроваджено методологічний підхід щодо забезпечення БСКІ до загроз будь-якого типу та їх комбінацій як складової забезпечення національної стійкості [4].

Надалі запропоновані ідеї знайшли своє втілення у розробці теоретичних засад створення державної системи БСКІ, визначення її організаційно-інституційної основи, а також інструментів та механізмів державного управління у цій сфері.

Дослідження фахівців НІСД щодо створення державної системи БСКІ мають вагоме значення, оскільки формують наукові засади впровадження у систему державного управління нових підходів до управління та організації життєдіяльності суспільства [5]. Водночас для практичного впровадження теоретичних розробок необхідно провести окрему організаційно-діяльністну роботу щодо усвідомлення суспільством запропонованих підходів, формування консенсусу серед залучених суб'єктів та їхньої готовності до практичного використання отриманих знань.

Це завдання потребує деякого додаткового розкриття місця та ролі системи забезпечення БСКІ в системі забезпечення національної стійкості, а також співвідношення пропонованих рішень із чинними підходами, відображеними в законодавстві, передусім на концептуальному рівні.

---

[3] Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету Міністрів України від 06.12.2017 № 1009-р. // База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/go/1009-2017-%D1%80

[4] Зелена книга з питань захисту критичної інфраструктури в Україні: зб. матер. міжнар. експерт. нарад/упоряд. Д. С. Бірюков, С. І. Кондратов; за заг. ред. О. М. Суходолі. Київ: НІСД, 2016. 176 с. URL: http://www.niss.gov.ua/articles/2213/

[5] Kondratov, S., Bobro, D., & Horbulin, V., et al. (2017). *Developing the Critical Infrastructure Protection System* in *Ukraine.* (General editor O. Sukhodolia). Kyiv: NISS. 184 p. URL: http://en.niss.gov.ua/content/articles/files/niss_EnglCollection_druk-24cce.pdf

1.1. Термінологічні особливості формування системи забезпечення безпеки та стійкості критичної інфраструктури

Перш за все розкриємо підходи до розуміння співвідношення змісту понять «захист», «безпека», «стійкість», які використовуються науковцями та практиками у сфері національної безпеки та ЗКІ.

В українській і зарубіжній практиці використовується різна термінологічна база для опису діяльності у цій сфері. При цьому спостерігається не тільки змістовна неузгодженість, а й часто відсутність відповідників окремих термінів. Ураховуючи те, що «Зелена книга з питань захисту критичної інфраструктури України» розроблялася переважно з урахуванням досвіду США у цій сфері, продемонструємо проблематику змістовного наповнення термінів на прикладі термінології, що використовується у США.

Одразу варто вказати на гнучкість законодавства США щодо фіксації змісту термінів, на відміну від жорсткості законодавства України. Ідеться про те, що визначення термінів не завжди фіксуються законами США, а зміст діяльності державних органів врегульовується на рівні окремих органів влади, відповідальних за реалізацію тих чи тих напрямів у сфері національної безпеки, навіть у рамках політичних документів.

До прикладу, базовий закон США щодо формування системи забезпечення національної безпеки «National Security Act of 1947» [6] не дав визначення терміна «національна безпека». Проте він визначив пріоритетні напрями державної політики у цій сфері [7] та встановив інституційну основу й систему координації забезпечення національної безпеки, що в основному стосувалося зовнішнього виміру зусиль країни. Таким чином, визначені законом органи державної влади, що становили основу цієї інституційно-організаційної структури забезпечення національної безпеки, отримали конкретний рівень гнучкості при реалізації визначених законом завдань.

---

[6] National Security Act of 1947. URL: https://www.cia.gov/library/readingroom/docs/1947-07-26.pdf

[7] Ці напрями стосувалися: забезпечення системи координації визначених органів влади; забезпечення їх ресурсами та повноваженнями відповідно до завдань; запровадження демократичного контролю над ними; забезпечення стратегічного управління силами сектору оборони.

Пізніше, після терористичних атак 11 вересня 2001 р., зміст поняття «національна безпека» було доповнено виміром «внутрішня безпека». Зокрема, у законі США «Homeland Security Act of 2002» [8], де про це йдеться, запропоновано також відповідну інституційну основу щодо забезпечення внутрішньої безпеки США. Серед нових завдань системи забезпечення національної безпеки з'явилося завдання щодо ЗКІ. Поряд із тим, і в цьому законі відсутнє визначення терміна «безпека» (національна чи внутрішня).

Тлумачення змісту терміна «безпека» [9] дається в інших актах уряду США (або відповідальних за «безпеку» органів влади). Зокрема, у них ідеться про те, що безпека – це:

- координовані національні зусилля для запобігання реалізації терористичних атак у США, зниження вразливості країни до тероризму, мінімізація шкоди та відновлення від атак, що сталися (National Strategy for Homeland Security (2002, 2007)) [10];
- спільні зусилля, спрямовані на попередження та припинення атак шляхом виявлення та перешкоджання загрозам, унеможливлення дій зловмисників у межах країни, захист найважливішої інфраструктури країни та ключових ресурсів і забезпечення кіберпростору (National Security Strategy, 2010) [11];
- узгоджене національне зусилля, котре гарантує, що країна убезпечена від нещасних випадків, захищена від та стійка до терористичних актів та інших небезпек, а інтереси країни, прагнення та спосіб життя можуть процвітати (Quadrennial Homeland Security Review, 2010, 2014) [12].

При цьому відзначається деяка еволюція у розумінні терміна «безпека» (security) залежно від поточних загроз національним

[8] Homeland Security Act of 2002. URL: https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf

[9] Оскільки нас цікавить еволюція розуміння змісту «security», будемо використовувати документи, що описують завдання забезпечення «homeland security», тому що забезпечення «national security» доповнює внутрішній вимір («homeland security») діями країни на міжнародній арені.

[10] National Strategy for Homeland Security. (2002). URL: https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf

[11] National Security Strategy. (2010). URL: http://nssarchive.us/NSSR/2010.pdf

[12] Quadrennial Homeland Security Review. (2010). URL: https://www.dhs.gov/xlibrary/assets/qhsr_report.pdf ; Quadrennial Homeland Security Review. (2014). URL: https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf

інтересам. Зокрема, на зазначеному відрізку часу – від діяльності лише стосовно захисту (protection) від кінетичних атак терористів до багатоцільової діяльності, що передбачає захист від фізичних атак, забезпечення технологічної безпеки (safety) та стійкість (resilience) щодо всіх типів загроз (передусім фізичні загрози та кіберзагрози).

Фактично ця еволюція зумовлює й зміщення акцентів та змісту діяльності органів державної влади США у сфері забезпечення національної безпеки у новому напрямі, який одержав нове визначення – забезпечення стійкості (resilience).

Трактування терміна здійснює Міністерство внутрішньої безпеки США (МВБ; U.S. Department of Homeland Security, DHS) [13] який пропонує розуміти поняття «стійкість» як «*спроможність адаптуватися до змінних умов та протистояти загрозам порушень функціонування та швидко відновлюватися від порушень внаслідок криз*» [14].

Директива президента США 2013 року (PPD-21) [15], яка трактує поняття «стійкість» подібним чином, уже передбачає завдання щодо забезпечення безпеки та стійкості і дає такі визначення щодо завдань політики у сфері захисту критичної інфраструктури:

- *стійкість* КІ – «спроможність підготуватись та адаптуватися до змінних умов, а також протистояти загрозам порушень функціонування та швидко відновлюватися від порушень. Стійкість включає спроможність протистояти загрозам та відновлюватися від цілеспрямованих атак, аварій, природних загроз та інцидентів»;
- *забезпечення безпеки (безпека)* КІ – «зменшення ризику критичної інфраструктури від втручання, атак або ефектів, спричинених природними катастрофами або людською діяльністю, за рахунок реалізації заходів із фізичного захисту або кіберзахисту».

[13] Department of Homeland Security. URL: https://www.dhs.gov/

[14] Department of Homeland Security. Resilience. URL: https://www.dhs.gov/topic/resilience

[15] Presidential Policy Directive – Critical Infrastructure Security and Resilience. (2013). URL: https://www.dhs.gov/sites/default/files/publications/PPD-21-Critical-Infrastructure-and-Resilience-508.pdf

Як приклад подальшого роз'яснення змісту цих понять МВБ наводить такі заходи [16]:

- *безпека*: огорожа споруд; блокування вхідних дверей; використання антивірусного програмного забезпечення; блокування екранів комп'ютерих моніторів;
- *стійкість*: розробка плану безперервності бізнесу; встановлення генератора для резервного живлення; використання міцніших будівельних матеріалів.

Таким чином, очевидним є зміщення уваги зі змісту діяльності щодо безпеки на діяльність із недопущення пошкодження функціонування умовного об'єкта переважно внаслідок зловмисних дій (з поступовим розширенням також на загрози природного і техногенного характеру), з фокусуванням на створенні додаткового захисту від загроз. Термін же «стійкість» фокусується на діяльності зі створення можливостей для підготовки щодо запобігання та реагування на загрози, адаптації до нових умов функціонування та відновлення нормального режиму роботи (хоча це також включає питання, які охоплені поняттям «захист»).

При цьому, на думку експертів [17], стійкість у практиці США розглядається як цінність, якість та бажана характеристика суспільства й держави (системи) та як її засадничий елемент. Справді, аналіз застосування поняття «стійкість» свідчить про використання цього терміна для виокремлення двох інструментів формалізації діяльності системи забезпечення національної безпеки, а саме як:

- вимоги до діяльності, що має враховувати різні типи загроз та спроможність реагувати протягом усього діапазону можливого розвитку ситуації (передбачення – підготовка – запобігання – реагування – відновлення), що формує запит на методологічний вимір;
- цільового стану, який, серед іншого, передбачає формування спроможностей більшої системи, що відображає цілепокладальний вимір діяльності.

В українській практиці необхідність усвідомлення діяльністного виміру в забезпеченні безпеки й стійкості та його формалізованого

[16] Department of Homeland Security. URL: https://www.dhs.gov/what-security-and-resilience

[17] Svitkova, Katarina. (2017). Resilience in the national security discourse. *Defence & Strategy Journal*. Vol. 1.

закріплення у визначеннях цих термінів додатково ускладнюється. Зокрема, слід вказати на відмінності у трактуванні змісту терміна «безпека» в українськомовному та англомовному дискурсах.

В українській практиці безпека переважно розуміється як стан об'єкта безпеки, тобто як ціль, а не як діяльність суб'єктів із забезпечення його безпеки, що розуміється у документах США. Так, у першому українському національному акті законодавства у сфері національної безпеки термін «національна безпека» трактувався як «*стан захищеності життєво важливих інтересів особи, суспільства та держави від внутрішніх та зовнішніх загроз*, що є *необхідною умовою збереження та примноження духовних та матеріальних цінностей*» [18].

Закон України «Про основи національної безпеки України» залишив незмінним таке розуміння, дещо його модифікувавши та визначивши термін «національна безпека» як «*захищеність життєво важливих інтересів людини і громадянина, суспільства і держави* (тобто стан. – *Авт.*)*, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам*» (опосередковано дається вимір діяльності із досягнення стану) [19]. Новоприйнятий Закон України «Про національну безпеку України» [20] трактує національну безпеку як «*захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз*» [21].

Така ситуація може суттєво вплинути на організаційно-діяльнісний вимір у сфері забезпечення БСКІ. На наше переконання, визначення змісту терміна «безпека» та діяльності в цій сфері має акцен-

---

[18] Про Концепцію (основи державної політики) національної безпеки України: Постанова Верховної Ради України від 16 січня 1997 р. № 3/97-ВР. *Відомості Верховної Ради України (ВВР).* 1997. № 10. Ст. 85. URL: http://consultant.parus.ua/?doc=003A119363

[19] Про основи національної безпеки України: Закон України від 19 червня 2007 р. № 964-IV // База даних «Законодавство України»/ВР України. URL: http://zakon2.rada.gov.ua/laws/show/964-15

[20] Про національну безпеку України: Закон України від 21 червня 2019 р. № 2469-VIII // База даних «Законодавство України»/ВР України. URL: https://zakon.rada.gov.ua/go/2469-19

Слід зазначити, що цей Закон фактично повторює підхід, запропонований законом США National Security Act of 1947, фокусуючись на завданнях органів сектору безпеки і оборони.

[21] Там само.

тувати увагу на діяльності із створення спроможності системи запобігти реалізації загроз будь-якого типу та зберегти систему функціонуючою. З точки зору забезпечення національної безпеки, то йдеться про формування спроможності забезпечення виконання важливих функцій для життєдіяльності країни за будь-яких умов.

Термін «стійкість» ще не визначений українським законодавством, а лише входить у практику використання, а відтак може бути відносно безпроблемно перенесений в Україну. Робота фахівців НІСД з утвердження концепції ЗКІ в Україні дозволила запропонувати визначення стійкості критичної інфраструктури як «*спроможність надійно функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після реалізації загроз будь-якого виду*» [22].

У подальшому зміст поняття «стійкість» було імплементовано у Концепцію створення державної системи захисту критичної інфраструктури, де сказано, що «*створення державної системи захисту критичної інфраструктури спрямоване на забезпечення стійкості критичної інфраструктури до загроз усіх видів, включаючи загрози природного і техногенного характеру, загроз, що спричинені протиправними діями, та інших загроз*» [23].

Фактично закладений концептуальний підхід до формування системи ЗКІ із самого початку імплементував результати еволюції розуміння змісту термінів «безпека» та «стійкість» у США (а також інших країнах – членах НАТО) як ініціаторів та лідерів у цій сфері.

Згідно із запропонованим підходом безпека КІ має забезпечити вихід за межі лише захисту та включати в себе питання адаптації та відновлення. Відтак у процесі створення системи ЗКІ мають бути сформовані вимоги законодавства, запроваджені механізми та інструменти, щоб забезпечити діяльність залучених суб'єктів відповідно до пропонованого змісту терміна «стійкість».

Водночас, ураховуючи чинну практику діяльності потенційних суб'єктів системи, стан розроблення і практичної імплементації термінології в цій сфері, надалі державну систему ЗКІ будемо трак-

[22] Зелена книга з питань захисту критичної інфраструктури в Україні.

[23] Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р // База даних «Законодавство України»/ВР України. URL: http://zakon0.rada.gov.ua/laws/show/1009-2017-%D1%80

тувати як систему забезпечення БСКІ, що дозволяє акцентувати увагу на вищезгаданих особливостях діяльності у цій сфері.

Такий підхід застосовується до цього часу й у США. Зокрема, мета чинного Національного плану захисту критичної інфраструктури США [24] вимагає від органів влади спрямовувати свою діяльність за двома основними напрямами, а саме: «забезпечення безпеки та стійкості країни через посилення захищеності національної критичної інфраструктури шляхом: запобігання, стримування, нейтралізації або пом'якшення наслідків цілеспрямованих дій з боку терористів, спрямованих на знищення, виведення з ладу або зловмисне використання критичної інфраструктури; а також посилення національної готовності, своєчасне реагування та швидке відновлення критичної інфраструктури в разі атаки, стихійного лиха або інших надзвичайних ситуацій».

1.2. Забезпечення безпеки та стійкості критичної інфраструктури у системі забезпечення національної стійкості

Завдання забезпечення національної стійкості останнім часом усе частіше стає пріоритетом також і для інших країн та міждержавних об'єднань. До того ж у національному законодавстві цих країн забезпечення БСКІ є одним із основних елементів формування національної стійкості. Однак є потреба чітко розмежувати завдання у сфері стійкості КІ та національної стійкості.

З позицій системного підходу сфера відповідальності державної системи БСКІ стосується переважно організаційно-функціональної структури життєдіяльності об'єкта, яка забезпечує взаємодію, обмін ресурсами та інформацією між елементами об'єкта [25]. У свою чергу, відповідальність системи забезпечення національної стійкості має охоплювати ширше коло питань життєдіяльності об'єкта, у т. ч. й питання якісних характеристик елементів, які складають цю систему (наприклад, рівень та якість освіти, патріотизм, якість та ефективність діяльності систем).

[24] National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience. URL: https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

[25] Для наших цілей основними елементами системного представлення об'єкта є людина, суспільство, держава, політична організація, економіка, ресурси, довкілля.

Таким чином, система забезпечення БСКІ може виступати складовою частиною системи забезпечення національної стійкості, а результати її роботи та інформація, що в ній циркулюватиме, будуть використовуватися в рамках цієї більшої системи. Виходячи з цього, вважаємо, що розроблені теоретичні засади формування системи БСКІ дозволяють поширити розроблені концепції, моделі та методологію на систему національної стійкості.

Саме така еволюція спостерігається останнім часом на міжнародній арені. Так, питання забезпечення БСКІ є одним із основних елементів формування національної стійкості для країн – членів НАТО. Актуальність цього питання саме для сфери національної безпеки однозначно підтверджують гібридні методи ведення війн, що стали набувати поширення в останні десятиліття.

Гібридні війни відкрили нові виклики національній безпеці, зокрема, оскільки внаслідок їх ведення відбуваються: розмивання раніше чітко визначених меж між станом війни та миру та меж повноважень національних та міжнародних систем безпеки; прогресуюче ускладнення регулювання міжнародних економічних, політичних та безпекових відносин; зростання екстремізму; нівелювання морально-етичних обмежень на застосування насилля як з боку окремих країн, так і громадян; поява нових загроз внаслідок поширення сучасних технологічних новацій (зокрема, у кіберпросторі) [26].

Усі ці виклики стають загрозою для країн, які не здійснюють адаптацію своєї системи забезпечення національної безпеки до викликів часу. Саме це характеризувало Україну до 2014 р. Система забезпечення національної безпеки України, яка до останнього часу значною мірою базувалася на радянських моделях функціонування, фактично виявилася неспроможною адекватно відреагувати на виклики, які виникли. Саме неготовність сектору безпеки і оборони до протидії сучасним загрозам, реалізованим у концепції гібридних війн, поставило Україну в ситуацію екзистенційної кризи та безальтернативності модернізації своєї моделі життєдіяльності та системи безпеки [27].

[26] Суходоля О. М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. *Стратегічні пріоритети*. 2016. № 3. С. 62–76.

[27] Світова гібридна війна: Український фронт: монографія/за заг. ред. В. П. Горбуліна. Київ: НІСД, 2017. 496 с.

Вивчення досвіду реагування України на гібридну війну, розв'язану проти неї Росією, стало серйозним поштовхом до перегляду підходів щодо забезпечення національної безпеки не тільки в Україні, а й у низці інших країн.

Так, главами держав та урядів країн на Варшавському саміті НАТО у липні 2016 р. було визначено сім базових вимог (the Seven Baseline Requirements) до країн – членів НАТО щодо забезпечення національної стійкості [28]:

- безперервність урядування та надання найважливіших державних послуг;
- стійкість енергозабезпечення;
- здатність ефективно справлятись із неконтрольованим переміщенням людей;
- стійкість водозабезпечення та постачання продовольства;
- здатність надавати допомогу великій кількості людей, що отримали пошкодження;
- стійкість систем комунікацій;
- стійкість транспортної системи.

Євросоюз запропонував Глобальну стратегію ЄС із зовнішньої політики та політики безпеки [29], де питання БСКІ є пріоритетними у подальшій стратегії розвитку ЄС.

Глобальна стратегія ЄС визнала потребу посилити спроможність Співтовариства орієнтуватись та рухатися вперед «у цьому більш взаємозв'язаному, конкурентному та складному світі». Основним пріоритетом та інструментом забезпечення такої спроможності було визнано «стійкість демократичного розвитку», яка, у свою чергу, створює «зовнішній авторитет та вплив» ЄС, а відтак буде нівелювати загрози.

Глобальна стратегія ЄС визначила стійкість основним інструментом та ціллю як щодо розбудови власної спроможності, так і щодо взаємовідносин із своїми сусідами.

---

[28] Commitment to Enhance Resilience/NATO. URL: http://www.nato.int/cps/en/natohq/official_texts_133180.htm?selectedLocale=en

[29] Див.: European Union. Global Strategy fo the European Union's Foreign and Security Policy: Shared Vision, Common Action: A Stronger Europe. (June 2016). Brussels: European Union. P. 7. URL: https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf ; https://europa.eu/globalstrategy/en/global-strategy-foreign-and-security-policy-european-union

У внутрішньому вимірі ставиться завдання посилення та розвитку механізмів взаємодопомоги і солідарності в діях країн-членів з метою сприяння колективній безпеці ЄС. Виокремлюються п'ять основних напрямів із формування стійкості ЄС і прикладення зусиль держав, громадськості та бізнесу в найближчій перспективі:

- безпека та оборона – ЄС має взяти на себе більшу відповідальність за безпеку та «бути готовим і здатним стримувати, відповідати і захищати себе від зовнішніх загроз»;
- боротьба з тероризмом – ЄС вважає за необхідне збільшення інвестицій та посилення солідарності в боротьбі з тероризмом, здійснюючи з метою формування спроможності швидкого відновлення держав-членів у разі нападу посилення зусиль щодо забезпечення постачання ресурсів, захисту критичної інфраструктури та захисту від кіберзагроз;
- кіберзахист – ЄС визначає необхідність формування спроможності країн-членів захищати себе від кіберзагроз при збереженні та підтримці відкритого, вільного та безпечного кіберпростору. Це потребує заходів щодо посилення технологічних можливостей, спрямованих на пом'якшення загроз та зміцнення стійкості критично важливої інфраструктури, мереж та послуг, а також зменшення кіберзлочинності;
- енергетична безпека – ЄС продовжить докладати зусилля щодо диверсифікації джерел, маршрутів та постачальників енергії, особливо в газовій сфері, а також просування найвищих стандартів ядерної безпеки в третіх країнах. Досягти цього планується за допомогою заходів енергетичної дипломатії, зокрема зміцнення відносини в усьому світі з надійними енергогенеруючими і транзитними країнами, підтримання створення інфраструктури доступу енергоносіїв на європейські ринки;
- стратегічні комунікації – ЄС посилюватиме стратегічні зв'язки із партнерами, інвестуватиме у публічну дипломатію в різних сферах з метою формування прихильності громадян, іноземних країн до політики ЄС. Поліпшуватиме механізми та швидкість обміну інформацією з партнерами, застосовувати інструменти та заходи щодо спростовування дезінформації.

У зовнішньому вимірі Глобальною стратегією ЄС фактично формуються нові принципи та вимоги щодо співпраці із країнами-

партнерами виключно крізь призму посилення стійкості цих партнерів. При цьому наголошується, що «стійке суспільство, демократія, довіра до інституцій та стабільність розвитку є основою стійкості держави».

У зазначеній Стратегії вводиться поняття «суспільна стійкість» та відображається його розуміння, а саме: жодна держава не може бути стійкою, якщо до уваги системи забезпечення безпеки не входять питання, що стосуються гуманітарної сфери, розвитку, торгівлі, інвестицій, інфраструктури, освіти та охорони здоров'я – усіх аспектів, що є центральними елементами стійкості суспільства.

При цьому Глобальна стратегія ЄС пропонує переглянути програми та механізми співпраці та допомоги країнам-партнерам з метою побудови стійких націй та систем урядування. Наголошується, що ЄС запровадить різносторонній підхід до співпраці із партнерами, проводячи індивідуальну політику формування стійкості партнера, спрямовану на підтримку інклюзивної діяльності у сфері управління, боротьби з тероризмом, корупцією та організованою злочинністю, захищаючи права людини та підтримуючи демократію.

За цим напрямом ЄС пропонує розвивати «Комплексний підхід до конфліктів та криз». Передбачається збільшення практичного залучення ЄС у безпекову співпрацю з країнами-партнерами, щоб побудувати комплексну систему, предметна увага якої зосереджуватиметься на широкому діапазоні питань: від безпеки до гендерної рівності, від державного управління до економічної діяльності. Запровадження багатостороннього аналізу та планування через реалізацію відповідних політик та інструментів співпраці спрямовуватиметься на запобігання виникнення конфліктів, їх менеджменту та вирішення. При цьому зазначається, що такий підхід до кризового менеджменту вдосконалюватиметься на основі багатофазового підходу щодо формалізації співпраці на різних етапах циклу розвитку кризи. Стратегія наголошує, що ЄС буде інвестувати у попередження виникнення кризи, її розв'язання і стабілізацію ситуації, а також унеможливлення передчасного зниження уваги до ситуації з метою недопущення рецидиву кризи цієї ж природи.

Деталізація змісту діяльності у цій сфері відбувається на національному рівні. Окремі країни за власною ініціативою, а також на виконання Глобальної стратегії ЄС розпочинають усе активніше приділяти увагу питанням національної стійкості. До прикладу,

Фінляндія розробила Стратегію безпеки суспільства (The Security Strategy for Society) [30], якою цю безпеку визначено за мету та пропонуються основні принципи формування стійкого суспільства.

Всеохоплююча модель безпеки, що закладається у Стратегії Фінляндії, – це модель співпраці, в якій життєво важливі функції [31] життєдіяльності суспільства забезпечуються спільно державою, підприємцями, організаціями та громадянами. Відтак забезпечення безпеки досягається в рамках моделі співпраці, в якій актори повідомляють одне одному інформацію про безпеку та аналізують цю інформацію, готують спільні плани, а також навчаються та діють разом. Таким чином, модель охоплює всіх відповідних суб'єктів: від громадян до влади, а співпраця базується на окремих документах (секторальних, галузевих угодах про співпрацю та урядових програмах).

Фінляндія виокремлює найважливіші функції, що описують широкий спектр та міжгалузевий характер розвитку спроможностей держави. Тому у Стратегії цієї країни описано, як слід застосовувати загальні принципи готовності та управління в кризових ситуаціях на урядовому, регіональному та муніципальному рівнях. Життєво важливими, на думку творців цієї Стратегії, є такі сім складових:

- лідерство;
- міжнародне співробітництва та діяльність у рамках ЄС;
- оборонна спроможність;
- внутрішня безпека;
- стійкість економіки, інфраструктури та безпеки постачання (ресурсів);
- функціональна спроможність населення та публічних служб;
- психологічна стійкість населення.

У Стратегії безпеки суспільства, розробленій Фінляндією, наголошується на необхідності залучення всього суспільства до виконання визначених завдань та пропонуються механізми координації зусиль та концентрації приватних і державних ресурсів на різних рівнях. Ця Стратегія визначає за мету забезпечення реалізації

[30] The Security Strategy for Society. Finnish Government Resolution. (2017, November 02). URL: https://www.defmin.fi/files/1883/PDF.SecurityStrategy.pdf

[31] *Життєво важливі функції* – це функції, які виконують державні органи, державні установи, підприємства та організації будь-якої форми власності, порушення яких призводить до швидких негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки.

життєво важливих функцій держави за будь-яких умов. При цьому встановлюються окремі завдання органам влади та іншим суб'єктам, залученим до системи забезпечення національної стійкості, а також організаційні принципи їх виконання.

Загалом у документі визначено 57 основних завдань забезпечення реалізації життєво важливих функцій. Серед яких, зокрема, такі:

- забезпечення стратегічного лідерства держави; забезпечення допомоги громадянам за межами країни;
- закріплення ролі країни на міжнародній арені (у міжнародних організаціях, наприклад ЄС, у механізмах та організаціях кризового реагування; гуманітарних місіях тощо);
- включеність Фінляндії у світовий розподіл праці (безпроблемність вільного руху товарів та послуг між Фінляндією та іншими країнами);
- посилення внутрішньої безпеки Фінляндії (правоохоронна система, кризові служби, імміграційний контроль);
- посилення обороноздатності країни, контроль кордону, морського простору;
- безпека постачання палива, енергії, води;
- безпека та надійність роботи системи комунікацій і транспорту;
- збереженість важливої промислової бази та послуг;
- функціональність систем соціального захисту та медичного забезпечення;
- підтримка ефективної системи навчання, підготовки кадрів та наукових досліджень;
- гарантування наявності товарів повсякденного використання, системи допомоги останньої надії;
- гарантування належного рівня житлових умов;
- підтримання системи закладів культури та захист культурних цінностей;
- забезпечення безперервності ведення бізнесу, страхування;
- розвиток волонтерських ініціатив;
- формування здатності до відновлення.

Усе зазначене вище дозволяє нам запропонувати модель розмежування відповідальності та завдань у сферах:

1) забезпечення безпеки та стійкості критичної інфраструктури;
2) національної стійкості.

Реалізація життєво важливих функцій для життєзабезпечення населення, суспільства і держави можлива за наявності структури (інфраструктури) та елементів, що її виконують. Інфраструктура, призначена для забезпечення реалізації життєво важливої функції, має переважно фізичний вимір (включно Інтернет як система кабелів та пристроїв електронної комунікації). Зауважимо, що окремі елементи системи мають також і якісні характеристики забезпечення реалізації життєво важливої функції, як-от: кваліфікація персоналу, об'єм економіки країни, психологічна стійкість населення тощо.

Наприклад, функцію державного управління можливо реалізувати за наявності:

- інфраструктури системи у фізичному (споруди, обладнання систем зв'язку, витратні матеріали тощо) та організаційному (завдання органів влади, їхні взаємовідносини між собою та суспільством, способи донесення до споживачів послуг із урядування інформації) вимірах;
- елементів системи, що її здійснюють, а саме персоналу органів влади, який використовує інфраструктуру при здійсненні своїх обов'язків.

При цьому ефективність реалізації функції державного управління залежить не тільки від наявності та роботоспроможності інфраструктури, а й від характеристик якості елементів: кваліфікації персоналу, його моральності, патріотизму тощо.

Завдяки цій моделі можна проілюструвати підхід щодо розмежування сфери відповідальності систем забезпечення захисту та стійкості критичної інфраструктури та національної стійкості. Так, державна система БСКІ має забезпечити наявність та постійність роботи інфраструктури для забезпечення реалізації життєво важливих функцій. Одночасно система забезпечення національної стійкості, використовуючи результати роботи системи забезпечення БСКІ, має охоплювати питання якості елементів, що використовують інфраструктуру, а також ураховувати всю складність взаємовідносин національної системи стійкості з іншими більшими системами (інші національні системи, міжнародні утворення, світоглядні концепції тощо).

Дійсно, такими життєво важливими функціями, як-от забезпечення психологічної стійкості населення, як це визначено у Фінляндії, система БСКІ займатись не буде. Це завдання відноситься в осно-

вному до системи національної стійкості, при обмеженій увазі з боку системи БСКІ.

Натомість інша життєво важлива функція, а саме: забезпечення безперервності урядування та надання найважливіших державних послуг, як це визначається країнами НАТО, потребуватиме залучення обох систем. Система БСКІ має опікуватися питаннями інфраструктури забезпечення реалізації життєво важливої функції (фізичний, організаційний, структурний виміри), у той час як інші аспекти, пов'язані із якістю елементів, слід віднести до сфери уваги системи національної стійкості.

Відповідно до цієї моделі така життєво важлива функція, як стійкість економіки, за визначенням більшості країн світу, окрім системи забезпечення БСКІ, потребуватиме також залучення різних інших систем. Однак для недопущення негативного впливу застосування різних механізмів управління для різних цілей (забезпечення БСКІ, недопущення використання суб'єктів економіки для фінансування тероризму, захист національного виробника) необхідне їхнє розмежування. При цьому недоцільно зводити всі завдання до управління однією із систем, проте різні системи мають налагодити механізми обміну інформацією для досягнення своїх цілей.

Зауважимо, що стійкість енергозабезпечення як життєво важлива функція з точки зору багатьох країн світу в основному має перебувати у сфері уваги системи БСКІ.

Таким чином, сфера відповідальності системи БСКІ залежатиме від визначення рівня втручання держави у регулювання життєдіяльності та набору життєво важливих функцій для життєдіяльності населення, суспільства і держави. Рівень втручання держави в регулювання діяльності суспільства залежить від обраної країною соціально-політичної моделі здійснення владних повноважень.

Перелік життєво важливих функцій (послуг), щодо забезпечення безпеки та стійкості яких національні уряди вживають заходів, залежить від соціокультурного, економічного та технологічного розвитку країн і, окрім цього, може змінюватись у часі відповідно до динаміки цього розвитку.

Наприклад, зважаючи на появу кіберзагроз як нового типу загроз, а відтак і розширення можливостей втручання у демократичні процедури життєдіяльності суспільства за допомогою викривлення інформації, США ідентифікували виборчу інфраструктуру як кри-

тичну для національної безпеки. Так, за результатами розслідування втручання Російської Федерації у процес виборів Президента США у 2016 р. були підготовлені заходи запобігання повторення таких ситуацій у майбутньому. Функція демократичного волевиявлення була визначена життєво важливою для США, а отже, і її забезпечення на найвищому рівні. Відтак інфраструктура, яка забезпечує процес демократичного волевиявлення, стала ідентифікуватись як критична.

Відповідно у 2018 р. Конгресом США було розроблено законопроект [32], яким запропоновано внести зміни у визначення дефініції «критична інфраструктура», що раніше було введено законом США (USA PATRIOT ACT, 2001) [33]. Зокрема, пропонувалося таке визначення: «Критична інфраструктура означає системи та ресурси, фізичні або віртуальні, що є надзвичайно важливими для Сполучених Штатів, а недієздатність або знищення таких систем та активів матиме катастрофічний регіональний чи національний вплив на здоров'я населення або безпеку, економічну безпеку або національну безпеку, *в т. ч. бази даних для реєстрації виборців*, *машини для голосування та інші системи зв'язку*, *які керують виборчим процесом*, *а також представляють і публікують результати від імені державних та місцевих органів влади* (пропоноване доповнення виділено курсивом. – *Авт.*)».

Отже, як бачимо, підтримання життєво важливих функцій життєдіяльності суспільства, захист базових потреб його членів та формування у них відчуття безпеки – це базова умова забезпечення національної стійкості. Відтак забезпечення БСКІ як організаційно-функціональної структури життєдіяльності визначено базовим елементом забезпечення національної стійкості [34].

У свою чергу, розподіл та об'єм завдань для органів державної влади, залучених до забезпечення функціонування системи БСКІ,

[32] Defending American Security from Kremlin Aggression Act of 2018. URL: https://www.congress.gov/bill/115th-congress/senate-bill/3336/text?q=%7B%22search%22%3A%5B%22S.3336%22%5D%7D&r=1

[33] Закон США (USA PATRIOT ACT, 2001). URL: https://www.congress.gov/bill/107th-congress/house-bill/3162

Визначення дефініції «критична інфраструктура», подане цим законом, наведено далі на с. 33.

[34] Суходоля О. М. Захист критичної інфраструктури: сучасні виклики та пріоритетні завдання сектору безпеки. *Науковий часопис Академії національної безпеки*. 2017. № 1–2 (13–14). С. 50–80.

залежатиме від моделі організації державної влади та структури її органів, що також конкретизується рішеннями уряду певної країни.

На нашу думку, до основних життєво важливих функцій, підтримання яких має забезпечити КІ, слід віднести:

- надання належних послуг для забезпечення життєдіяльності членів суспільства (населення);
- надійність і гарантованість забезпечення належних послуг, у т. ч. енергозабезпечення, транспортування, водопостачання, продовольче забезпечення;
- розвиненість та ефективність фінансово-економічної інституційної основи національної економіки та життєдіяльності суспільства;
- мінімальний негативний вплив на довкілля (екологічно сприятливе господарювання);
- надання медичної допомоги членам суспільства та реагування на випадок виникнення кризових ситуацій;
- розвиненість інформаційно-комунікаційної системи суспільства;
- скерованість розвитку суспільства та дотримання його членами визначених правил життєдіяльності;
- спроможність нейтралізувати зовнішні негативні впливи (силового, економічного, інформаційного тощо).

Така організаційно-функціональна структура схоплює основні процеси життєдіяльності суспільства і, за поточних умов розвитку, визначає стійкість системи, а відтак і сектори КІ (як інфраструктура, що має спільну функціональну спрямованість), що потребують першочергового захисту. У «Зеленій книзі з питань захисту критичної інфраструктури України» виокремлено десять секторів КІ [35]. Стійкість функціонування цієї інфраструктури має стати одним із основних індикаторів забезпечення національної безпеки України.

[35] Слід зазначити, що кількість секторів КІ залежить від спроможності суб'єкта управління забезпечити моніторинг, оцінку, запобігання та реагування на випадок реалізації загроз для вибраної кількості критичних елементів. Фактично йдеться про ресурсну та кваліфікаційну спроможність держави відстежувати визначену кількість процесів (найбільш важливих, на її погляд) та забезпечувати вплив на їхнє протікання. Перелік секторів, включених до національної КІ США, є, очевидно, найбільш повним і містить 16 секторів. У цій публікації пропонується для України виокремити 11 секторів критичної інфраструктури, що забезпечують надання життєво важливих функцій (послуг) (*Додаток 1.4*).

Отже, запропонований теоретико-методологічний підхід до ***Концепції створення державної системи захисту критичної інфраструктури*** може стати основою для запровадження системи національної стійкості, оскільки дозволяє методологічно поєднати зусилля різних чинних державних систем безпеки (захисту) та реагування на кризові ситуації.

При цьому урядові рішення та документи, розроблені для створення державної системи БСКІ, лише доповнюватимуться переліком життєво важливих функцій та відповідними розділами щодо завдань, які будуть поставлені перед залученими суб'єктами.

Р о з д і л 2

СВІТОВИЙ ДОСВІД СТВОРЕННЯ НАЦІОНАЛЬНИХ СИСТЕМ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1. Передовий зарубіжний досвід створення національних/державних систем забезпечення безпеки та стійкості критичної інфраструктури

Незважаючи на те, що проблема захисту важливих для функціонування держави, суспільства та життєдіяльності населення систем та об'єктів існувала завжди, до числа тих, що потребують системного підходу з точки зору національної та/або державної безпеки, вона потрапила наприкінці минулого століття. Саме тоді в офіційних документах США були вперше визначені й термін «критична інфраструктура», і сектори, які віднесли до неї [36]. Натомість посилений розвиток відповідного безпекового напряму розпочався як наслідок уроків, винесених із терактів 11 вересня 2001 р., коли було усвідомлено рівень загроз міжнародного тероризму.

На теперішній час системи забезпечення БСКІ національного рівня створені практично в усіх розвинених країнах світу. Що стосується України, то до 2014 р. сектор безпеки і оборони країни перебував у стані поступової деградації, наслідком чого стало теперішнє відставання України на цьому напрямі від більшості європейських країн не менш ніж на 10–15 років, не кажучи вже про такі провідні країни, як США, Велика Британія та Німеччина.

Для скорочення відставання України від провідних країн світу за цим напрямом необхідно максимально повно використовувати кращий зарубіжний досвід, вивчати та адаптувати до національних умов передові практики побудови й розвитку державної системи БСКІ. З-поміж багатьох країн, де функціонують такі системи,

[36] On July 15, 1996, President Clinton signed Executive Order 13010 establishing President's Commission on Critical Infrastructure Protection (PCCIP). *Critical Infrastructure Protection. Federal Register*. July 17, 1996. Vol. 61. No. 138.

особливу увагу привертають США, Велика Британія, та Польща. Цей вибір було зроблено на основі зазначених нижче міркувань.

1. США – лідер у запровадженні інноваційних підходів, мають розвинуту, добре розгалужену національну державну систему забезпечення БСКІ.

2. Велика Британія є одним із європейських лідерів у запровадженні ЗКІ, активно розвиває концепцію БСКІ. Немаловажним фактором у виборі стало й те, що представники британського уряду неодноразово висловлювали свою зацікавленість і готовність у наданні допомоги Україні саме в цій сфері.

3. Польща – наш сусід, і за своєю територією та населенням, економічним потенціалом та промисловою інфраструктурою є порівняною з Україною, що дозволяє використовувати польський досвід при оцінці у першому наближенні масштабів відповідних завдань, які постануть перед Україною при створенні державної системи БСКІ.

Слід зауважити, що проблематика КІ пов'язана із бурхливим розвитком нових підходів до забезпечення національної безпеки в розвинених країнах світу, що спричинено швидкими змінами, які відбуваються у безпековому середовищі у глобальному, регіональному та національному вимірах. Зрозуміло, що це знаходить відповідне відображення у розвитку національних законодавств, у т. ч. в термінологічному забезпеченні діяльності державних органів тієї чи тієї країни.

Україна перебуває на початковому етапі створення державної системи БСКІ, тому при розгляді зарубіжного досвіду в цій сфері з метою його використання важливо виокремити загальні підходи до створення національних систем, їх основні цілі, структурні особливості та базові елементи, механізми та інструменти, які забезпечують їхнє функціонування. При цьому, звичайно, слід пам'ятати, що механічне перенесення навіть передового досвіду без належного урахування специфіки та реалій українського сьогодення може лише підірвати зусилля на цьому напрямі, скомпрометувати його та в такий спосіб суттєво затримати його розвиток у нашій країні.

Виходячи з наведених вище міркувань та задля полегшення сприйняття зведеної інформації про зарубіжний досвід у цій сфері, стисло викладемо огляд національних систем БСКІ згаданих країн, представлений, наскільки це було можливо, у єдиному форматі, максимально зручному для порівняння.

2.1.1. Система забезпечення безпеки та стійкості критичної інфраструктури в США

Правові засади створення державної системи БСКІ. Перш за все слід навести низку базових термінів, які існують у політичних та законодавчих актах США.

Під *критичною інфраструктурою* закон США розуміє «системи та засоби, фізичні чи віртуальні, настільки важливі для Сполучених Штатів, що недієздатність або знищення таких систем та активів підривало би національну безпеку, національну економіку, загрожувало би здоров'ю чи безпеці населення, чи мало би результатом будь-яку комбінацію із переліченого» [37].

Політична директива Президента США (PPD-21) [38] визначає *безпеку* «як зменшення ризиків для критичної інфраструктури шляхом вжиття фізичних заходів чи захисних кіберзаходів стосовно вторгнень, нападів або дії природних лих чи техногенних аварій».

PPD-21 визначає *стійкість* «як здатність підготуватися та адаптуватися до умов, що змінюються, а також протистояти збоям і швидко відновлюватися після них. Стійкість включає здатність протистояти зловмисним нападам, аваріям чи загрозам та інцидентам природного походження».

Варто зважити на те, що, починаючи з 2005 р., державна політика США щодо КІ конкретизується *планами захисту національної інфраструктури*, які регулярно оновлюються [39], а в структурі МВБ США функціонує спеціальний *Офіс захисту критичної інфраструктури* [40]. Визначення самого терміна «захист критичної інфраструктури»

---

[37] USA PATRIOT ACT (2001) defined critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." URL: https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf

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

[39] Нині реалізація політики США щодо безпеки та стійкості КІ відбувається на основі положень чинного Плану захисту критичної інфраструктури (2013): Партнерство для безпеки і стійкості критичної інфраструктури. (див. URL: https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf).

[40] Office of National Infrastructure Protection. URL: https://www.dhs.gov/office-infrastructure-protection

у національному законодавстві Сполучених Штатів відсутнє, що, ймовірно, пов'язанне із поширенням на цю сферу принципів, уже визначених національним законодавством щодо захисту інших об'єктів (наприклад, таких як ядерні матеріали та ядерні установки).

Політика США спрямована на посилення *безпеки та стійкості КІ стосовно фізичних і кіберзагроз*. З цією метою Федеральний уряд співпрацює із власниками та операторами відповідних об'єктів і систем, державними органами всіх рівнів, місцевими органами влади з тим, щоб вживати активних заходів з *управління ризиками*, враховуючи при цьому *всі види загроз*, реалізація яких може призвести до тяжких наслідків для національної безпеки, стабільності економіки, здоров'я та безпеки населення чи будь-якої комбінації з переліченого. При цьому зусилля спрямовуються на зменшення уразливостей, мінімізацію наслідків, ідентифікацію та ліквідацію загроз, прискорення реагування та застосування відновлювальних заходів, пов'язаних з КІ. Уряд ураховує міжнародний контекст проблем, пов'язаних із безпекою та стійкістю КІ, та взаємодіє з міжнародними партнерами у цій сфері.

Зусилля США, спрямовані на забезпечення безпеки та стійкості КІ, мають вживатись у комплексний та цілісний спосіб, щоб відобразити взаємозв'язки та взаємозалежності елементів КІ. До того ж у PPD-21 *енергетичні системи та системи зв'язку визначені як такі, що мають унікальний рівень критичності* внаслідок того, що вони забезпечують функціонування всіх інших секторів КІ.

Підходи Федерального уряду на цьому напрямі визначаються *трьома стратегічними імперативами*:

1) уточнювати та роз'яснювати взаємозв'язки всіх урядових структур задля забезпечення загальнонаціональної єдності при посиленні безпеки та стійкості КІ;

2) забезпечувати ефективний обмін інформацією між усіма суб'єктами процесу;

3) забезпечувати виконання функцій інтегрування та аналізу даних для підтримки процесів планування та прийняття рішень стосовно КІ.

Усі керівники міністерств та федеральних агентств несуть відповідальність за ідентифікацію, визначення пріоритетів та оцінку (загроз), корегувальні дії та безпеку підпорядкованих їм елементам КІ, які забезпечують виконання життєво важливих функцій у рамках

доручених цим органам основних місій. Відповідні заходи щодо КІ мають бути відображені в планах та при виконанні вимог *Національної політики безперервності* [41].

Відповідно до Плану захисту національної інфраструктури (2009), *стратегічну та нормативно-правову основу діяльності* у цій сфері становлять три категорії актів та ініціатив, а саме:

1) стратегічні документи і закони США, які визначають політику держави у забезпеченні внутрішньої безпеки;

2) президентські директиви з питань внутрішньої безпеки;

3) національні ініціативи, плани тощо.

Завдяки всьому комплексу елементів, що становлять стратегічну та нормативно-правову основу діяльності всіх учасників процесу, запроваджується їх скоординований підхід до забезпечення БСКІ.

Із загалу документів і стратегій насамперед слід виокремити:

- Національну стратегію внутрішньої безпеки (жовтень 2007 р.) [42];
- Національну стратегію фізичного захисту критичної інфраструктури та ключових активів (лютий 2003 р.) [43];
- Національну стратегію захисту кіберпростору (лютий 2003 р.) [44];
- Закон про внутрішню безпеку (листопад 2002 р.) [45].

Серед найбільш важливих щодо безпеки та стійкості КІ президентських директив необхідно назвати такі:

- президентська політична Директива 21 «Безпека та стійкість критичної інфраструктури» (лютий 2013 р.) [46];
- указ президента США № 13636 «Удосконалення кібербезпеки критичної інфраструктури» (лютий 2013 р.) [47];

---

[41] National Continuity Policy (див. сайт U.S. FEMA. URL: https://www.fema.gov/media-library-data/1384886826028-729844d3fd23ff85d94d52186c85748f/NCPIP.pdf).

[42] The National Strategy for Homeland Security. URL: https://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf

[43] The National Strategy for the Physical Protection of Critical Infrastructures and Key Asset. URL: https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

[44] The National Strategy to Secure Cyberspace. URL: https://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf

[45] Homeland Security Act of 2002. URL: https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf

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

[47] Executive Order 13636: Improving Critical Infrastructure Cybersecurity. URL: https://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf

- президентська політична Директива 8 «Національна готовність» (березень 2011 р.) [48];
- президентська Директива 7 з питань внутрішньої безпеки «Ідентифікація, пріоритетизація та захист критичної інфраструктури» (грудень 2003 р.) [49].

Основні документи, які належать до категорії документів, що утворюють нормативно-правову основу державної політики США щодо КІ, такі:

- План захисту національної інфраструктури (2013): Партнерство заради безпеки та стійкості критичної інфраструктури [50]. Це основний чинний документ з питань КІ, що замінив попередні, а саме: План захисту національної інфраструктури (2009): Партнерство заради захисту та стійкості критичної інфраструктури [51]; План захисту національної інфраструктури (2006) [52].

Крім того, відповідно до підходу МВБ до цієї ж категорії планів та ініціатив віднесено: Національну систему управління інцидентами (2008) [53], Національну основу реагування (2008) [54]; Національні керівні принципи для забезпечення готовності (2007) [55].

Чинний План захисту національної інфраструктури 2013 узгоджений з указом президента № 13636 «Удосконалення кібербезпеки критичної інфраструктури» [56], а також із Системою забезпечен-

[48] Presidential Policy Directive/PPD-8: National Preparedness. URL: https://www.dhs.gov/presidential-policy-directive-8-national-preparedness

[49] Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection. URL: https://www.dhs.gov/homeland-security-presidential-directive-7

[50] План захисту критичної інфраструктури (2013): Партнерство для безпеки і стійкості критичної інфраструктури. URL: https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

[51] National Infrastructure Protection Plan (2009). URL: https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2009-508.pdf.

[52] National Infrastructure Protection Plan. (2006). URL: https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf

[53] National Incident Management System. (2008). URL: https://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf

[54] National Response Framework. (2008). URL: https://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf

[55] National Preparedness Guidelines. (2007). URL: https://www.fema.gov/media-library-data/20130726-1718-25045-3265/npg.pdf

[56] Executive Order 13636: Improving Critical Infrastructure Cybersecurity. (2013). URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

ня національної готовності (National Preparedness System), що створена на виконання президентської політичної Директиви 8 «Національна готовність» [57].

Організаційні засади створення державної системи БСКІ в США. Ключову роль у державній системі БСКІ Сполучених Штатів відіграє Міністерство внутрішньої безпеки США, на керівника якого покладено функцію *стратегічного керівництва об'єднаних зусиль нації щодо забезпечення безпеки та стійкості КІ*, як це визначено в PPD-21. Відповідно до зазначеної Директиви міністр внутрішньої безпеки США повинен забезпечувати щоденну взаємодію з визначеними *відповідальними за конкретні сектори агентствами* (Sector-Specific Agency) [58], постійне залучення спеціалізованих можливостей та досвіду відповідального за конкретний сектор агентства, ефективну взаємодію з операторами та власниками об'єктів і систем КІ, місцевими органами влади всіх рівнів. Партнерство з усіма переліченими суб'єктами є імперативом у діяльності МВБ.

У *табл. 2.1* представлений перелік секторів національної (критичної) інфраструктури США (загалом їх 16) та відповідальні за конкретний сектор КІ державні органи.

Крім того, що МВБ відіграє провідну роль у забезпеченні взаємодії у рамках зусиль, спрямованих на підвищення БСКІ на національному рівні, це міністерство виконує функції відповідального федерального органу за 10 секторів КІ (у т. ч. для семи секторів на МВБ покладена виключна відповідальність, і ще для трьох – спільно з іншими федеральними органами).

У зв'язку з провідною роллю МВБ у системі БСКІ важливі функції на національному рівні виконує і спеціалізований підрозділ міністерства – *Офіс захисту інфраструктури* [59], призначений керувати національними програмами та координувати їх виконання, а також

[57] Presidential Policy Directive 8 8/PPD-8 National Preparedness. URL: https://www.dhs.gov/presidential-policy-directive-8-national-preparedness

[58] Відповідно до PPD-21, «відповідальне за конкретний сектор агентство» – це федеральний орган, на який згаданою директивою «покладена відповідальність за забезпечення інституційного знання та спеціалізованих експертних можливостей, а також за керування, сприяння чи за підтримку програм з безпеки та стійкості та пов'язаної з ними діяльності у закріпленому за цим органом секторі критичної інфраструктури в безпекових умовах, які враховують загрози усіх видів».

[59] Office of Infrastructure Protection. URL: https://www.dhs.gov/office-infrastructure-protection

Таблиця 2.1. **Сектори критичної інфраструктури США та відповідальні за них федеральні органи**

Сектор критичної інфраструктури	Відповідальний орган
Хімічний сектор (Chemical)	МВБ
Комерційні об'єкти (Commercial Facilities)	»
Зв'язок (Communications)	»
Критичне виробництво (Critical Manufacturing)	»
Дамби та інші гідротехнічні споруди (Dams)	»
Оборонно-промислова база (Defense Industrial Base)	Міністерство оборони
Служби екстреної допомоги населенню, реагування на надзвичайні ситуації (Emergency Services)	МВБ
Енергетичний сектор (Energy)	Міністерство енергетики
Банки та фінанси (Financial Services)	Міністерство фінансів
Продукти харчування та сільське господарство (Food and Agriculture)	Міністерство сільського господарства, Міністерство охорони здоров'я та соціальних служб
Урядові об'єкти (Government Facilities)	МВБ, Адміністрація служб загального призначення
Охорона здоров'я та медицина (Healthcare and Public Health)	Міністерство охорони здоров'я та соціальних служб
Інформаційні технології (Information Technology)	МВБ
Ядерні реактори, ядерні матеріали та відходи (Nuclear Reactors, Materials, and Waste)	»
Транспортні системи (Transportation Systems)	МВБ, Міністерство транспорту
Водні ресурси, системи водопостачання та стічних вод (Water and Wastewater Systems)	Агентство захисту навколишнього середовища

Джерело: складено автором за інформацією сайту МВБ США (див.: URL: https://www.dhs.gov/cisa/critical-infrastructure-sectors).

реалізовувати державну політику щодо безпеки та стійкості КІ. Офіс розвиває ефективне партнерство між урядом та приватним сектором, здійснює оцінку уразливості та наслідків з тим, щоб сприяти власникам і операторам об'єктів і систем, а також партнерам на всіх рівнях управління усвідомити ризики для КІ та вжити необхідних заходів щодо їх зниження. Офіс надає інформацію про появу нових загроз та небезпек, забезпечує можливості для навчання з метою управління ризиками щодо КІ.

До складу Офісу захисту інфраструктури входять такі підрозділи: Відділ збирання інформації про інфраструктуру (Infrastructure Information Collection Division); Відділ дотримання вимог щодо безпеки інфраструктури (Security Compliance Division); Центр координування національної інфраструктури (National Infrastructure Coordinating Center); Відділ координації з фізичної безпеки (Protective Security Coordination Division) та деякі інші.

Згідно із PPD-21 на кожний федеральний орган, уповноважений виконувати функції відповідального за сектор агентства, покладено відповідальність за розробку та виконання *секторальних планів*, у яких концептуальні положення Плану захисту національної інфраструктури мають бути конкретизовані відповідно до унікальних характеристик кожного із секторів та безпекових умов, у яких він перебуває. Секторальні плани мають постійно оновлюватися для того, щоб відповідати положенням чинного Плану захисту національної інфраструктури.

Забезпечення ефективного обміну інформацією віднесено до одного з трьох стратегічних імперативів, які мають визначати підходи федеральних органів до забезпечення БСКІ.

Крім того, у чинному Плані захисту національної інфраструктури (2013) досягнення обміну «придатною до використання та відповідною інформацією у рамках спільноти критичної інфраструктури з метою формування усвідомлення та підтримки процесу прийняття рішень» віднесено до п'яти стратегічних цілей, на яких упродовж кількох найближчих років має бути сфокусована діяльність у цій сфері.

План захисту національної інфраструктури реалізується через управління ризиками та розбудову партнерства, одним з основних інструментів для яких є обмін інформацією між усіма учасниками процесу.

PPD-21 на міністра внутрішньої безпеки покладено відповідальність за належне функціонування *центрів з питань національної критичної інфраструктури*, які забезпечують:

- можливості для отримання інформації про поточну ситуацію на об'єктах і в системах КІ;
- узагальнення та підготовку інформації про появу нових трендів, неминучих загроз та розвиток інцидентів і криз на об'єктах та в системах КІ.

Відповідно до уточненої структури у сфері управління МВБ мають функціонувати *центри з питань фізичної інфраструктури* та *з питань кіберінфраструктури*. Обидва повинні діяти як єдиний комплекс та слугувати координаційними центрами для партнерів міністерства, де вони можуть отримувати інформацію про конкретні умови на тому чи іншому майданчику, а також зведену, готову до використання інформацію для вжиття заходів з фізичної та кібербезпеки на об'єктах і в системах КІ.

У взаємодії з відповідальними за сектори КІ агентствами та іншими федеральними органами міністр має сприяти наданню доступу власникам і операторам до інформації (у т. ч. розвідувальної), необхідної для забезпечення безпеки та стійкості КІ, підтримувати заходи з обміну такою інформацією між усіма суб'єктами процесу.

Положення чинного Плану захисту національної інфраструктури (2013) у частині обміну інформацією узгоджені з Національною стратегією обміну інформацією та її захистом (2012) (National Strategy for Information Sharing and Safeguarding 2012), відповідно до якої мають бути створені механізми та протоколи обміну інформацією державних органів з приватними партнерами в рамках конкретних секторів з тим, щоб забезпечити належну якість і своєчасність інформації, необхідної для захисту національної інфраструктури.

У США перші кроки в напрямі системної розбудови державно-приватного партнерства (ДПП) у сфері захисту КІ були зроблені після 9/11. Зокрема, у Плані захисту національної інфраструктури (2006) було визначено *Модель секторального партнерства* (Sector Partnership Model) як основу для координування діяльності щодо захисту критичної інфраструктури та ключових активів на всіх рівнях управління та в рамках усіх секторів КІ. У подальші роки в оновлених версіях цього державного документа зазначена модель уточнювалася та відшліфовувалася.

Відповідно до PPD-21, окрім секторів КІ та відповідальних за сектори, визначено *механізми та інструменти* забезпечення секторального та міжсекторального партнерства:

- урядові координувальні ради (Government Coordinating Councils), призначені для координування виконання урядових стратегій, програм та забезпечення зв'язків між урядовими органами;
- секторальні координувальні ради (Sector Coordinating Councils), що утворюються на добровільній основі та призначені для координації виконання стратегій і здійснення відповідної діяльності власників та операторів об'єктів і систем КІ;
- міжсекторальні ради (Cross-Sector Councils) – створено три структури: Партнерство для безпеки КІ (координує діяльність представників приватного сектору); Рада вищих федеральних керівників (Federal Senior Leadership Council), призначення якої – координувати інтереси федеральних органів; Рада координації діяльності штатів, місцевих органів управління, призначена для координації всіх інших державних органів нефедерального рівня.

Усі ці ради та відповідальні за сектори КІ агентства окремих секторів разом із федеральними органами управління, урядами штатів, регіональними і місцевими органами влади, приватним сектором і неурядовими організаціями повинні співпрацювати при виконанні програм та з метою реалізації підходів до забезпечення безпеки та стійкості КІ, досягнення пов'язаних із цим цілей.

США є лідером у запровадженні передових підходів, використанні новітніх технологічних рішень у розв'язанні проблем безпеки та стійкості КІ. Зазначені чинники зумовлюють теперішню ситуацію з *підготовкою кадрів і населення* за цим безпековим напрямом, яку можна охарактеризувати як бурхливий розвиток. У цій діяльності провідна роль суб'єктів належить МВБ, підтвердженням чого можна вважати різноманітність охоплення тем, інструментів і форматів, цільових аудиторій, які спостерігаються в діяльності цього міністерства. До найкращої національної практики в цьому питанні [60] слід віднести таке:

[60] Докладніше про підготовку кадрів і населення з питань захисту і стійкості критичної інфраструктури йдеться в підрозділах 2.5 та 3.6.

1. Увесь комплекс навчальних курсів та інших навчальних інструментів, а також відповідної інформації ділиться на два *основні модулі*: загальний (для всіх секторів КІ) та специфічний (для кожного окремого сектору).

2. *Загальний модуль* включає навчальні курси та інформаційні матеріали, що стосуються питань, актуальних до певної міри для всіх секторів КІ. При цьому зазвичай навчання та надання інформації для заходів та інструментів загального модуля здійснюється на безоплатній основі або за дуже низькими цінами.

3. *Специфічний модуль* обов'язково має включати навчальні заходи щодо підвищення інформованості з питань ЗКІ ключових суб'єктів цього процесу: представників державних органів, у т. ч. органів управління; правоохоронних органів; служб екстреної допомоги; власників та операторів об'єктів КІ тощо.

4. Активний розвиток *освітніх курсів* та інших навчальних інструментів з питань кібербезпеки КІ у рамках підготовки кадрів і населення.

Загалом, СЗБЗКІ у Сполучених Штатах активно розвивається. Відтак унаслідок ролі, яку відіграє країна у системі глобальної безпеки взагалі та у сфері захисту КІ зокрема, відповідним національним відомствам України було би доцільно постійно вивчати та аналізувати американський досвід у цій сфері.

2.1.2. Система забезпечення безпеки та стійкості критичної інфраструктури у Великій Британії

Правові засади створення державної системи БСКІ у Великій Британії. Уряд визначає *критичну структуру Великої Британії* як «ті критичні елементи інфраструктури (установки, системи, майданчики, об'єкти, власність, інформація, люди, мережі та процеси), втрата або порушення діяльності яких призвели б до серйозного негативного впливу на можливість отримання і надання або на цілісність важливих послуг, унаслідок чого можуть виникнути тяжкі наслідки для економіки і соціальної сфери або втрати життя людей» [61].

[61] Cabinet Office. Public Summary of Sector Security and Resilience Plans. (2017). URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/678927/Public_Summary_of_Sector_Security_and_Resilience_Plans_2017__FINAL_pdf___002_.pdf

Стійкість – це здатність активів, мереж та систем прогнозувати руйнівні події, переносити їх, адаптуватися до та швидко відновлюватися після них [62].

Слід зазначити, що попри існування у Сполученому Королівстві урядового *Центру захисту національної інфраструктури* [63] у британському законодавстві спеціальне визначення терміна «захист критичної інфраструктури» відсутнє. Останнім часом у контексті проблематики стосовно КІ переважно використовується термін «безпека КІ».

Основоположними стратегічними документами, що формують нормативно-правову базу для національної СЗБСКІ, у Великій Британії є такі чинні документи:

1) Стратегія національної безпеки (2010) [64];

2) урядова настанова «Забезпечення функціонування країни: Природні небезпеки та інфраструктура» (2011) [65];

3) Стратегія кібербезпеки Сполученого Королівства. Захист та сприяння Сполученого Королівства у цифровому світі (2011) [66];

4) Стратегічна національна основа стійкості громад (2011) [67];

5) Стратегічний огляд у сфері оборони та безпеки: захищене та процвітаюче Сполучене Королівство (2015) [68];

---

[62] *Див.*: Cabinet Office. Keeping the Country Running: Natural Hazards and Infrastructure. A Guide to improving the resilience of critical infrastructure and essential services (2011). URL: https://www.gov.uk/government/publications/keeping-the-country-running-natural-hazards-and-infrastructure

[63] Centre for the Protection of National Infrastructure. URL: https://www.cpni.gov.uk/

[64] A Strong Britain in an Age of Uncertainty: The National Security Strategy. (2010). URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

[65] Cabinet Office. Keeping the Country Running: Natural Hazards and Infrastructure. A Guide to improving the resilience of critical infrastructure and essential services (2011). URL: https://www.gov.uk/government/publications/keeping-the-country-running-natural-hazards-and-infrastructure

[66] The UK Cyber Security Strategy Protecting and promoting the UK in a digital world. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

[67] Strategic National Framework on Community Resilience. (2011). URL: https://m.oxfordshire.gov.uk/cms/sites/default/files/folders/documents/fireandpublicsafety/emergency/Strategic-NationalFramework.pdf

[68] National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom. (2015). URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/ attachment_data/file/555607/2015_Strategic_Defence_and_Security_Review.pdf

6) Національний реєстр ризиків цивільних надзвичайних ситуацій (2017) [69];
7) Відкрите резюме секторальних планів з питань безпеки та стійкості (2017)[70].

Стратегія національної безпеки (2010) та Стратегічний огляд у сфері оборони та безпеки (2015) визначають як пріоритетну необхідність підвищення безпеки та стійкості КІ щодо атак, руйнувань та шкоди. Серед широкого спектру загроз у цих стратегічних документах виокремлено загрози міжнародного тероризму, кібератак, серйозних аварій та природних лих як такі, що формують найбільш серйозні ризики для національної безпеки Великої Британії. Забезпечення безпеки найбільш важливих послуг, які надають державний та приватний сектори країни проти зазначених загроз та небезпек, визначено невід'ємною частиною Стратегії національної безпеки [71].

У Великій Британії перший урядовий документ, що стосувався безпеки національної КІ, було прийнято в 2011 р., у ньому було зроблено акцент переважно на небезпеках, які спричиняють природні лиха, насамперед повені. Подальші стратегічні та програмні документи, включно й згаданий вище Стратегічний огляд (2015), охопили всі види загроз, у т. ч. фізичні загрози, загрози персоналу та кібербезпеці.

Уряд здійснює оцінку загроз та небезпек щодо національної КІ, спираючись на неперервний цикл вивчення досвіду, винесеного з аналізу реальних подій у світі, та вдосконалюючи методи розрахунків ймовірності та можливих наслідків реалізації загроз і небезпек. Визначення діапазону загроз та небезпек національній КІ є критично важливим для вжиття необхідних безпекових заходів, з тим щоб останні були пропорційними, вчасними та ефективними.

За оцінкою *Центру захисту національної інфраструктури*, національна КІ може стати мішенню для нападів з боку ворожих держав, кіберзлочинців, терористів чи представників криміналітету

[69] National Risk Register Of Civil Emergencies. (2017). URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644968/UK_National_Risk_Register_2017.pdf

[70] Public Summary of Sector Security and Resilience Plans. (2017). URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/678927/Public_Summary_of_Sector_Security_and_Resilience_Plans_2017__FINAL_pdf___002_.pdf

[71] Там само.

з метою спричинення збоїв КІ, шпіонажу та/або отримання фінансової вигоди.

Відповідно до теперішньої оцінки вважається, що, хоча на нинішньому етапі терористична загроза національній КІ є в цілому обмеженою, *Сектор транспорту* продовжує стикатися з постійно високим рівнем загрози з боку міжнародного тероризму. Крім того, *Сектор служб невідкладної допомоги* та *Сектор оборони* (конкретно, поліція та військовослужбовці) також перебувають під загрозою високого рівня. Терористична загроза постійно змінюється, тому наміри та можливості терористичних угруповань вразити національну КІ, швидше за все, будуть еволюціонувати.

Згідно з оцінкою *Національного центру кібербезпеки* кіберзагрози національній КІ постійно зростають. Ворожі держави та кіберзлочинці можуть спробувати здійснити атаки на організації та національну інфраструктуру Сполученого Королівства задля здійснення їхніх планів та отримання вигоди. Це може бути зроблено шляхом шпіонажу, викрадення та викривлення даних або шляхом використання хакерських програм, вимог викупу тощо.

Велика Британія враховує різноманітні *природні небезпеки* (наприклад, повені, екстремальні погодні умови, шторми), а також соціальні заворушення та соціальні фактори, спричинені, зокрема, *епідеміями* грипу та іншими обставинами, що переривають надання важливих послуг або суттєво зменшують їх обсяг.

Нині основою діяльності щодо КІ є *секторальні плани з питань безпеки та стійкості*, або *СПБС* (Sector Security and Resilience Plans, SSRPs) [72]. Таку назву плани отримали в 2015 р. Повні тексти секторальних планів є засекреченими, але уряд Великої Британії щорічно публікує в стислому вигляді відкриті версії зазначених документів, щоб інформувати все суспільство щодо заходів, які вживаються у кожному із секторів для підвищення рівня безпеки та стійкості КІ.

Організаційні засади створення державної системи БСКІ у Великій Британії. На вершині управлінської піраміди щодо національної КІ перебуває *Секретаріат Кабінету міністрів* (Cabinet Office), який організовує відповідну діяльність, спираючись на секторальну

[72] Перші секторальні плани стосувалися лише загроз повенів і мали назву Секторальні плани з питань стійкості (Sector Resilience Plans). Питання фізичної безпеки і кібербезпеки були включені до них у 2015 р.

структуру державної системи БСКІ та згадані вище секторальні плани з питань безпеки та стійкості.

Плани розробляються *провідними урядовими органами* (Lead Government Departments, LGDs), на які покладена відповідальність за розробку (включно й законодавче забезпечення) і реалізацію державної політики на рівні сектору щодо БСКІ, підготовку секторальних планів, якими визначаються ризики та основні заходи, спрямовані на їх зменшення протягом наступних років. До розробки планів залучаються інші суб'єкти СЗБСКІ.

Структура системи забезпечення БСКІ Великої Британії включає 13 секторів КІ, три з яких додатково поділені на 15 підсекторів. Діяльність щодо безпеки та стійкості КІ у рамках зазначених секторів та підсекторів координують 11 провідних урядових органів (переважно міністерств). Сектори, підсектори та провідні урядові органи представлені нижче у *табл. 2.2*.

Таблиця 2.2. **Сектори КІ та провідні державні органи Великої Британії, відповідальні за їх стійкість**

Сектор	Підсектор (-и)	Провідний урядовий орган, відповідальний за стійкість
Хімічний		Міністерство з питань бізнесу, іновацій і кваліфікованих кадрів (Department for Business, Innovation and Skils)
Цивільний ядерний		Міністерство з питань енергетики та змін клімату (Department of Energy and Climate Change)
Зв'язку	Мовлення (теле- і радіо-)	Міністерство з питань культури, засобів масової інформації та спорту (Department for Culture, Media and Sport)
	Телекомунікаційний	
	Інтернет	
	Поштовий	
Оборони		Міністерство оборони (Ministry of Defence)

Продовження табл. 2.2

Сектор	Підсектор (-и)	Провідний урядовий орган, відповідальний за стійкість
Служби невідкладної допомоги	Невідкладна медична допомога	Міністерство охорони здоров'я (Department of Health)
	Берегова охорона	Міністерство транспорту (Department for Transport)
	Протипожежна та рятувальна служба	Міністерство з питань громад та місцевих органів влади (Department for Communities and Local Government)
	Поліція	Міністерство внутрішніх справ (Home Office)
Енергетика	Електроенергія	Міністерство з питань енергетики та змін клімату (Department of Energy and Climate Change)
	Газ	
	Нафта	
Фінансовий		Казначейство (HM Treasury)
Продовольства		Міністерство з питань навколишнього середовища, продовольства та сільського господарства (Department for Environment, Food and Rural Affairs)
Урядовий		Секретаріат Кабінету міністрів (Cabinet Office)
Охорони здоров'я		Міністерство охорони здоров'я (Department of Health)
Космічний		Міністерство з питань бізнесу, іновацій і кваліфікованих кадрів (Department for Business, Innovation and Skils)
Транспорту	Авіаційний транспорт	Міністерство транспорту (Department for Transport)
	Порти	
	Залізничний транспорт	
	Автомобільний транспорт	
Водопостачання		Міністерство з питань навколишнього середовища, продовольства та сільського господарства (Department for Environment, Food and Rural Affairs)

Джерело: складено автором за інформацією сайту Центру захисту критичної інфраструктури (Centre for the Protection of National Infrastructure) (див.: URL: https://www.cpni.gov.uk/critical-national-infrastructure-0).

Відповідальність за повсякденне функціонування національної КІ, забезпечення безпеки та стійкості відповідних активів, у т. ч. оцінку ризиків, прийняття рішень, навчання і тренування персоналу, відповідні інвестиції тощо, несуть *власники та оператори* цих активів.

Відповідно до Закону про надзвичайні ситуації 2004 р. місцеві органи влади та служби невідкладної допомоги повинні визначити, оцінити ймовірність та наслідки можливих надзвичайних ситуацій, у т. ч. тих, що пов'язані з інфраструктурою, та розробити плани реагування у рамках своїх повноважень на такі надзвичайні ситуації.

Кілька *урядових агентств* надають центральному уряду, регуляторам, а також власникам та операторам консультації й рекомендації щодо безпеки та стійкості КІ, зокрема стосовно ризиків і заходів, спрямованих на їх зменшення. До цих агентств належать уже згадуваний *Центр захисту національної інфраструктури*, який консультує з питань фізичної безпеки та безпеки персоналу з метою мінімізації ризиків та уразливостей щодо загроз тероризму, шпіонажу та інших загроз національній безпеці. До цієї ж категорії агентств належить і *Національний центр кібербезпеки* [73], головним завданням якого є зменшення ризиків для кібербезпеки Великої Британії, у т. ч. через співпрацю з бізнесом та окремими громадянами шляхом надання їм надійних та узгоджених консультацій з кібербезпеки, управління кіберінцидентами.

На *регуляторів* покладено завдання підтримувати провідні урядові органи через забезпечення виконання відповідних нормативно-правових актів, наприклад, через контроль виконання ліцензійних умов на об'єктах КІ.

У частині координації дій та обміну інформацією Стратегія національної безпеки та Стратегічний огляд у сфері оборони та безпеки (2015) вказують на необхідність продовження розвитку та вдосконалення координації між місцевим і національними рівнями реагування; підтримки обміну інформацією та досвідом участі в реальних подіях і навчаннях між організаціями, залученими до планування реагування; важливість запровадження платформ для обміну цифровою інформацією тощо.

До цієї ж категорії заходів та інструментів можна віднести ініціативу *Партнерства з обміну інформацією щодо кібербезпеки* [74], спільно

[73] National Cyber Security Centre (NCSC). URL: https://www.ncsc.gov.uk/

[74] Cyber Security Information Sharing Partnership (CiSP). URL: https://www.ncsc.gov.uk/cisp

започатковану урядом та промисловістю задля обміну інформацією через захищені конфіденційні канали в умовах динамічних змін у безпековому середовищі з метою оцінки ризиків, планування та підтримки взаємодії.

Згідно із секторальними планами забезпечення безпеки та стійкості КІ відповідальними за навчання та тренування персоналу визначені оператори та власники об'єктів і систем.

Централізовану інформаційно-консультативну та методологічну допомогу всім суб'єктам системи БСКІ надають *спеціалізовані урядові установи*. Зокрема, для сприяння персоналу організацій у виявленні «незвичної та несподіванної поведінки на робочому місці, а також в інформуванні про неї» Центр захисту національної інфраструктури розробив овсвітню програму «Буде правильно повідомити» [75]. Інший приклад роботи центру – Настанова з проведення кампанії з підвищення пильності [76]. У своїй діяльності за цим напрямом фахівці Центру використовують різноманітні інструменти, включно детальні інструкції, слайди, анімаційні матеріали, постери, попереджувальні картки тощо.

У зв'язку із різким загостренням проблем кібербезпеки активну роботу з надання освітніх та навчальних послуг, у т. ч. щодо КІ, провадить *Національний центр кібербезпеки*. Центром, серед іншого, розроблені настанови щодо забезпечення кібербезпеки організацій державного сектору, йдеться про центральний уряд та місцеві органи влади, медичні та соціальні служби, служби невідкладної допомоги та ін. Зазначений Центр підготував низку настанов і рекомендацій, які сприяють самостійній діяльності організацій та підприємств, спрямованій на підвищення кібербезпеки. Серед таких матеріалів можна назвати: «10 кроків до кібербезпеки»[77], «Настанова для кінцевого користувача приладу»[78], «Принципи хмарної безпеки»[79] тощо.

[75] It's OK to say / Education Programme Overview. (n. d.). URL: https://www.cpni.gov.uk/system/files/documents/d7/92/IOTS-Programme-Overview.pdf

[76] Running a Staff Vigilance Campaign. (n. d.). URL: https://www.cpni.gov.uk/system/files/documents/53/50/Running%20a%20staff%20vigilance%20campaign.pdf

[77] Guidance: 10 Steps to Cyber Security. (n. d.). URL: https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

[78] End User Devices Security Guidance: Introduction. (n. d.). URL: https://www.ncsc.gov.uk/guidance/end-user-devices-security-guidance-introduction-0

[79] Guidance: Cloud Security Collection. (n. d.). URL: https://www.ncsc.gov.uk/guidance/cloud-security-collection

На відміну від Сполучених Штатів, у Великій Британії об'єднання зусиль державних органів та інших суб'єктів процесу забезпечення безпеки та стійкості КІ вирішується, головним чином, через *забезпечення стійкості місцевих громад та безперервності ведення бізнесу*. Принципи розбудови стійкості місцевих громад та компаній були сформульовані в урядовому документі Стратегічні національні основи стійкості громад (2011) [80], де акцент зроблено на стійкості окремих громад, організацій, а також на індивідуальній стійкості осіб, що є членами громад та організацій.

2.1.3. Система забезпечення безпеки та стійкості критичної інфраструктури у Польщі

Правові засади створення державної системи захисту критичної інфраструктури у Польщі. До основних нормативно-правових актів, які врегульовують ті чи ті аспекти функціонування національної системи захисту КІ в Польщі належать:

1. Стратегія національної безпеки Республіки Польща 2014 [81]. Захисту КІ спеціально присвячений 86-й пункт цього документа. У ньому підкреслено, що КІ включає ключові системи та елементи, функціонування яких гарантує безпеку держави та її громадян. Документом визначено, що захист КІ є обов'язком операторів і власників, підтримку яким надає держава. Стратегія націлює на запровадження інноваційного підходу, в основу якого покладено розподілену відповідальність, широке співробітництво та взаємну довіру.

2. Стратегія розвитку системи національної безпеки Республіки Польща до 2022 року [82] визначає, що третя (з п'яти) стратегічних цілей для країни полягає у «розвитку стійкості стосовно загроз національній безпеці, включно й надзвичайні ситуації та неочікувані події… Ця ціль має бути досягнута головним чином через посилення захисту критичної інфраструктури та розбудову системи стратегічних ресурсів».

[80] Strategic National Framework on Community Resilience. (2011). URL: https://m.oxfordshire.gov.uk/cms/sites/default/files/folders/documents/fireandpublicsafety/emergency/StrategicNationalFramework.pdf

[81] The National Security Strategy of the Republic of Poland. (2014). URL: https://www.bbn.gov.pl/ftp/dok/NSS_RP.pdf

[82] The Strategy of Development of the National Security System of the Republic of Poland 2022. URL: http://en-m.mon.gov.pl/p/pliki/dokumenty/rozne/2014/01/ENGLISH_SRSBN_RP_do_pobrania.pdf

3. Закон «Про кризове управління» [83] від 26 квітня 2007 р. (зі змінами і доповненнями, внесеними у 2013 та 2015 рр.). У цьому законі визначені основні обов'язки посадових осіб і державних органів стосовно захисту КІ, а також низка базових для цієї сфери термінів.

4. Національна програма захисту критичної інфраструктури 2015 [84]. Національні програми захисту КІ (попередня версія датована 2013 р.) є інструментом реалізації державної політики Польщі в цій сфері. Чинна редакція програми від 2015 р. містить також визначення низки специфічних для сфери захисту КІ термінів.

5. Постанова Ради Міністрів «Про Національну програму захисту критичної інфраструктури» [85] від 30 квітня 2010 р., якою визначені процедури та механізми розробки, затвердження, обслуговування й реалізації національних програм, розписані відповідні ролі, повноваження та сфери відповідальності координаційного органу – Урядового центру безпеки, залучених державних органів, операторів/власників тощо.

6. Постанова Ради Міністрів «Про плани захисту критичної інфраструктури» [86] від 30 квітня 2010 р., якою встановлені вимоги до структури, змісту, строків подання і затвердження, підстав для відхилення планів захисту критичної інфраструктури, що їх оператори систем КІ повинні подавати до Урядового центру безпеки.

7. Закон «Про антитерористичну діяльність та поправки до інших законів» (2016) [87], яким врегульовані питання захисту КІ стосовно терористичних загроз.

8. Закон про захист осіб та власності від 22 серпня 1997 р. (із змінами і доповненнями) [88].

---

[83] The Act of 26 April 2007 on Crisis Management. URL: https://rcb.gov.pl/wp-content/uploads/WERYF_-ACT_Crisis_Management_English-1.pdf_

[84] The National Critical Infrastructure Protection Programme 2015. URL: http://rcb.gov.pl/wp-content/uploads/NPOIK-2015_eng-1.pdf

[85] Regulation of the Council of Ministers of 30 April 2010 on National Critical Infrastructure Protection Programme. URL: http://rcb.gov.pl/wp-content/uploads/REGULATION-on-NATIONAL-CRITICAL-INFRASTRUCTURE-PROTECTION-PROGRAMME-AB.pdf

[86] Там само.

[87] Act of 10 June 2016 on Anti-Terrorist Activities and on the Amendments to Other Acts. URL: http://www.legislationline.org/download/action/download/id/6361/file/Poland_Act_on%20_anti-terrorist%20_activities_2016_en.pdf

[88] Act of 22 August, 1997 on protection of persons and property. (2005). *Journal of Laws of the Republic of Poland*. No. 145. Item 1221.

Функціонування системи захисту КІ в Польщі регулюється кількома основними документами. Зокрема, визначальним серед них є Закон про кризове управління [89] від 26 квітня 2007 р., до якого в 2013 та 2015 рр. вносилися поправки. Безпосередньо у цьому законі не зазначено, чому саме в цей час на національному рівні розпочалася робота із захисту КІ в Польщі. Але, ураховуючи те, що у ЄС активна діяльність із розробки стратегічних документів щодо захисту КІ розпочалася в середині 2004 р., можна з упевненістю стверджувати, що саме поворот до цієї проблематики на рівні керівних органів ЄС і започаткував створення національних систем ЗКІ у східноєвропейських країнах – членах ЄС, таких як Польща, Чехія, Угорщина, Болгарія, де рівень терористичних загроз був суттєво нижчим, ніж у Франції, Іспанії, Великій Британії, Німеччині.

У законодавстві Польщі є такі визначення основних термінів, що стосуються КІ.

Так, зазначається, що під *критичною інфраструктурою* слід розуміти системи та взаємопов'язані функціональні об'єкти, які входять до цих систем, включно споруди, установки, обладнання, а також послуги, критично важливі для безпеки держави та її громадян, а також для ефективного функціонування органів державного управління, установ та підприємств.

Критична інфраструктура включає [90] (надається перелік 11 секторів):

a) енергетичні системи, системи постачання палива та енергетичних ресурсів;
b) системи зв'язку;
c) систем телеінформаційних мереж;
d) фінансові системи;
e) системи постачання продуктів харчування;
f) системи водопостачання;
g) системи охорони здоров'я;
h) транспортні системи;
i) аварійно-рятувальні системи;

[89] The Act of 26 April 2007 on Crisis Management. URL: https://rcb.gov.pl/wp-content/uploads/WERYF_-ACT_Crisis_Management_English-1.pdf

[90] У національному законодавстві Польщі щодо КІ не використовується термін «сектор». Таким чином, у наведеному визначенні фактично нададається перелік секторів національної КІ у тому розумінні, яке прийнято у більшості країн – членів НАТО та ЄС.

j) системи забезпечення неперервності функціонування державної влади;
k) системи виробництва, зберігання та використання хімічних та радіоактивних речовин, трубопроводи для небезпечних речовин.

Під *захистом критичної інфраструктури* слід розуміти всі заходи, що мають на меті забезпечення функціональності, неперервності та цілісності роботи критичної інфраструктури для запобігання загрозам, ризикам або вразливостям, а також для обмеження та нейтралізації їхнього впливу і для швидкого відновлення інфраструктури у випадку збоїв, нападів та інших подій, які порушують її належне функціонування.

Крім цього, важливі для сфери захисту КІ терміни, у т. ч. й ті, що визначені іншими нормативно-правовими актами, представлені у чинній Національній програмі захисту критичної інфраструктури 2015 [91], а саме:

- *координатор системи КІ*;
- *оператор КІ*;
- *кризова ситуація*;
- *обов'язковий захист* (стосується захисту важливих для оборони, економіки держави і безпеки населення об'єктів);
- *спеціальний захист* (стосується захисту особливо важливих для безпеки і оборони держави об'єктів).

Державна політика Республіки Польща у сфері захисту КІ спрямована на досягнення найважливішої цілі – підвищення рівня безпеки держави. Для цього мають бути виконані такі важливі завдання:

- досягнення певного рівня усвідомлення, обізнаності та компетенції всіх суб'єктів забезпечення захисту КІ щодо значення КІ для ефективного функціонування держави;
- запровадження методології оцінки ризиків з урахуванням всіх видів загроз КІ, у т. ч. й щодо ризиків з низькою ймовірністю реалізації, але з катастрофічними наслідками;
- запровадження координації при виконанні завдань, визначених унаслідок оцінки ризиків;
- розбудова партнерства учасників забезпечення захисту КІ.

[91] The National Critical Infrastructure Protection Programme 2015. (2015). URL: http://rcb.gov.pl/wp-content/uploads/NPOIK-2015_eng-1.pdf

Особливістю виконання *Національної програми захисту критичної інфраструктури* (далі – *Національна програма*) в Польщі є те, що цей документ базується на безсанкційному (sanction-free) підході як інструменті досягнення балансу між регулювальним впливом держави та витратами на підвищення безпеки КІ, які мають нести її оператори/власники. Проте уряд Польщі залишив за собою право змінити цей підхід, якщо він не буде забезпечувати необхідний рівень безпеки КІ.

Найбільш важливі засади реалізації Національної програми:

- *розділена відповідальність*, яку було встановлено під час створення системи захисту КІ, ураховуючи важливість безпеки критичної інфраструктури як для функціонування державних органів, так і для операторів КІ, суспільства, економіки та держави як такої;
- *співробітництво*, що передбачає спільне виконання суб'єктами захисту КІ певних завдань, необхідність цього випливає із численних та взаємопов'язаних завдань, які необхідно виконувати, забезпечуючи при цьому ефективне використання наявних можливостей і ресурсів;
- *довіра*, яка має бути встановлена насамперед між державою та операторами КІ, зважаючи на те, що вони мають спільні цілі – досягнення національної безпеки та безпеки КІ.

2.1.4. Висновки для України з огляду на зарубіжний досвід щодо державної системи забезпечення безпеки та стійкості критичної інфраструктури

Викладений вище огляд національних підходів до забезпечення БСКІ дозволяє сформулювати такі основні висновки щодо побудови аналогічної системи в Україні:

1. Попри наявність загальновизнаних принципів та підходів щодо забезпечення БСКІ кожна національна система є по суті унікальною і неминуче несе на собі відбиток національної специфіки, тому слід уникати механічного копіювання зарубіжного досвіду на українських теренах.

2. Разом із тим, для більшості розвинутих країн, насамперед країн – членів ЄС та НАТО, загальновизнаними є низка *осново-*

положних підходів і принципів, які реалізуються при створенні системи БСКІ з тими чи тими варіаціями залежно від конкретних умов:

1) безпека та стійкість КІ належать до пріоритетних завдань секторів національної безпеки і оборони, а відповідна діяльність урегульовується цілою низкою нормативно-правових актів, у т. ч. національного рівня;

2) забезпечення БСКІ здійснюється на системній основі, тобто шляхом створення відповідних національних (державних) систем;

3) системи БСКІ, що створюються, призначені забезпечувати безпеку та стійкість щодо всіх видів фізичних загроз та кіберзагроз;

4) національні системи БСКІ для забезпечення виконання поставлених перед ними цілей повинні:

- удосконалювати механізми та процедури ВОІ на всіх рівнях управління, функціонувати на основі ризик-орієнтованих підходів, чіткого розподілу повноважень і відповідальності щодо КІ (для цього зазвичай визначають відповідальний державний орган або органи);
- розвивати ДПП, взаємодію з іншими суб'єктами системи з метою ефективного залучення населення, суспільства, бізнесу та державних установ і організацій до розв'язання проблем забезпечення БСКІ;
- налагоджувати ефективний обмін інформацією між усіма суб'єктами процесу забезпечення БСКІ;
- забезпечувати виконання функцій інтегрування та аналізу даних для підтримки процесів планування та прийняття рішень стосовно КІ;
- проводити підготовку кадрів і населення для забезпечення БСКІ;
- постійно перевіряти готовність сил і засобів, планів і процедур ВОІ під час регулярних навчань на всіх рівнях управління.

2.2. Розвиток законодавства ЄС у сфері безпеки енергопостачання

Те, як відбувається пошук шляхів формалізації вимог до учасників системи щодо забезпечення БСКІ, може бути продемонстровано на прикладі поступового вдосконалення законодавства ЄС щодо безпеки функціонування *критичної енергетичної інфраструктури*.

Таке завдання зумовлено суттєвим ускладненням балансування різносторонніх інтересів між суб'єктами господарювання, що працюють на енергетичних ринках, операторів (власників) критичної енергетичної інфраструктури та державою внаслідок розширення кола учасників ринків, їх взаємозв'язаності та зростання рівня глобалізації.

Пошук шляхів унормування підходів до забезпечення стійкості функціонування енергетики також мотивувався загрозами, породженими гібридними методами ведення війн нового покоління, зокрема використанням енергетики (енергопостачання) як інструменту досягнення політичних цілей окремими країнами [92].

У відповідь на нові виклики розпочалось активне формування вимог щодо забезпечення безпеки та стійкості критичної енергетичної інфраструктури. Зокрема, у ЄС було прийнято важливі директиви та регламенти, які передбачали розроблення низки механізмів запобігання виникнення кризових ситуацій та застосування інструментарію, що виходить далеко за межі чисто технічних заходів оператора енергетичних систем.

Так, у 2004 р. була прийнята Директива Ради ЄС щодо заходів забезпечення безпеки постачання природного газу [93], яка пізніше деталізувалась та посилювалася через регламенти ЄС, зокрема в 2010 [94] та 2017 рр. [95]. У 2006 р. було прийнято Директиву Парламенту та Ради ЄС щодо заходів забезпечення безпеки електропостачання

[92] О. Суходоля. «Енергетична зброя» в умовах гібридної війни // Світова гібридна війна: український фронт / за ред. Горбуліна В. П. Київ: НІСД, 2017. 496 с. С. 291–300.

[93] Council Directive 2004/67/EC of 26 April 2004 Concerning Measures to Safeguard Security of Natural Gas Supply. URL: http://eur-lex.europa.eu/eli/dir/2004/67/oj

[94] REGULATION (EU) 994/2010 of the European Parliament and of the Council of 20 October 2010 Concerning Measures to Safeguard Security of Gas Supply and Repealing Council Directive 2004/67/EC. URL: http://eur-lex.europa.eu/eli/reg/2010/994/oj

[95] REGULATION (EU) 1938/2017 of the European Parliament and of the Council of 25 October 2017 Concerning Measures to Safeguard the Security of Gas Supply and Repealing Regulation (EU) 994/2010. URL: http://eur-lex.europa.eu/eli/reg/2017/1938/oj

та інвестицій в інфраструктуру [96], яка, як очікується, буде уточнена в 2019 р. шляхом прийняття Регламенту ЄС щодо підготовки електроенергетичного сектору до ризиків реалізації різних загроз [97].

Загалом слід відзначити позитивний вплив України (на жаль, негативного для самої нашої держави досвіду) на розвиток концептуальних засад та механізмів забезпечення стійкості енергетичних систем ЄС. Перші директиви ЄС із цього питання були прийняті внаслідок загроз та проблем ЄС, породжених станом ринкового регулювання в Україні та кризою відносин між Україною та Росією в 2004–2006 рр. Наступне вдосконалення законодавства та механізмів реагування ЄС на кризові ситуації відбувалося за результатами вивчення уроків криз, зумовлених використанням «енергетичної зброї» Росією проти України (другої газової війни 2009 р. та гібридної війни, активна фаза якої розпочалася в 2013–2014 рр.).

Усвідомивши загрози стійкості функціонування енергетичних систем «не технічного» плану, ЄС запровадив низку механізмів «раннього попередження», «координації та обміну інформацією», «планування запобігання, реагування та функціонування у кризових ситуаціях» тощо.

Директива № 67/2004 з метою координації зусиль Співтовариства для забезпечення безпеки постачання газу на випадок значного переривання поставок, створювала *Газову координаційну групу* (the Gas Coordination Group). Група також ставала механізмом регулярного аналізу постачання та обміну інформацією щодо загроз постачанню газу. Також передбачалося створення триетапного механізму попередження криз: заходи, що будуть застосовуватись підприємствами газопостачання; заходи національного рівня та на рівні Співтовариства, якщо попередні заходи не могли виправити ситуацію.

Однак Директива потребувала прийняття національного законодавства країнами – членами ЄС, що не завжди виконувалося. Цю проблему було актуалізовано другою газовою війною у 2009 р., що призвело до посилення законодавчого регулювання цієї сфери,

[96] DIRECTIVE 89/2005/EC of the European Parliament and of the Council of 18 January 2006 Concerning Measures to Safeguard Security of Electricity Supply and Infrastructure Investment. URL: http://eur-lex.europa.eu/eli/dir/2005/89/oj

[97] Proposal for a REGULATION of the European Parliament and of the Council on Risk-Preparedness in the Electricity Sector and Repealing Directive 2005/89/EC. Brussels, 30.11.2016. COM(2016) 862 final. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0862

шляхом прийняття регламентів ЄС, які мають пряму дію для всіх країн та якими було запропоновано нові механізми забезпечення безпеки постачання.

Регламент № 994/2010 вимагав ще й призначення відповідальних за реалізацію заходів компетентних органів. Передбачалося також розроблення на основі ризик-аналізу *Плану попередження криз* та *Плану дій на випадок криз* і визначались дії всіх залучених осіб, а також регулярний моніторинг безпеки постачання на національному рівні. Також передбачалося затвердження інфраструктурних стандартів та стандартів безпеки постачання, які, серед іншого, включали заходи щодо формування додаткових потужностей та об'ємів (запасів) чи напрямів транспортування, укладання додаткових контрактів на постачання (чи продаж із сховищ додаткових об'ємів) та контрактів із споживачами, що дозволяли переривання постачання, а також різні технічні та організаційні рішення. Встановлювались вимоги щодо ризик-аналізу, критерії безпеки постачання й рівні та механізми кризового реагування.

Регламент, прийнятий наприкінці 2017 р. (№ 1938/2017), передбачав уже детальну регламентацію змісту *Плану попередження криз* та *Плану дій на випадок криз*, процедур залучення приватного сектору до реагування на випадок криз; визначення критеріїв рівнів кризової ситуації та встановлення вимог щодо застосування різних механізмів реагування залежно від рівня кризи; процедури взаємодопомоги різних учасників (країн, підприємств галузі, споживачів) на рівні регіонів та загалом ЄС.

У сфері електроенергетики відбувались аналогічні процеси. Прийнята Директива № 89/2005 визначала межі забезпечення безпеки електропостачання та інвестування в електроенергетичну інфраструктуру. Ця Директива стосувалася переважно технічних аспектів забезпечення стійкості функціонування енергосистем країнчленів та розширення зв'язків між системами з метою зняття обмежень національних кордонів для розвитку спільного ринку електроенергії Співтовариства та підвищення рівня безпеки електропостачання у випадку кризових ситуацій. У 2012 р. у ЄС була створена також експертна *Електроенергетична координаційна група* (the Electricity Coordination Group), яка стала форумом сприяння обміну інформацією та координації зусиль щодо забезпечення безпеки електропостачання.

Зазначена Директива до 2014 р. була переважно виконана країнами-членами шляхом урегулювання окремих завдань у рамках інших директив щодо організації ринку електроенергії та функціонування системного оператора. Ураховуючи досвід розвитку законодавства в газовій сфері та уроки гібридної війни Росії проти України та ЄС, у 2016 р. на заміну Директиві № 89/2005 було підготовлено проект Регламенту з фокусом на специфічних безпекових завданнях, а саме: запобігання виникненню кризових ситуацій у секторі та управлінням ними.

Регламент (прийняття планувалося на 2019 р.) також суттєво посилює вимоги до учасників ринку електроенергії щодо готовності до криз (запобігання виникнення, функціонування під час та відновлення нормального режиму після ліквідації криз), спричинених загрозами різного типу та їх комбінаціями. Зокрема, передбачається встановлення загальної методології визначення кризових сценаріїв, узгодження національних планів щодо готовності до криз, що містять національні й регіональні заходи та регіональне співробітництво. Визначаються процедури обміну інформацією та координації зусиль, правила та відповідальність за проведення ризик-аналізу, а також вимоги до оцінки ресурсної адекватності (достатності потужностей, гнучкості та запасів для балансування коливань виробництва/споживання електроенергії).

Загальний огляд удосконалення законодавства ЄС щодо забезпечення БСКІ одного із ключових секторів КІ свідчить про те, що ЄС послідовно розвиває своє законодавство з питань забезпечення БСКІ та безпеки цільової функції (послуги), яку ця інфраструктура забезпечує. Зокрема, у частині безпеки енергопостачання спостерігається поступове посилення вимог до учасників системи енергозабезпечення, формалізація зазначених вимог у законодавстві, а також координація зусиль різних учасників для запобігання до, реагування на та відновлення функціонування КІ після виникнення кризової ситуації.

Можна виокремити такі механізми забезпечення стійкості функціонування енергетичних систем, які вимагаються до застосування у ЄС:

- визначення компетентного органу з питань безпеки постачання, його завдань та повноважень, тобто призначення відповідального за загальну методологію реагування та контактної точки у процесі прийняття рішень;

- залучення широкого кола учасників та застосування механізмів взаємодопомоги, тобто визнання на політичному рівні пріоритетності енергозабезпечення споживачів та можливості використання ресурсів учасників енергетичних ринків (у т. ч. суміжних) на доповнення до заходів та компетенції оператора енергосистем;
- здійснення ризик-аналізу [98] та розроблення можливих кризових сценаріїв функціонування енергосистем (вищим рівнем управління – національним компетентним органом або спеціалізованим галузевим органом на рівні ЄС визначення рівня загроз, на які мають бути розраховані заходи забезпечення безпеки енергопостачання з точки зору більшої системи;
- розроблення Плану запобігання виникнення криз [99] та Плану дій на випадок криз [100] з урахуванням залучення до заходів широкого кола учасників енергетичного ринку та застосування механізмів взаємодопомоги, виділення етапів «проектної готовності» та «надзвичайної ситуації»;
- розроблення стандартів операційної безпеки системних операторів, «планів запобігання» та «планів дій на випадок», формалізація вимог до змісту діяльності учасників ринку відповідно до можливого рівня кризової ситуації (рівня та кола загроз), переліку заходів (у межах «проектних» механізмів регулювання ринку та «позапроектних» обмежувальних) тощо;
- визначення критеріїв оцінки рівня загроз та процедур прийняття рішень щодо застосування «проектних» та «позапроектних» механізмів реагування на виникнення кризових ситуацій, порядку та процедур прийняття рішення щодо застосування заздалегідь визначених заходів реагування;
- забезпечення обміну інформацією та координації зусиль учасників ринку з питань забезпечення безпеки постачання, формування контактних точок та регламентів і форм обміну інформацією та прийняття рішень у різних режимах функціонування енергосистем;

[98] Типова структура та вимоги щодо ризик-аналізу наведені у *Додатку 3.*

[99] Типова структура та вимоги щодо Плану запобігання виникнення криз наведені у *Додатку 1*.

[100] Типова структура та вимоги щодо Плану дій на випадок криз наведені у *Додатку 2*.

- проведення періодичних тестувань готовності до криз, створення механізму навчання та перевірки готовності учасників до реагування на кризові ситуації;
- транскордонне співробітництво та взаємодопомога (тісна координація країн-членів та системних операторів на регіональному рівні та рівні ЄС).

Слід відзначити, що подібні підходи щодо забезпечення стійкості функціонування енергетичної інфраструктури повністю узгоджуються із підходами НІСД, які закладені у створення державної системи захисту критичної інфраструктури [101]. Детальніше пропозиції щодо розбудови інструментарію забезпечення безпеки та стійкості критичної енергетичної інфраструктури висвітлено в підрозділі 3.1, також у типовій структурі та вимогах до відповідних планів у *додатках 1–3*.

2.3. Планування у забезпеченні безпеки критичної інфраструктури

Відповідно до сучасних підходів національна критична інфраструктура включає різноманітні об'єкти, системи і мережі (як фізичні, так і віртуальні), які є настільки важливими для життєдіяльності країни, що їх знищення або ведення з ладу (повне або часткове) можуть призвести до швидких тяжких наслідків для населення, суспільства і держави в цілому.

Масштаб і комплексний характер наслідків криз, пов'язаних із необхідністю забезпечення БСКІ щодо всіх видів загроз, гостро ставлять на порядок денний питання забезпечення необхідного рівня координації дій, взаємодії та обміну інформацією між численними суб'єктами процесу реагування [102].

Відтак буде доцільно коротко розглянути прогресивний зарубіжний досвід у цій сфері (насамперед на прикладі США як безумовного

[101] Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету Міністрів України від 06.12.2017 № 1009-р // База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/go/1009-2017-%D1%80

[102] У цьому контексті поняття «реагування» включає забезпечення готовності до реагування, безпосередньо дії відповідних суб'єктів процесу під час реагування на інцидент або кризу, пов'язану з безпекою об'єкта КІ, а також ліквідацію та/або пом'якшення наслідків кризи.

лідера у запровадженні сучасних підходів до БСКІ, а також у сфері кризового реагування [103]), проаналізувати ситуацію в Україні з точки зору відповідності чинних систем реагування у кризових та надзвичайних ситуаціях сучасним підходам до захисту КІ та, зважаючи на викладене, запропонувати деякі рекомендації щодо заходів, спрямованих на посилення можливостей України у сфері реагування на безпекові інциденти та кризи, пов'язані з об'єктами КІ.

Перед детальним оглядом досвіду США в означеній сфері варто зупинитися на деяких посутніх термінологічних визначеннях, що даються Федеральним агентством США з надзвичайних ситуацій [104].

Національна система готовності (НСГ, National Preparedness System, NPS). Ціль НСГ полягає у підвищенні рівня безпеки та посиленні стійкості США шляхом системної підготовки до реагування на загрози, які пов'язані з найбільшими ризиками для національної безпеки. У рамках НСГ визначені п'ять місій: (1) запобігання; (2) захист; (3) пом'якшення наслідків; (4) реагування; (5) відновлення.

До ключових документів, які пов'язані з НСГ, слід віднести:

Ціль національної готовності (ЦНГ, National Preparedness Goal, NPG) – визначає основні засоби та можливості для кожної місії.

Концептуальні основи національного планування (КОНП, National Planning Frameworks, NPF) – формулює стратегію та доктрину побудови, надійного функціонування та надання основних засобів та можливостей, необхідних для досягнення ЦНГ.

Федеральні міжвідомчі оперативні плани (ФМОП, Federal Interagency Operational Plans, FIOP) – розробляються на основі КОНП і являють собою концепцію операцій, що застосовуються для інтегрування та синхронізації існуючих федеральних засобів та можливостей, які призначені для підтримки планів місцевих органів, штатів, племен, територій тощо, а також федеральних планів. ФМОП, при необхідності, підтримуються Федеральними оперативними планами міністерського рівня.

---

[103] Під *системами кризового реагування* будемо розуміти всі національні (державні) системи, які забезпечують реагування суб'єктів процесу реагування на безпекові інциденти та кризи різного походження.

[104] National Planning System / Fact Sheet. URL: https://www.fema.gov/media-library-data/1454437367834-69ac2b642e9e34945b903455dcbde679/NPLANS_Fact_Sheet_011916_For508.pdf

2.3.1. Планування реагування на загрози критичної інфраструктури за умови забезпечення її безпеки та стійкості в США

На сьогодні в США існує високорозвинута комплексна *Національна система планування* (далі – *НСП*; *англ.* – National Planning System, NPS), яка спирається на низку взаємопов'язаних концептуальних і нормативно-правових документів, що забезпечують системний підхід до процесу планування на всіх рівнях управління та для всіх юрисдикцій і категорій суб'єктів процесу.

Нижче наведено стислий опис цієї системи [105].

Особливості Національної системи планування США. Поточний стан безпеки всередині країни вимагає постійного розширення кола партнерів, які мають працювати разом. За таких умов НСП призначена забезпечувати уніфікований підхід та єдину термінологію для всього процесу планування щодо всіх видів загроз та небезпек, а також для всього ланцюга п'яти взаємопов'язаних місій, визначених Національною системою готовності: запобігання; захист; пом'якшення наслідків; реагування; відновлення. Відповідні плани (стратегічного, оперативного і тактичного рівнів) дозволяють залучити все суспільство до процесів побудови, підтримки в належному стані та забезпечення ключових можливостей, визначених у документі Ціль національної готовності.

Національна система планування США включає два основних елементи: *архітектуру планування* (у т. ч. стратегічний, оперативний і тактичний рівні планування та інтегрування процесу планування), а також сам *процес планування*, який описує кроки, необхідні для розробки всеосяжного плану дій. Архітектура планування і процес планування об'єднують елементи усієї Національної системи готовності

Загалом НСП включає три рівні планування:

- *планування стратегічного рівня* встановлює стратегічний контекст та очікування для оперативного планування;
- *планування оперативного рівня* визначає завдання та ресурси, необхідні для реалізації стратегії;

[105] National Preparedness System/Site FEMA. URL: https://www.fema.gov/national-planning-system

- *планування тактичного рівня* показує, яким чином використовувати ресурси при виконанні оперативних завдань у певний проміжок часу.

Зазначені рівні планування зазвичай розділені ще на дві категорії:

- *цілеспрямоване планування* (Deliberate Planning), яке включає розробку *стратегічних*, *оперативних* і *тактичних планів* з метою виконання згаданих вище п'яти взаємопов'язаних місій;
- *планування дій під час інциденту* (Incident Action Planning), котре здійснюється в умовах обмеженого часу для розробки планів, що забезпечують швидке переналаштування на оперативному і тактичному рівнях з тим, щоб швидко відреагувати на умови, які свідчать про неминучість безпекового інциденту або під час самого інциденту.

Згідно з прийнятим у США підходом процес планування передбачає виконання таких етапів: 1) формування спільної групи планування; 2) усвідомлення ситуації; 3) визначення цілей та завдань; 4) розробка плану; 5) підготовка плану, його розгляд і затвердження; 6) реалізація та обслуговування плану.

У країні напрацьований певний досвід, спираючись на нього для кожного етапу можна виокремити певні ключові моменти, а саме:

1) на етапі *формування спільної групи планування*: а) об'єднання зусиль, ресурсів і можливостей усього суспільства потребує залучення широкого кола спеціалістів; б) найбільш реалістичні та всеосяжні плани створюються групами планувальників, до складу яких входять представники різноманітних організацій та структур;
2) на етапі *досягнення усвідомлення ситуації*: а) планування є по суті методом управління ризиками, процесом, під час якого визначається контекст, ідентифікуються та оцінюються ризики, аналізуються і приймаються рішення щодо напрямів діяльності для управління цими ризиками; б) досягнення розуміння загальної картини ризиків надає можливість групам планування приймати кращі рішення (Threat and Hazard Identification and Risk Assessment);
3) на етапі *визначення цілей та завдань*: а) група планування встановлює *пріоритети* (тобто кінцевий стан, на досягнення якого націлена реалізація плану), *цілі* (розгорнуті, загальні

заяви про наміри застосувати певні методи для досягнення цілей місії з урахуванням пріоритетів) та *завдання* (конкретні дії, які виконуються під час операції з реагування); б) визначення пріоритетів, цілей та завдань дозволяє забезпечити єдність дій та узгодженість цілей при виконанні плану всіма суб'єктами процесу;

4) на етапі *розробки плану*: а) спочатку група планування готує та аналізує можливі варіанти напрямів дій задля досягнення *цілей* і виконання *завдань*; б) після цього планувальники оцінюють кожний напрям дій за низкою встановлених критеріїв з точки зору досягнення визначених цілей; в) завдяки порівнянню група планування добирає найбільш прийнятні варіанти і продовжує планування, а керівні особи схвалюють рішення про дібрані напрями діяльності;
5) на етапі *підготовки*, *розгляду та затвердження плану*: визначені на попередньому етапі напрями дій перетворюються на план: а) група планування розробляє чорновий проект плану, у т. ч. додатки, таблиці, графіки тощо; б) група готує остаточну версію проекту та розсилає її для отримання коментарів та зауважень від суб'єктів виконання плану; в) група планування перевіряє роздрукований варіант плану щодо його узгодженості з правовими вимогами та нормами, визначає його практичну користь; після перевірки правильності та дієвості плану (зазвичай шляхом його випробування під час навчання або в умовах реальної події), заінтересовані сторони підписують план і розсилають його суб'єктам процесу реагування;
6) на етапі *реалізації та обслуговування плану*: а) процедура вдосконалення плану може запускатися: внаслідок виявлення необхідності у корегувальних заходах за результатами аналізу навчань (тренувань) або реального інциденту; у процесі регулярного обслуговування (наприклад, щорічно, кожні два роки); внаслідок змін у конфігурації ризиків; змін у відповідному законодавстві, політиці або у доктринальних документах; б) мають бути встановлені процедури регулярного процесу розгляду та перегляду плану; в) суб'єкти реагування використовують навчання і тренування, а також реальні інциденти для оцінювання ефективності планів.

Координування та інтегрування робіт з планування. Діяльність, спрямована на координування та інтегрування планів багатьох організацій, забезпечує поєднання зусиль шляхом досягнення загального уявлення про відповідні можливості, наявні взаємозв'язки, спільні завдання та вимоги до ресурсного забезпечення. Функціонування НСП сприяє запровадженню єдиного підходу до процесу планування шляхом горизонтального і вертикального інтегрування планів у всьому суспільстві.

Вертикальне інтегрування – це включення процесів планування різного масштабу в рамках забезпечення конкретної функції (послуги). Наприклад, суб'єкти реагування, що забезпечують функції підтримки аварійних служб на федеральному рівні та на рівні штату, повинні координувати свої зусилля з тим, щоб забезпечити єдині очікування від процесу планування (наприклад, щодо правозастосування, управління надзвичайною ситуацією тощо).

Горизонтальне інтегрування – включення процесів планування з урахуванням різноманітних функцій, місій, організацій та юрисдикцій, що дає змогу здійснювати підтримку партнерів у розробці планів, які задовольняють їхнім внутрішнім потребам та/або нормативно-правовим вимогам.

Об'єднані разом процеси горизонтального та вертикального планування допомагають забезпечити координацію очікувань (цілей) управління інцидентами для всіх функцій та можливостей, які потрібні для реагування на всі види загроз та небезпек. НСП створює основу для ефективної спільної роботи планувальників суб'єктів процесу реагування, у т. ч. щодо планування дій у зв'язку із ризиками, координації створення оперативних структур, ефективного розподілу наявних ресурсів.

Взаємодопомога в усьому суспільстві є важливим принципом процесу забезпечення національної готовності, що вимагає формування загального чіткого усвідомлення інформації про ресурси та послуги, які можуть бути надані іншими організаціями. Взаємний обмін ресурсами та взаємодопомога повинні здійснюватися як для діяльності у стабільній ситуації, так і під час інциденту (кризи) або при проведенні якогось особливого заходу. Важливо, щоб при цьому всі заінтересовані сторони мали спільне розуміння того, за якими процедурами має відбуватися доступ до інших ресурсів або їх об'єднання.

2.3.2. Планування дій у кризових ситуаціях в Україні з точки зору забезпечення безпеки та стійкості критичної інфраструктури

Беручи до уваги основні підходи, реалізовані при створенні НСП США, стисло розглянемо ситуацію в Україні щодо планування дій під час інцидентів та криз різного походження, пов'язаних із безпекою критичної інфраструктури. При цьому будемо мати на увазі, що спроби механічного перенесення зарубіжного досвіду без адекватного урахування національних особливостей, як правило, виявляються невдалими.

Перш за все слід зазначити, що Україна поки що перебуває на самому початку створення сучасної цілісної системи реагування на безпекові інциденти та кризи, пов'язані з КІ, відстаючи у цій сфері від передових країн світу щонайменше на 5–10 років.

Так, лише 2016 р. в національному законодавстві України з'явилося визначення основного для цієї сфери терміна «критична інфраструктура». Наявні державні (національні) системи безпеки (захисту) та кризового реагування України є значною мірою автономними, а плани та процедури взаємодії між ними – або недостатньо деталізовані, або мають значною мірою декларативний характер. Загалом на сьогодні в Україні функціонує або перебуває на стадії створення кілька систем. Їхнє завдання – опікуватися об'єктами та системами КІ (у широкому значенні цього поняття), серед яких у контексті означеної проблеми виокремимо:

- Єдину державну систему цивільного захисту (ЄДСЦЗ) [106];
- Єдину систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків (ЄСЗРПТА) [107];
- Державну систему фізичного захисту (ДСФЗ) [108] (мається на увазі державна система фізичного захисту ядерних установок, ядерних матеріалів);

[106] Про затвердження Положення про єдину державну систему цивільного захисту: Постанова Кабінету Міністрів України від 09.01.2014 № 11 // База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/11-2014-%D0%BF

[107] Про затвердження Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків: Постанова Кабінету Міністрів України від 18.02.2016 № 92 // База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/92-2016-%D0%BF

[108] Про затвердження Порядку функціонування державної системи фізичного захисту: Постанова Кабінету Міністрів України від 21.12.2011 № 1337 // База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/1337-2011-%D0%BF

- Національну систему кібербезпеки (НСК), що створюється в рамках реалізації Стратегії кібербезпеки України [109].

Недостатню або суто декларативну взаємодію існуючих державних (національних) систем можна проілюструвати на конкретному прикладі. Розглянемо ситуацію: від розвідувальних органів надходить підтверджена інформація про загрозу теракту на одній з українських АЕС (такі ядерні об'єкти включають до КІ всі країни, що їх мають). Згідно із цим повідомленням існує небезпека завдання тяжких наслідки життю та здоров'ю населення не тільки в результаті застосування терористами, скажімо, стрілецької зброї, а й пошкодження технологічного обладнання, тобто з точки зору ядерної, техногенної, екологічної безпеки. Відтак, одержавши таку інформацію, різні системи розпочинають працювати за власними процедурами.

Аналіз їхніх дій указує на те, що системи використовують різні терміни для опису режимів функціонування, а саме: «режими», «умови» та «рівні». По суті про майже повний збіг можна говорити лише для ЄДСЦЗ та ДСФЗ для двох перших режимів/умов, які при цьому можна вважати певною мірою найпростішими з точки зору планування й реагування на інциденти та кризи [110].

Для ЄСЗРПТА, на відміну від двох інших систем, відсутній режим (рівень загрози), який можна було б зіставити із режимам «повсякденного» або «нормального» функціонування.

З ускладненням режимів невідповідності критеріїв термін їхнього запровадження збільшується. Тому, наприклад, для запропонованої події (загроза теракту на одній з українських АЕС із можливими тяжкими наслідками комплексного характеру) різні системи будуть працювати в різних режимах:

- ДСФЗ – в режимі кризової ситуації [111];
- ЄДСЦЗ – в режимі повсякденного функціонування [112];

---

[109] Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 № 96/2016 // База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/96/2016

[110] Саме тому в таблиці для переважної більшості режимів (умов, рівнів) однієї системи неможливо знайти однозначну відповідність режимів (умов, рівнів) з іншими системами.

[111] Це фактично стан найвищої мобілізованості системи, адже наступний за шкалою «режим відновлення нормального функціонування».

[112] Положення про ЄДСЦЗ стосовно терористичних агроз передбачає реагування лише у *режимі надзвичайного стану* за умови «здійснення масових терористичних актів, що супроводжуються загибеллю людей чи руйнуванням особливо важливих об'єктів життєзабезпечення».

- ЄСЗРПТА – у режимі, що відповідає передостанньому, «жовтому рівню» шкали терористичної загрози [113].

З упевненістю можна сказати, що розробка дієвих планів взаємодії та координації дій потребує, щонайменше, узгодження і прийняття спільної термінології, визначення співвідношень між *режимами*, *рівнями* та *умовами* функціонування систем, узгодження принципів управління комплексною кризою (у т. ч. чіткого розподілу відповідальності між суб'єктами процесу на всіх стадіях кризи), адже комплексна криза пов'язана з одночасною дією кількох небезпечних факторів.

Спираючись на наведене вище, можна констатувати, що в Україні проблеми забезпечення БСКІ загалом і розробки планів взаємодії та координації дій зокрема значною мірою зумовлені тим, що жодна із перелічених вище систем не призначена для реагування на *всі види фізичних загроз* та *кіберзагроз* та їх можливі комбінації. У результаті цього на національному рівні поки що тільки формується *системний підхід до захисту КІ*, який має враховувати численні взаємозв'язки її елементів, розглядаючи КІ при цьому як надскладний, але єдиний об'єкт захисту.

Одним із наслідків такої ситуації є те, що *жоден орган державної влади не опікується проблемами захисту КІ в цілому* (тобто на надвідомчому рівні). Можна припускати, що саме це стало однією з головних причин невдалих попередніх спроб запровадити в Україні прийнятий у провідних країнах світу підхід, що враховує всі види загроз та небезпек (all hazards approach), адже реалізовували такі спроби державні органи, в управлінні яких і перебувала та чи інша система кризового реагування на певні види загроз.

Ще один висновок із наведеного прикладу – вирішальну роль в об'єднанні зусиль населення, суспільства і держави у цій сфері може відіграти система концептуальних та стратегічних документів, яка створить надійну основу для планування дій усіх суб'єктів забезпечення захисту та стійкості КІ у разі безпекових інцидентів та кризових ситуацій, як це значною мірою реалізовано в США.

[113] Для цього конкретного випадку, а також для всієї «кольорової шкали» рівнів терористичних загроз, не зовсім зрозуміло, чому найвищий («червоний») рівень терористичної загрози встановлюється, а загроза терористичного акту вважається «реальною» тільки після того, як терористичний акт було вчинено.

2.4. Взаємодія та обмін інформацією

2.4.1. Структура системи взаємодії та обміну інформацією

Досягнення цілей та виконання завдань із забезпечення БСКІ потребує участі багатьох державних органів і організацій, компаній усіх форм власності, ЗМІ, неурядових організацій, місцевих громад і населення тощо. За такої умови зрозуміло, що відповідна діяльність та заходи, що вживаються щодо КІ, лише тоді будуть достатньо ефективними, коли забезпечуватимуться належні рівні координації дій, взаємодії та обміну інформацією між усіма заінтересованими сторонами (акторами). Це, у свою чергу, передбачає наявність певних систем, мереж та центрів, які мають забезпечувати ВОІ, обробку та представлення інформації у необхідному вигляді для здійснення діяльності акторів щодо:

- запобігання безпековим інцидентам та кризам на об'єктах КІ;
- реагування на такі інциденти та кризи у випадках, коли вони трапилися;
- пом'якшення та ліквідацію наслідків інцидентів та криз;
- відновлення функціонування об'єктів критичної інфраструктури (ОКІ).

Окремі системи реагування та ВОІ, котрі існують в Україні, є значною мірою фрагментованими, що відображає використання застарілих вузьковідомчих підходів до кризового управління, закріплених у чинній нормативно-правовій базі, відповідно до якої системи безпеки та кризового реагування і відповідальні за них державні органи мають опікуватися лише певними категоріями загроз та ризиків.

При цьому навіть тоді, коли така система має статус *державної* чи *національної*, її функціональність виявляється обмеженою «зверху» рівнем відповідального міністерства чи відомства, що не передбачає наявності дієвих процедур ВОІ з вищим політичним керівництвом держави. Додамо, що на умовно «нижчому» рівні архітектури процесів ВОІ, який мав би включати таких акторів як населення, ЗМІ, неурядові організації та експертне співтовариство, ВОІ систем із зазначеними суб'єктами у найкращому випадку зведені до оповіщення населення в умовах надзвичайних ситуацій.

Багатоаспектні швидкі негативні впливи на всі сфери життя країни й населення, які можуть спричинити збої у функціонуванні

елементів КІ або їх знищення, очевидно, проявлятимуться у формі *ефектів доміно* та *каскадних ефектів*, коли тяжкі наслідки безпекових криз на одному із елементів КІ в якомусь із її секторів розповсюджуються на інші елементи і сектори КІ.

Запобігання таким сценаріям і є одним із головних завдань державної системи забезпечення безпеки та стійкості критичної інфраструктури. І саме цей міжвідомчий і міжсекторальний вимір виявляється практично поза межами повноважень, функцій і завдань чинних систем безпеки та кризового реагування. Одним із проявів цього родового недоліку згаданих систем є відсутність дієвих процедур і механізмів ВОІ між системами.

У найкращих випадках положення про існуючі системи містять лише згадки про створення для управління кризовою ситуацією певних міжвідомчих структур (*комісій*), яким доручається забезпечити ВОІ між суб'єктами реагування, у т. ч. інформування Уряду та Президента України.

Слабко розвинута практика проведення навчань і тренувань для забезпечення перевірки готовності до кризових ситуацій, особливо на регіональному та національному рівнях, сприяла консервації суто формального ставлення до процедур ВОІ між чинними системами безпеки та кризового реагування України, що проявляється у декларативності та неконкретності положень відповідних документів, які мають урегульовувати такі процедури.

2.4.2. Основні підходи до формування архітектури національної мережі ситуаційно-кризових та інформаційно-аналітичних центрів

Згадані вище проблеми можуть бути значною мірою розв'язані завдяки функціонуванню *Національної мережі ситуаційно-кризових центрів* (НМ СКЦ) та *інформаційно-аналітичних центрів*, яку передбачено створити в Україні для забезпечення інформаційно-аналітичної підтримки процесу прийняття рішень, у т. ч. через усунення названих вище «вузьких місць» та вдосконалення чинних механізмів і процедур ВОІ.

Слід зазначити, що у сфері захисту КІ забезпечення адекватного сучасним загрозам рівня взаємодії та обміну інформацією визначено як пріоритетне багатьма розвиненими країнами світу та між-

народними організаціями. Адже кризові ситуації, спричинені реалізацією загроз і небезпек, передусім комплексного характеру, на об'єктах і системах КІ, можуть мати безпосередній вплив не тільки на національну, а й на регіональну і навіть глобальну безпеку. Це потребує готовності до мобілізації всіх наявних у державі ресурсів і, за необхідності, запиту міжнародної допомоги від країн-партнерів, що неможливо без належної інформаційно-аналітичної підтримки процесів прийняття рішень, у т. ч. на політичному рівні.

Сформульовані вище міркування зумовлюють необхідність розміщення «на вершині» ієрархічно побудованої НМ СКЦ центру, який би виконував функції *головного ситуаційно-кризового центру держави*, забезпечуючи безпосередню інформаційно-аналітичну підтримку процесу прийняття рішень вищим політичним керівництвом держави.

Нині за своєю приналежністю та поставленими перед ним завданнями, на нашу думку, цій ролі найбільшою мірою відповідає Головний ситуаційний центр України (ГСЦУ) при Раді національної безпеки і оборони України (РНБОУ). Проте слід зазначити, що наразі відбувається складний процес реформування сектору безпеки держави, у ході якого не можна виключати, що виконання такої ролі може бути покладено на інший СКЦ, створений, наприклад, при Президентові або при Уряді України. Але в усіх варіантах побудови НМ СКЦ, на наш погляд, важливо не обмежуватися декларативними формулюваннями, а передбачити надійне та своєчасне інформування вищого політичного керівництва держави у кризових ситуаціях, що стосуються національної та державної безпеки, зокрема БСКІ.

При ієрархічному структуруванні НМ СКЦ доцільно використати апробовані підходи до підготовки інформації для прийняття рішень у сфері національної безпеки, які застосовуються в розвинених країнах світу. Залежно від функцій, повноважень і сфери відповідальності отримувача інформації кількість і назва етапів, їх основні завдання можуть дещо відрізнятися, але в узагальненому вигляді послідовність стадій такого циклу може бути представлена так, як це зображено на схемі (*рис. 2.1*.)

Деталізуємо завдання за кожною стадією.

Стадія 1. Постановка завдання («формулювання вимог») щодо необхідної інформації.

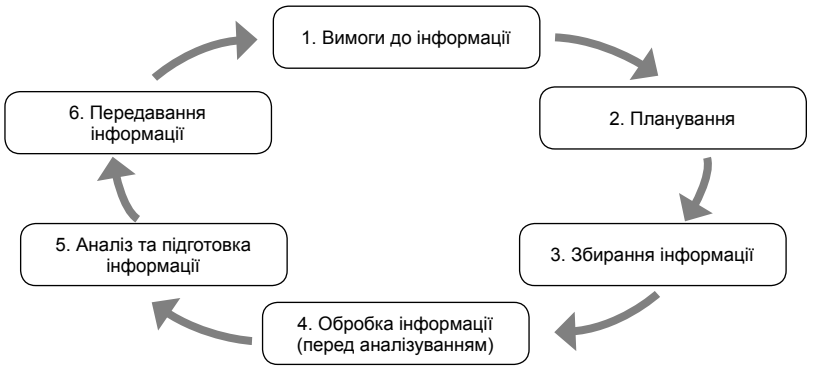


Рис. 2.1. Адаптований до цілей та завдань НМ СКЦ цикл підготовки інформації для підтримки прийняття рішень щодо КІ

Джерело: побудовано автором за матеріалами сайту ЦРУ (див. URL: https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html).

Стадія 2. Планування заходів та управління ресурсами з метою виконання завдання.

Стадія 3. Збирання первинної (необробленої) інформації різноманітними способами і шляхами.

Стадія 4. Обробка та форматування інформації з тим, щоб представити зібрані масиви даних у формі, прийнятній для використання аналітиками, у т. ч. узагальнення інформації, введення даних до відповідних баз тощо.

Стадія 5. Аналіз та підготовка інформації для прийняття рішень (у нашому контексті – це аналіз, оцінювання та перевірка даних, об'єднання даних та інформації у єдину взаємоузгоджену картину розвитку кризової ситуації, на основі якої робляться висновки щодо можливих сценаріїв розвитку ситуації та пропонуються варіанти рішень).

Стадія 6. Надання підготовленої інформації (у нашому випадку її споживачами є ті посадові особи/уповноважені державні органи, які приймають рішення на оперативному, стратегічному та політичному рівнях).

У результаті прийняття таких рішень можуть бути сформульовані нові вимоги (запити) щодо отримання певної інформації, що означатиме подальше продовження циклу підготовки інформації.

Спираючись на представлений вище загальний опис стадій циклу підготовки інформації, можна передбачати, що функціонування НМ СКЦ має забезпечувати виконання завдань, віднесених до стадій 2–6 циклу.

Зіставлення циклу підготовки інформації (*рис. 2.1*) із чинною в Україні практикою показує, що наразі у процедурах, котрі запроваджені для ВОІ в нашій країні, недостатньо уваги приділяється стадіям обробки та аналізу інформації. Зокрема, за важливості отримання оперативної інформації безпосередньо з місця подій (в онлайн-режимі) ефективний процес прийняття рішень неможливий (особливо на найвищому політичному рівні) без серйозної попередньої роботи з обробки, аналізу та оцінювання інформації, прогнозування можливих варіантів розвитку подій, а також формулювання запропонованих у певному форматі варіантів рішень.

Інший важливий аспект, який має бути відображений в архітектурі НМ СКЦ, полягає в тому, що в Україні існують *національні* та *галузеві системи*, *сфокусовані на протидії певним видам загроз*, включно й забезпечення готовності до кризового управління у випадку реалізації таких загроз. У рамках функціонування цих систем передбачені механізми ВОІ (у т. ч. через спеціально створені з цією метою СКЦ). Йдеться, зокрема, про такі системи та підсистеми, що мають певний взаємозв'язок із питанням, котре розглядається, зокрема вже згадані системи ЄДСЦЗ (цивільний захист), ЄСЗРПТА (антитерор), ДСФЗ (фізичний захист), НСК (кіберзахист) та деякі ін.

Крім наявності значної кількості важливих систем і підсистем (наприклад, ядерної безпеки), які мають статус національних чи державних, слід також брати до уваги, що за кількома безпековими напрямами Україна має міжнародні зобов'язання. На їх виконання до таких міжнародних організацій, як-от МАГАТЕ, а також до держав-партнерів та їхніх компетентних органів має надаватися інформація, зокрема про безпекові інциденти та надзвичайні ситуації.

Ураховуючи це, створені при державних органах СКЦ, які забезпечують діяльність систем і підсистем національного рівня, а також інформування міжнародних організацій та країн-партнерів, доцільно віднести до наступного за Головним ситуаційним центром

України рівня, на якому здійснюються заходи з аналізу інформації та взаємодії, віднесені до *стадії 5* інформаційного циклу (див. перелік стадій вище).

Окремий наголос слід зробити на обміні інформацією з населенням, громадськістю та експертним середовищем. Необхідність розробки та інтегрування до системи ВОІ процедур та механізмів надійного обміну інформацією з населенням, ЗМІ та експертним співтовариством випливає з того, що саме населення та довкілля є основними об'єктами захисту для всіх безпекових систем у державі, а ЗМІ та експертна спільнота можуть серйозно вплинути на сприйняття населенням безпекових загроз та ризиків, дій держави та інших акторів у ході реагування та ліквідації наслідків криз і, таким чином, суттєво впливати на перебіг подій. До основного принципу ВОІ з цією категорією учасників процесу слід віднести необхідність своєчасного надання виваженої інформації для запобігання паніці та мобілізації ресурсів місцевих спільнот для ефективного реагування у разі кризи. Тому, як і для випадку інформування вищого політичного керівництва держави, було би неправильним і недоцільним надавати населенню та широкому колу ЗМІ первинну інформацію без попередньої її перевірки та обробки.

Наведені вище міркування можемо узагальнити у вигляді *табл. 2.3* (*див. с. 76-77*) на прикладі реагування на кризові ситуації в енергетиці України.

Важливо зазначити, що будь-які пропозиції щодо вибору моделей ВОІ для НМ СКЦ мають відштовхуватися від того складного фінансово-економічного стану, в якому поки що перебуває Україна і який зумовлює доцільність максимально можливого використання наявної інфраструктури, ресурсів і технічних можливостей, котрі є в розпорядженні державних органів, компаній різних форм власності, інших суб'єктів забезпечення безпеки та стійкості КІ. Виходячи з цього, у найближчій перспективі основні рекомендації щодо забезпечення ВОІ доцільно формулювати, фокусуючись на *запровадженні дієвих механізмів ВОІ між системами безпеки, які існують, та кризового реагування, беручи до уваги всі види фізичних загроз та кіберзагрози, а також необхідність забезпечення ВОІ з політичним та публічним рівнями,* включеними до ієрархічної піраміди, яка представляє процеси ВОІ щодо захисту критичної інфраструктури.

Таблиця 2.3. **Рівні та суб'єкти ВОІ щодо реагування на кризові ситуації, пов'язані з КІ**

Ієрархічні рівні системи ВОІ	Структурні елементи/суб'єкти НМ СКЦ	Роль і функції при ВОІ (за стадіями циклу підготовки інформації у кризових ситуаціях)
Політичний рівень	Президент (РНБОУ), Уряд України	*Стадії 1 та 2 інформаційного циклу:* • формування запиту на певну інформацію, стратегічне планування заходів та управління ресурсами з метою виконання завдання. *Стадія 6 інформаційного циклу*: • отримання інформації для прийняття рішення; формування наступного запиту
Перший рівень НМ СКЦ	СКЦ національного рівня (наприклад, Головний ситуаційний центр України при РНБОУ та ін.)	*Стадія 6 інформаційного циклу:* • остаточний аналіз інформації, підготовка, розробка та подання у необхідному форматі альтернативних варіантів стратегічних та політичних рішень щодо кризової ситуації; • обмін інформацією з іншими СКЦ національного рівня (наприклад, із СКЦ КМУ, у разі їх створення) – горизонтальне інтегрування; • обмін інформацією з другим рівнем НМ СКЦ – вертикальне інтегрування
Другий рівень НМ СКЦ	СКЦ за основними видами загроз, у т. ч. СКЦ таких суб'єктів процесу: • СБУ (АТЦ при СБУ); • МВС (Нацгвардія); • Міненерговугілля; • ДСНС України; • Держатомрегулювання; • Міноборони; • МОЗ (Державна служба медицини катастроф, екстрена медична допомога)	*Стадія 5 інформаційного циклу:* • аналіз, оцінювання, перевірка даних та інформації; • об'єднання інформації для отримання взаємоузгодженої (наскільки це можливо) картини розвитку кризової ситуації; • підготовка рекомендацій щодо набору варіантів прийняття рішень для виходу із кризи та зменшення наслідків кризи; • обмін інформацією з першим і третім рівнями (вертикальне інтегрування); • обмін інформацією на другому рівні (горизонтальне інтегрування); • брифінги для ЗМІ та експертів, інформування населення

Третій рівень НМ СКЦ	СКЦ державних і приватних компаній (НАЕК «Енергоатом», «Укренерго», «Укргідроенерго», українських АЕС), інформаційні служби правоохоронних органів та аварійних служб відповідного рівня	*Стадія 4 інформаційного циклу*: • обробка та форматування первинної інформації з тим, щоб представити її у формі, прийнятній для подальшого використання аналітиками, у т. ч. попереднє узагальнення інформації; • внесення інформації до спеціалізованих баз даних; • обмін інформацією з другим, четвертим і публічними рівнями (вертикальне інтегрування); • обмін інформацією на третьому рівні (горизонтальне інтегрування)
Четвертий рівень НМ СКЦ	СКЦ об'єктів та систем критичної інфраструктури, системи моніторингу безпекових характеристик, інформаційні служби правоохоронних органів та аварійних служб відповідного рівня	*Стадія 3 інформаційного циклу:* • збирання первинної інформації та подальше її передавання різноманітними способами і шляхами, у т. ч.: – від систем моніторингу; – від персоналу та особового складу, від підрозділів первинного реагування на об'єктах КІ згідно з прийнятими процедурами; – від окремих осіб із числа населення (через загальнонаціональні системи аварійного та надзвичайного зв'язку); – від правоохоронних органів, аварійних та інших служб з місця подій тощо; – обмін інформацією із СКЦ об'єктів і систем КІ (горизонтальне інтегрування); – обмін інформацією із третім рівнем НМ СКЦ та із публічним рівнем (вертикальне інтегрування)
Публічний рівень	Населення, ЗМІ, експертне співтовариство	З одного боку, із цього рівня можуть надходити сигнали та первинна (необроблена) інформація щодо загрози або початку кризової ситуації на об'єкті КІ, а з іншого – безпека населення є одним із найвищих пріоритетів реагування на кризові ситуації. ЗМІ та експертне співтовариство повинні сприяти цьому процесу, який має включати, не обмежуючись, таке: • передавання інформації на третій та четвертий рівні НМ СКЦ (вертикальне інтегрування); • обмін інформацією зі ЗМІ та експертами, іншими членами спільноти (горизонтальне інтегрування).

Джерело: складено автором.

2.5. Огляд форм і форматів навчальних курсів

Незважаючи на те, що ЗКІ є порівняно новою безпековою концепцією, наразі у світі існує безліч інформації з цієї проблематики, у т. ч. стосовно підготовки кадрів та підвищення інформованості населення щодо захисту та забезпечення стійкості КІ. Наприклад, запит інформації в Google за ключовими словами «training critical infrastructure protection» дає близько 47 млн 500 тис. посилань. Звичайно, найбільший інтерес викликає передовий досвід у цій сфері таких країн, як США – визнаного лідера в запровадженні сучасних підходів у сфері безпеки.

Що стосується галузевих підходів, то тут належну увагу слід приділити ядерному сектору КІ, в якому історія захисту ядерних установок та ядерних матеріалів, що перебувають за рамками військових програм, налічує вже кілька десятків років. Крім ядерної галузі, багатий досвід у забезпеченні фізичної безпеки (захищеності) відповідних об'єктів, персоналу та матеріальних цінностей, зменшенні ризиків, пов'язаних із загрозами злочинних дій, включно й тероризм, мають авіатранспорт та банківсько-фінансова сфера.

Разом з тим, система підготовки кадрів та населення щодо ЗКІ для кожної країни *завжди буде унікальною*, оскільки на конфігурацію та функціонування такої системи завжди впливає цілий комплекс чинників: від особливостей національного законодавства до розподілу повноважень між державними органами; від менталітету та рівня освіти населення до його комп'ютерної грамотності; від соціальної відповідальності бізнесу до розвитку державно-приватного партнерства у цій сфері тощо. При цьому, звичайно, висновок про унікальність конкретних форм реалізації системи підготовки кадрів і населення зовсім не означає заклик до нехтування загальновизнаними у світі підходами.

З початку XXI ст. у світі відбуваються швидкі безпекові зміни, зокрема, триває процес загострення загроз тероризму та екстремізму, що зумовлює необхідність підвищення безпеки та стійкості КІ. Комплексний характер цього завдання вимагає забезпечення потреб у навчанні в широкому діапазоні цільових аудиторій для різних секторів КІ, створення можливостей як для розповсюдження серед населення базових понять та знань (підвищення інформованості) про КІ, так і отримання спеціалізованої вищої освіти.

Ефективному виконанню цих вимог може сприяти те, що в теперішній час триває процес бурхливого розвитку ІТ технологій, результати якого дозволяють провідним країнам світу, корпораціям, неурядовим організаціям, залученим до цього процесу, значно урізноманітнити форми й методи навчання на всіх рівнях та в усіх напрямах. У рамках цього процесу все більшої популярності набувають дистанційні форми навчання з використанням можливостей Інтернету, що дає змогу суттєво зменшити витрати на організацію та проведення навчальних та освітніх курсів, а також розширює доступ до необхідних інформаційних ресурсів і створює додаткові можливості для залучення до цього процесу висококваліфікованих викладачів та експертів.

У цьому контексті навіть швидке ознайомлення з формами, форматами і методами підготовки кадрів та освітньої діяльності щодо ЗКІ дозволяє стверджувати, що наразі в провідних країнах світу для цього використовуються практично всі види, форми та інструменти навчання, які притаманні системам загальної освіти та підготовки кадрів.

2.5.1. Організація підготовки кадрів і населення на державному рівні та в межах секторів критичної інфраструктури

Відомо, що кожна країна, яка запроваджує концепцію захисту КІ, зазвичай визначає сектори, що включають відповідні об'єкти, системи та ресурси. Кількість секторів КІ може варіюватися від країни до країни. Їх кількість залежить від багатьох чинників, зокрема від можливостей (ресурсів) держави, інших акторів, як-от приватних компаній, забезпечити захист відповідних об'єктів і систем. Причому кожний сектор закріплено за одним (іноді двома) державними органами (агентствами), на який (які) покладено завдання і щодо підготовки кадрів і населення до захисту від специфічних для цього сектору загроз і ризиків, що є одним із напрямів діяльності відповідальних міністерств (відомств).

Огляд доступних інформаційних ресурсів дозволяє зробити попередній висновок про те, що у чітко структурованому вигляді підготовка кадрів та населення щодо захисту об'єктів та систем КІ, які віднесені до того чи того її сектору, нині існує лише в США. При цьому можна констатувати, що організаційні підходи із виконання цього завдання перебувають у стадії динамічного розвитку, тому про певну

завершеність обґрунтовано можна говорити лише для секторів КІ, відповідальність за які покладено на МВБ США [114].

Розділ сайту міністерства, присвячений підготовці персоналу та навчанню з питань ЗКІ [115], містить інформацію про навчання за такими напрямами:

- Навчання щодо хімічного сектору;
- Навчання щодо комерційних об'єктів [116];
- Серія з отримання знань про КІ [117];
- Навчання щодо сектору гідротехнічних споруд;
- Навчання щодо служб надання екстреної допомоги.

Звертає на себе увагу те, що в цьому списку відсутні сектори зв'язку (Communications*)* та інформаційних технологій (Information Technology), котрі належать до сфери відповідальності DHS, а також сектори, стосовно яких DHS несе спільну відповідальність: *за урядові об'єкти* (разом із Адміністрацією загальних служб, General Services Administration) та *за транспортну систему* (Transporting System) (разом із Міністерством транспорту, Department of Trans_ port). Саме цей факт дозволяє припустити, що в США процес формування секторальних систем підготовки персоналу та населення щодо ЗКІ перебуває у своїй активній фазі.

Крім того, головна сторінка сайту МВБ, присвячена навчанню з питань ЗКІ, інформує про широкий набір безкоштовних навчальних програм для урядовців та представників приватного сектору, включно й курси незалежного вивчення з використанням вебтехнологій, курси під керівництвом інструкторів, а також про доступ до необхідних навчальних матеріалів, призначених для державних

---

[114] Слід зазначити, що на національному рівні в організаційному плані ключову роль щодо захисту КІ, включно й підготовку кадрів та населення, відіграє *Офіс захисту інфраструктури* (Office of Infrastructure Protection), який було створено для керування національними зусиллями з метою захисту КІ від усіх видів загроз шляхом управління ризиками та забезпечення стійкості КІ, співпрацюючи з усіма заінтересованими сторонами процесу.

[115] U.S. Department of Homeland Security/Site. URL: https://www.dhs.gov/critical-infrastructure-training

[116] Маються на увазі торговельно-розважальні центри, стадіони, концертні зали, музеї та інші місця проведення масових заходів.

[117] Серія навчальних одногодинних безкоштовних веб-семінарів щодо ЗКІ, які проводяться експертами з метою ознайомлення із засобами, тенденціями, проблемами та передовим досвідом забезпечення безпеки та стійкості КІ. МВБ особливо рекомендує таке навчання своїм партнерам із уряду та приватного сектору, які несуть відповідальність за управління ризиками, безпекою та кризовими ситуаціями.

чиновників, власників та операторів об'єктів і систем критичної інфраструктури.

Наведемо перелік навчальних курсів, які пропонує МВБ:

- *Загальні онлайн-курси для секторів КІ.*

Ця категорія включає загальні для всіх секторів КІ курси та навчальні матеріали, у т. ч. інформацію про нормативно-правову базу ЗКІ, про засади партнерства та співпраці у галузі ЗКІ тощо. Крім того, для всіх секторів КІ пропонуються курси з підвищення загальної інформованості з питань фізичної безпеки, у т. ч. з таких тем:

- Підвищення інформованості про фізичну безпеку на робочому місці (workplace security awareness);
- Ситуація з «активним стрільцем» (an active shooter situation): що потрібно робити;
- Підвищення інформованості про безпеку на об'єктах роздрібної торгівлі (retail security awareness): усвідомлення прихованих небезпек;
- Підвищення інформованості про (незаконне) стеження (surveillance awareness): що потрібно робити;
- Захист критичної інфраструктури проти загроз внутрішнього порушника (insider threats);
- Фізична безпека критичної інфраструктури: крадіжки та переключення[118] (theft and diversion), що потрібно робити.

- *Курси для конкретних секторів КІ.*

У цьому розділі згруповано курси для перелічених вище окремих секторів КІ, за які несе відповідальність МВБ.

Крім того, основна сторінка сайту МВБ з питань навчання та підготовки кадрів для захисту і забезпечення стійкості КІ містить посилання на спеціальний освітній портал (Critical Infrastructure Security and Resilience Training Portal) з корисними посиланнями щодо інших можливостей для навчання з цієї проблематики. Окремий підрозділ присвячено курсам, підготовленим Міжвідомчим комітетом з фізичної безпеки міністерства (The Interagency Security Committee) для професіоналів з безпеки, інженерів, власників будівель, архітекторів та населення з метою надати базову інформацію про стандарти фізичної безпеки для урядових об'єктів, процедури забезпечення та найкращу практику досягнення цих стандартів.

[118] Під «переключенням» мається на увазі переключення використання матеріалів та обладнання на злочинні цілі.

Ще один розділ основної сторінки з навчання щодо КІ присвячено комплексу навчальних інструментів (Counter-Improvised Explosive Device (IED) Training and Awareness), розроблених міністерським Офісом із запобігання підривів (DHS Office for Bombing Prevention) з метою створення в державі базових можливостей із протидії застосуванню саморобних вибухових пристроїв та посилення інформованості про терористичні загрози. Навчальні курси розраховані на представників державних органів, починаючи з федерального рівня, чиновників місцевих органів влади, правоохоронців та менеджерів і співробітників служб екстреного реагування, власників та операторів об'єктів КІ, співробітників служб безпеки на підприємствах тощо.

Інший важливий напрям, присвячений навчанню щодо безпеки КІ, стосується загроз, пов'язаних із «активними стрільцями». МВБ пропонує на безоплатній основі семінари (Active Shooter Preparedness Workshops) із підвищення готовності до ситуацій, що виникають у результаті дій «активних стрільців», а також відповідні курси та навчальні матеріали, які спрямовані на ознайомлення з індикаторами поведінки, що можуть свідчити про намір особи (осіб) вчинити напад, а також із моделями поведінки злочинців.

Також слід відзначити наявність на веб-сторінці, що розглядається, спеціального розділу щодо *навчання для уповноважених користувачів* (Authorized User Training). Цим ураховано той факт, що відповідні навчальні курси містять інформацію з обмеженим доступом, і для участі в них допускаються особи, яким це необхідно за їхніми службовими обов'язками. До цієї категорії, наприклад, належить курс із вивчення інформації про вразливості з точки зору хімічного тероризму (Chemical-Terrorism Vulnerability Information).

У розділі «*Інші навчальні ресурси*» (Other Training Resources) слід акцентувати на такому дуже важливому напрямі підготовки кадрів і населення до захисту КІ та забезпечення її стійкості, як-от сприяння відповідній діяльності місцевих громад та місцевого бізнесу. Ця робота ведеться під девізом «*Безпека батьківщини починається з безпеки рідного міста*». У розділі надано посилання на спеціальну сторінку *«Безпека рідного міста»* (Hometown Security) [119], яка містить розроблені настанови із застосування чотирикрокового підходу за формулою: «Встановлюй зв'язок – Плануй – Тренуйся – Доповідай»

[119] Безпека рідного міста. URL: https://www.dhs.gov/hometown-security

(Connect, Plan, Train, Report). У цьому ж розділі є такий украй актуальний напрям підготовки кадрів і населення, як «*Планування і тренування для забезпечення безпеки шкіл*» (School Safety Planning and Training), що є особливо важливим для країн з високим рівнем терористичної загрози.

2.5.2. Основні форми та інструменти підготовки кадрів і населення у рамках сектору критичної інфраструктури на прикладі США

Значний інтерес представляє організація підготовки кадрів і населення для конкретного сектору КІ. Розглянемо досвід США у цьому питанні на прикладі хімічного сектору КІ.

Система підготовки кадрів і населення для хімічного сектору включає як *загальні* для всіх секторів КІ, так і *специфічні* для цього сектору інструменти та напрями діяльності.

До числа загальних слід віднести:

- Навчання з підвищення інформованості з питань безпеки з використанням мережі Інтернет (Web-based Security Awareness Training);
- Навчання та підвищення інформованості щодо протидії загрозам, пов'язаним із саморобними вибуховими пристроями (Counter-Improvised Explosive Device Training and Awareness);
- Серія заходів із вивчення проблематики безпеки критичної інфраструктури (Critical Infrastructure Learning Series).

Специфічний для хімічного сектору напрям діяльності:

- семінари й тренування для представників хімічної промисловості та інших заінтересованих сторін галузі (Security Seminars & Exercises for Chemical Industry Stakeholders). У рамках цього напряму діяльності МВБ підтримує виконання запитів від різноманітних рад та асоціацій галузі, а також від агентств з управління надзвичайними ситуаціями щодо виступів, навчальних курсів, виставок та тренувань, залучаючи до цієї роботи експертів і фахівців міністерства та його регіональних підрозділів.

Крім того, сторінка сайту МВБ, присвячена навчанню для хімічного сектору, має розділ «*Знайди додаткові можливості для навчання*» (Find Additional Training Opportunities), який надає інформацію про курси, семінари та освітні програми, що стосуються інших аспектів безпеки КІ, включно і її кібербезпеку.

Сучасні підходи до забезпечення безпеки КІ враховують її нерозривний зв'язок із *кібербезпекою*, і усвідомлення цього факту знаходить своє відображення у національних законодавствах, і українському також [120]. З упевненістю можна стверджувати, що значення проблематики кібербезпеки у захисті КІ у подальшому буде лише збільшуватися. Що стосується конкретних форм та інструментів навчання з питань кібербезпеки, то цей розділ містить посилання на такі спеціалізовані ресурси:

- сайт Національної ініціативи щодо кар'єри та досліджень у сфері кібербезпеки (National Initiative for Cybersecurity Careers and Studies, NICSS) [121], який пропонує у США понад 3000 курсів з цієї тематики, і ця кількість постійно зростає;
- сайт Програми безпеки систем управління (Control Systems Security Program) [122], який підтримує Група реагування на надзвичайні кіберподії, пов'язані з промисловими системами управління (The Industrial Control Systems Cyber Emergency Response Team, ICS-CERT);
- сайт заходів під назвою «*Кібершторм: захищаючи кіберпростір*» (cyber-storm-securing-cyber-space) [123]. На цьому сайті розміщено інформацію про фінансовані урядом та схвалені конгресом США тренування національного рівня для підвищення готовності державного та приватного секторів до кібератак. Ці тренування проводяться кожні два роки, починаючи з 2006 р.

Таким чином, підсумовуючи результати короткого огляду підходів до організації підготовки кадрів і населення щодо захисту та забезпечення стійкості КІ на прикладі хімічного сектору КІ в США, до найкращої практики у цьому питанні слід віднести таке:

1. Увесь комплекс навчальних курсів та інших навчальних інструментів та відповідної інформації ділиться на два основні модулі: *загальний* (для всіх секторів КІ) та *специфічний* (для кожного окремого сектору).

---

[120] Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держав: Постанова Кабінету Міністрів України від 23.08.2016 № 563 // База даних «Законодавство України»/ВР України. URL: http://zakon2.rada.gov.ua/laws/show/563-2016-п

[121] National Initiative for Cybersecurity Careers and Studies. URL: http://nicss.cert.gov

[122] The Industrial Control Systems Cyber Emergency Response Team. URL: http://ics-cert.us-cert.gov

[123] Cyber Storm: Securing Cyber Space. URL: https://www.dhs.gov/cyber-storm-i

2. *Загальний модуль* включає переважно безкоштовні чи з незначною оплатою навчальні курси та інформаційні матеріали з актуальних питань, які стосуються: підвищення безпеки на робочому місці; настанов для ситуацій, спричинених діями «активного стрільця»; виявлення незаконного стеження та реагування на нього; протидії застосування саморобних вибухових пристроїв; забезпечення безпеки на об'єктах роздрібної торгівлі; захисту критичної інфраструктури проти внутрішніх порушників; протидії крадіжкам і переключенню матеріалів та обладнання тощо.

Зазвичай навчання та надання інформації для заходів та інструментів загального модуля здійснюється на безоплатній основі або за дуже низькими цінами.

3. *Специфічний для кожного сектору модуль* обов'язково має включати навчальні заходи щодо підвищення інформованості з питань ЗКІ ключових суб'єктів цього процесу – представників керівної ланки компетентних державних органів, у т. ч. органів управління; правоохоронних органів; служб екстреної допомоги; власників та операторів об'єктів КІ тощо.

4. Подальше зростання ролі ІТ-технологій у житті окремої людини, суспільства та держави в цілому зумовлює виключне значення питань кібербезпеки для забезпечення безпеки та стійкості КІ. У провідних країнах світу це знаходить своє відображення в активному розвитку навчальних курсів та інших освітніх інструментів з питань кібербезпеки у рамках підготовки кадрів і населення для ЗКІ.

Як зазначалось у попередніх розділах, захист і забезпечення належної стійкості КІ є комплексним завданням, до виконання якого тією чи тією мірою має бути залучено широке коло осіб, починаючи від керівників вищих ланок державних органів та корпорацій до представників місцевих громад і населення. Очевидно, що цільові аудиторії процесу підготовки кадрів і населення щодо проблематики КІ доцільно визначати залежно від обов'язків та ролі певної категорії осіб у процесі захисту та забезпечення стійкості КІ.

Якщо стосовно підвищення інформованості щодо основ захисту та забезпечення стійкості КІ (іншими словами, ознайомлення з базовими знаннями щодо КІ) бажано, щоб таким навчанням було охоплено якомога більше представників населення, працівників підприємств і компаній, керівників і управлінців різного рівня та з різними функціональними обов'язками, то спеціалізоване навчання

потребує адресності навчальних матеріалів та конкретного визначення цільової аудиторії.

У цьому питанні має сенс послатися на передовий досвід *Всесвітнього інституту з фізичної ядерної безпеки* (World Institute for Nuclear Security, WINS) [124]. Одним із головних завдань цієї провідної спеціалізованої неприбуткової міжнародної організації, розташованої у Відні (Австрія), є поширення знань із фізичної ядерної безпеки (ФЯБ) та підготовка кадрів для цієї сфери.

При WINS створено академію, яка пропонує цілу низку навчальних курсів і матеріалів стосовно різних аспектів забезпечення фізичної ядерної безпеки. Усі категорії учасників курсів мають пройти базовий курс (foundation module) із ФЯБ, та, крім того, хоча б один зі спеціальних курсів, розроблених для таких категорій осіб (цільових аудиторій) [125]:

- державні управлінці вищої ланки та члени рад директорів великих компаній;
- керівники компаній, що мають ядерні матеріали та ядерні технології;
- наукові співробітники та інженерно-технічний персонал;
- управлінці з питань реагування на інциденти, пов'язані з фізичною безпекою ядерних об'єктів;
- особи, відповідальні за підтримання зв'язку з населенням та громадянським суспільством;
- управлінці, які несуть відповідальність за фізичну безпеку радіоактивних джерел;
- управлінці з питань виконання програм із фізичної безпеки;
- регулятори фізичної ядерної безпеки;
- управлінці з питань безпеки перевезень ядерних матеріалів.

Природно, що наведений список відображає специфіку ядерної галузі, але аналогічний загальний підхід до формування цільових аудиторій для підготовки кадрів і навчання достатньо просто можна розповсюдити на більшість інших секторів КІ, ураховуючи специфічність безпекових умов, загроз та ризиків, притаманних кожному сектору.

---

[124] World Institute for Nuclear Security/Site. URL: www.wins.org

[125] WINS Academy Nuclear Security Management Certification Programme. Reference Guide. (2014, November). URL: https://www.wins.org/files/2014_11_24-wins_academy_reference-guide_version1.pdf

Р о з д і л 3

МЕТОДОЛОГІЧНІ ТА ОРГАНІЗАЦІЙНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1. Модель організації взаємодії залучених суб'єктів у рамках державної системи забезпечення безпеки та стійкості критичної інфраструктури

Стратегією національної безпеки України [126] визначені пріоритетні завдання національної політики безпеки, одним із яких є *забезпечення безпеки критичної інфраструктури*.

Світовий досвід чітко демонструє тенденцію до об'єднання питань забезпечення захисту (protection) та безпеки критичної інфраструктури (security, на відміну від safety, тобто техніки безпеки) з питаннями забезпечення її стійкості (resilience).

Враховуючи те, що термін «стійкість» іще не визначений українським законодавством, а лише входить у практику використання, фахівцями НІСД запропоновано методологічний підхід до розмежування змісту понять «стійкість», «захист», «безпека» та, відповідно, визначення завдань різних суб'єктів реалізації державної політики у сфері захисту критичної інфраструктури [127]. Це уможливлює чітко визначити зміст діяльності суб'єктів системи забезпечення БСКІ та формалізувати вимоги щодо такої діяльності на окремих етапах.

По-перше, визначається завдання та пропонується методологія виокремлення того, *що саме потребує захисту.* Зокрема, потрібно ідентифікувати об'єкти/системи/ресурси, які надають життєво важливі для безпеки людини, суспільства і держави послуги та

[126] Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26.05.2015 № 287/2015 // База даних «Законодавство України»/ВР України. URL: https://zakon.rada.gov.ua/laws/show/287/2015#n7

[127] Детальніше див. *підрозділ 1.2* та «Зелену книгу з питань захисту критичної інфраструктури».

функції. А для цього, на думку фахівців НІСД, доцільно використати ризик-орієнтовані підходи, які вже отримали розповсюдження в Україні в низці галузей, зокрема ядерній, ІТ, авіаційній [128].

По-друге, встановлюється вимога визначення того, *від чого (кого) потрібно захищати КІ*. Зокрема, на національному рівні необхідно визначитися з переліком усіх видів загроз критичній інфраструктурі. Відтак запропоновані фахівцями НІСД підходи дають можливість розробити відповідні методологічні засади щодо формалізації виконання цього завдання [129].

По-третє, фіксується вимога визначення рівня готовності операторів КІ щодо оцінювання ними загроз та ступеня захищеності ОКІ від цих загроз через надання відповіді на питання: *як саме ОКІ захищатимуться від ідентифікованих загроз*. Це завдання ставить вимогу із розроблення методичних, організаційних та ресурсних засад забезпечення захисту КІ та їх фіксації у нормативних документах [130].

По-четверте, встановлюється вимога мати ефективну систему планування та координації дії учасників системи БСКІ, зокрема на етапах *запобігання реалізації загроз*, *реагування на випадок виникнення кризи та відновлення функціонування КІ* як на національному, так і на галузевому/місцевому/об'єктовому рівнях [131].

По-п'яте, вимагається створення *узгодженої системи ВОІ між учасниками системи* БСКІ відповідно до кращої світової практики [132], виникає необхідність враховувати українську практику (про це див. далі).

Запропонований фахівцями НІСД теоретико-методологічний підхід дозволяє поєднати зусилля різних чинних державних систем захисту та реагування на кризові ситуації (системи цивільного захисту, фізичного захисту, кіберзахисту, контртерористична система тощо) в узгоджену систему, яка буде спроможна реагувати на загрози будь-якого виду.

Пропонований підхід, ураховуючи досвід передових країн світу, дає змогу методологічно уніфікувати інструменти формалізації вимог та організації діяльності залучених суб'єктів у процесі забезпе-

[128] Див. *підрозділ 3.4*.
[129] Див. *підрозділи 3.3* та *3.5*.
[130] Див. *підрозділ 3.6*.
[131] Див. *підрозділ 2.3* та *Додаток 2*.
[132] Див. *підрозділ 2.4*.

чення БСКІ, що підвищить ефективність дій як окремих суб'єктів системи, так і системи у цілому. Зокрема, варто виокремити основні інструменти регламентації діяльності учасників системи БСКІ [133] за рівнями:

1. *На рівні оператора інфраструктури* необхідно врегулювати вимоги до оператора (в межах його відповідальності) щодо забезпечення БСКІ:

- *інженерно-технічні та організаційні стандарти* – для формалізації та врегулювання аспектів функціонування системи, щодо яких можлива кількісна оцінка рівня загроз (на основі фізичних та технічних характеристик або імовірнісних оцінок): встановлення комплексу інженерно-технічних та організаційних вимог для врегулювання заходів забезпечення безпеки та стійкості (технічні умови; стандарти виготовлення та роботи устаткування; стандарти безпеки інфраструктури, стандарти енергопостачання) [134], а також посадові інструкції та інструкції щодо організації систем захисту; стандарти менеджменту; плани аварійного реагування тощо;
- *проектна загроза (об'єктова)* – для формалізації та врегулювання аспектів, які проблематично оцінити у кількісному вимірі (наприклад, ціль, місце, час та спосіб цілеспрямованого порушення функціонування КІ (диверсія, кібератака)).

[133] На прикладі формалізації вимог до забезпечення стійкості такого сектору КІ як система електропостачання (див. Суходоля О. М. Стійкість енергетичної системи чи стійкість енергозабезпечення споживачів: постановка проблеми. *Стратегічні пріоритети.* 2018. № 2. С. 101–117).

[134] Такі стандарти передбачені новим законодавством ЄС щодо безпеки енергопостачання, зокрема Регламент № 1938/2017 передбачає:

– *інфраструктурні стандарти* (ст. 5 Регламенту), що вимагають від країн-членів передбачити заходи запобігання переривання постачання за умови, коли один найбільший елемент системи (джерело, маршрут постачання) припиняє свою роботу (критерій N-1, що розраховується за встановленою формулою), тобто потужності інфраструктури, яка залишається функціонувати, мають забезпечити виконання функції (енергозабезпечення) у повному обсязі протягом дня найбільшого споживання (при статистичній вірогідності переривання раз на 20 років);

– *стандарти постачання* (ст. 6 Регламенту), які вимагають вжити заходів щодо забезпечення постачання енергії захищеним категоріям споживачів за визначеного рівня загроз: (а) екстремальні температурні режими протягом 7 днів споживання (при статистичній вірогідності раз на 20 років); період у 30 днів екстремально високого споживання (при статистичній вірогідності раз на 20 років); період у 30 днів споживання при порушенні функціонування одного найбільшого елемента системи (джерело, маршрут постачання) при середніх умовах зимового періоду.

Проектна загроза [135] (об'єктова) має надати допомогу оператору КІ щодо ідентифікації загроз та встановити вимоги стосовно рівня захисту ОКІ відповідно до ризик-аналізу (оцінки рівня загроз), здійсненого на національному рівні відповідними складовими сектору безпеки і оборони;

- *паспорт безпеки* – для формалізації дій оператора (стосовно прогнозованих і непрогнозованих аспектів) та визначення заходів забезпечення стійкості КІ на рівні оператора [136]. Паспорт безпеки має стати процедурою постійного та періодичного обліку ОКІ. У свою чергу, облік ОКІ включатиме виконання комплексу заходів із забезпечення збору, накопичення та актуалізації необхідної інформації щодо заходів із забезпечення БСКІ на національному рівні;
- *плани оператора* (захисту, реагування, відновлення) – плани заходів оператора, спрямовані на забезпечення функціонування визначених ОКІ. Ці плани формалізують вимоги до дій оператора щодо забезпечення безпеки та стійкості ОКІ, а також процедур взаємодії з іншими суб'єктами державної системи БСКІ.

2. *На рівні сектору КІ/регіону* необхідно врегулювати вимоги до оператора та інших учасників, об'єднаних інфраструктурою, у випадках, коли можливостей оператора не вистачатиме для адекватного реагування, зокрема:

- *вимоги* – для формалізації вимог до діяльності операторів критичної інфраструктури щодо забезпечення стійкості КІ [137] відповідно до рівня загроз та режиму функціонування інфраструктури (штатний режим функціонування; режим реагу-

[135] Див. *Додаток 1.6*.

[136] Див. *Додаток 1.5*.

[137] Ці *«Вимоги»* можуть бути формалізовані у вигляді програм, правил або планів. Так, на виконання ст. 16 Закону України «Про ринок електричної енергії» (див.: https://zakon.rada.gov.ua/laws/show/2019-19) розроблено *«Правила про безпеку постачання електричної енергії»*, які визначають: 1) критерії/види порушень безпеки постачання електричної енергії; 2) заходи із забезпечення безпеки постачання електричної енергії; 3) заходи, що вживатимуться у випадках ризику порушення безпеки постачання електричної енергії; 4) заходи, що вживатимуться у разі порушення безпеки постачання електричної енергії; 5) заходи, обов'язкові до вжиття учасниками ринку (крім споживачів) для забезпечення безпеки постачання електричної енергії захищеним споживачам; 6) процедуру ініціювання вжиття необхідних заходів; 7) порядок застосування необхідних заходів і строк їх дії; 8) порядок інформування про вжиття необхідних заходів; 9) обов'язки та відповідальність суб'єктів владних повноважень та учасників ринку щодо забезпечення безпеки постачання електричної енергії (див.: https://zakon.rada.gov.ua/laws/show/z1076-18).

вання на випадок реалізації загрози; режим функціонування в кризовій ситуації; режим відновлення);

- *проектну загрозу (секторальну)* – для оцінки імовірного сценарію реалізації загроз для окремих секторів (галузей) критичної інфраструктури та специфікації вимог до захисту КІ окремого сектору (інфраструктури забезпечення окремої життєво важливої функції суспільства), що має свої специфічні вразливості та наслідки;
- *план захисту КІ* – для забезпечення готовності до реагування на випадок виникнення загроз порушення цільової функції, які забезпечує відповідний сектор (галузь). Зазначений секторальний план захисту, на відміну від плану оператора КІ, має передбачати дії всіх суб'єктів, залучених до забезпечення БСКІ (секторальної КІ) [138];
- *план реагування* – для забезпечення координації реагування всіх учасників на випадок кризової ситуації (оператори, учасники відповідного ринку, споживачі послуг КІ, органи влади). Секторальний план реагування потребує наявності всіх необхідних ресурсів для забезпечення безперервності надання життєво важливої функції (послуги) навіть у випадку втрати окремих ОКІ [139];
- *регламент обміну інформацією* – для інформаційного забезпечення запобігання та реагування на загрози, налагодження обміну інформацією між учасниками планів запобігання та реагування на кризові ситуації у відповідних секторах.

3. *На національному рівні* забезпечення КІ необхідно врегулювати вимоги щодо довгострокового планування розвитку КІ з урахуванням прогнозу розвитку технологічних, економічних, управлінських аспектів функціонування КІ та безпекового середовища на національному та глобальному рівнях [140], а можливими інструментами формалізації можуть бути:

- *ризик-аналіз* – для оцінки рівня загроз безпеці та стійкості КІ на національному рівні та попередньої оцінки спроможностей

[138] Див. *Додаток 1.1*.
[139] Див. *Додаток 1.2*.
[140] Доцільно визначити компетентним органом для цього комплексу питань спеціальний орган виконавчої влади, відтак пропонується утворення Урядового центру з питань захисту та забезпечення стійкості КІ. Зазначений центр має забезпечувати методологічну єдність підходів щодо реагування на різні типи загроз.

державної системи захисту КІ, та формування вимог до організації діяльності всіх суб'єктів системи [141];

- *проектна загроза (національна)* – для формування моделі загроз КІ на національному рівні на основі *Сценарного планування* та *Розвідувальних оцінок* загроз стійкості КІ;
- *перелік об'єктів (реєстр) КІ* – для ідентифікації сфери дії державної системи БСКІ, оцінки ресурсних потреб та встановлення вимог до рівня забезпечення БСКІ відповідно до категоризації об'єктів;
- *національний реєстр КІ* – для визначення найбільш важливої критичної інфраструктури, щодо якої на національному рівні формуються особливі вимоги та заходи забезпечення їх захисту;
- *національний план БСКІ* – для залучення ресурсів та координації зусиль на національному рівні, що має формалізувати заходи із запобігання виникнення загроз і реагування на кризову ситуацію та відновлення функціонування КІ;
- *національний уповноважений орган* – для методологічного забезпечення та координації діяльності учасників у сфері забезпечення БСКІ.

Структурна схема діяльності суб'єктів державної системи БСКІ, запропонована фахівцями НІСД у рамках вищенаведеного підходу, наведена на *рис. 3.1.*, а модель організації системи управління та координації – на *рис. 3.2*.

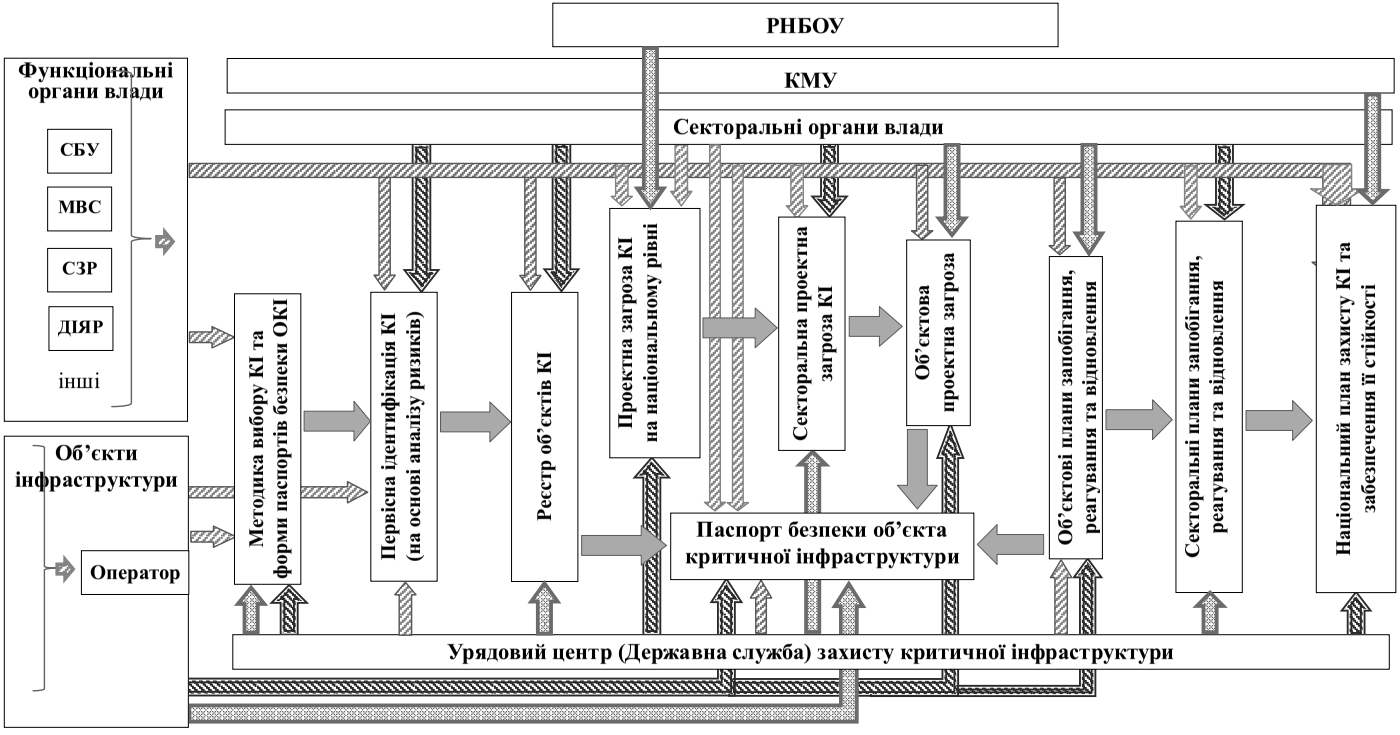
Ці схеми побудовані з урахуванням досвіду роботи чинних державних систем захисту і реагування, які функціонують у рамках, що визначені окремими комплексами законодавчих та нормативних актів. До таких систем перш за все слід віднести вже згадані системи цивільного захисту, боротьби з тероризмом, фізичного захисту ядерних матеріалів та установок, кіберзахисту.

Функціонування існуючих систем захисту і реагування координується окремими органами державної влади (надалі – функціональні органи) у державній системі БСКІ [142].

---

[141] Див. *Додаток 1.3*.

[142] Детальніше про відмінності у завданнях функціональних органів див.: Зелена книга з питань захисту критичної інфраструктури в Україні. URL: http://www.niss.gov.ua/articles/2213/ ; Kondratov, S., Bobro, D., Horbulin, V., et al. (2017). *Developing The Critical Infrastructure Protection System in Ukraine*. (O. Sukhodolia, Ed.). Kyiv: NISS. (184 p.). URL: http://en.niss.gov.ua/content/articles/files/niss_EnglCollection_druk-24cce.pdf



Примітка:

Стрілка, заштрихована з нахилом вправо – суб'єкт системи, що надає інформацію, пропозиції та/або погоджує документ.

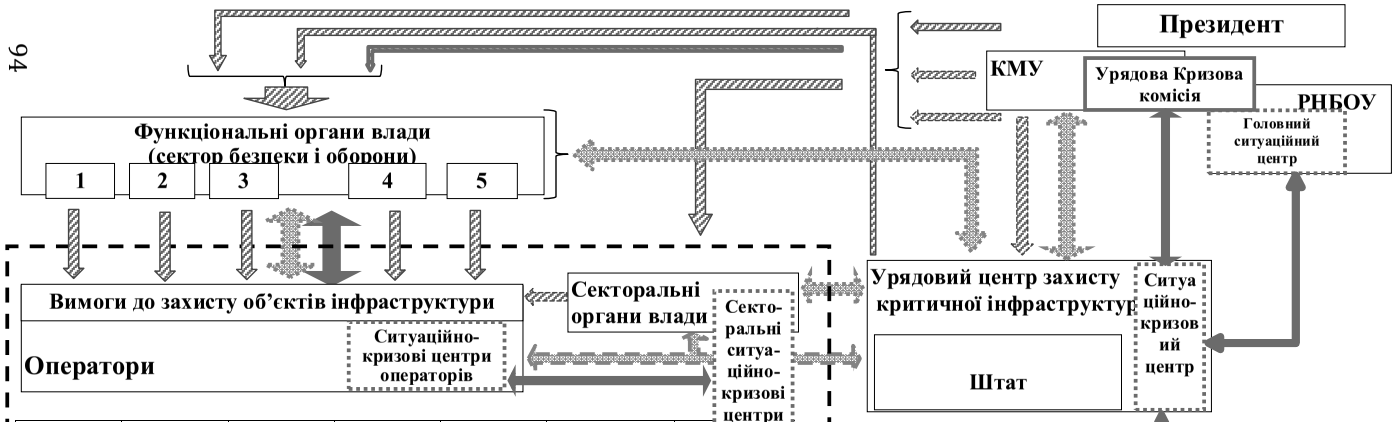
Стрілка, заштрихована з нахилом вліво – суб'єкт системи, що розробляє проект документа.

Стрілка, заштрихована хрестиком – суб'єкт системи, що затверджує документ.

Стрілка, заштрихована суцільно – зв'язок між документами.

Рис. 3.1. Структурна схема діяльності суб'єктів державної системи БСКІ

Джерело: складено автором.



System 1 (цвільний захист)	*System 2* (анти-терор)	*System 3* (фізичний захист)	*System 4* (кібер-захист)	Об'єкт	Оператор	Сектор
x	**x**		**x**	**Об (111)**	Operator 11	**Sector 1**
	x		**x**	**Об (121)**	Operator 12	(зв'язок)
x	**x**	**x**	**x**	**Об (211)**	Operator 21	**Sector 2**
x	**x**	**x**	**x**	**Об (212)**	Operator 21	(енерго)
x			**x**	Об (221)	Operator 22	
	x		**x**	**Об (311)**	Operator 31	**Sector …**
	x		**x**	Об (321)	Operator 32	
x	**x**			Об (1011)	Operator 1	**Sector 10**
x				Об (1021)	Operator 2	

Примітка.
Об(і) – об'єкти інфраструктури, управління якими здійснюють оператори у відповідних секторах економіки, діяльність яких регулюється в рамках чинних державних систем захисту і реагування (позначено **x**); виділені жирним шрифтом – внесені до переліку об'єктів КІ.

Стрілка, заштрихована з нахилом вправо – основний напрям доведення законодавчих та організаційних вимог до захисту КІ.
Стрілка, заштрихована хрестиком – основні напрями обміну інформацією та взаємодії у нормальному режимі.
Стрілка, заштрихована суцільно – основні напрями інформаційних повідомлень у кризовому режимі.

Рис. 3.2. Модель організації системи управління та координації в рамках державної системи БСКІ

Джерело: складено автором.

Поряд із функціональними органами на *рис. 3.2* наведено *секторальні органи*, котрі відображають органи державної влади (переважно центральні органи виконавчої влади), у компетенції яких – завдання формування та реалізації державної політики у відповідних сферах життєдіяльності суспільства. Саме секторальні органи будуть відповідальними за формування та реалізацію політики БСКІ у відповідних секторах.

Визначення секторів КІ та відповідальних органів державної влади за забезпечення БСКІ відповідних секторів є окремим важливим завданням, що потребуватиме детального опрацювання Урядом України. Тим не менш, відповідно до запропонованого методичного підходу щодо визначення секторів КІ на основі виділення життєво важливих функцій забезпечення життєдіяльності суспільства можна запропонувати орієнтовний *Перелік секторів КІ* та відповідальних органів влади (див. *Додаток 1.4*).

Наведена модель організації системи управління та координації в рамках державної системи БСКІ (*рис. 3.2*) відображає суб'єктів державної системи ЗКІ та основні завдання, якими вони опікуються:

1) *Кабінет Міністрів України* – формує та реалізує державну політику забезпечення БСКІ, створює необхідну організаційну, інституційну та нормативно-правову основу діяльності суб'єктів державної системи;
2) *Рада національної безпеки і оборони України* – здійснює координацію дій сектору безпеки і оборони та контроль за дотриманням вимог законодавства у сфері захисту КІ; затверджує Проектну загрозу КІ на національному рівні, забезпечує проведення *Національної оцінки ризиків*;
3) *Урядовий центр безпеки та стійкості (УЦБС) – Національний уповноважений орган* – забезпечує функціонування державної системи ЗКІ, а саме:
   - координацію взаємодії відповідних державних систем з питань забезпечення БСКІ;
   - розроблення єдиної методологічної основи функціонування державної системи БСКІ;
   - обмін інформацією між суб'єктами системи;
   - нагляд за дотриманням вимог законодавства.

У рамках УЦБС, як і секторальних органів державної влади, створюються ситуаційно-кризові центри (СКЦ), які мають забезпечити

ВОІ у всіх режимах функціонування БСКІ (докладно про засади функціонування СКЦ див. *підрозділ 3.2*);

4) *секторальні органи державної влади* (Мінінфраструктури, Мінпаливенерго, МОЗ та ін.) – несуть відповідальність за формування політики у визначених секторах КІ. Розробляють плани сектору, в яких відображають загрози всіх типів і заходи запобігання та реагування на їх реалізацію, забезпечення функціонування КІ відповідного сектору в кризовій ситуації та найшвидшого відновлення критичної інфраструктури для забезпечення сталого надання життєво важливих функцій/послуг;
5) *функціональні органи державної влади* (СБУ, Держспецзв'язок, МВС, Держатомрегулювання та ін.) – несуть відповідальність за врахування проблематики захисту КІ у діяльності відповідно до своїх повноважень. Формують вимоги щодо забезпечення БСКІ у відповідних сферах; надають секторальним органам влади, регуляторам, власникам та операторам інфраструктури консультації щодо загроз КІ та заходів із їх нейтралізації. У рамках визначених завдань та повноважень надають допомогу щодо фізичної та персональної безпеки, спрямовану на мінімізацію ризику та зменшення вразливості до тероризму, диверсій (саботажу), кібер- та інших загроз національній безпеці;
6) *оператори інфраструктури* – проводять оцінку ризиків на рівні об'єктів (ресурсів, мереж, систем), якими вони управляють, та розробляють заходи щодо забезпечення їхньої безпеки та стійкості, залучення інвестицій у систему захисту, проводять навчання тощо. Оператори у встановленому законодавством порядку забезпечують розробку та затвердження відповідних документів, що забезпечують виконання відповідних заходів захисту КІ, зокрема паспортів безпеки ОКІ, планів запобігання, реагування, відновлення тощо;
7) *місцеві органи державної влади* – визначають та оцінюють у межах своїх повноважень імовірність і наслідки можливих кризових ситуацій внаслідок реалізації загроз КІ. Розробляють плани запобігання виникнення кризових ситуацій, які можуть вплинути на громадськість; реагування на кризи та відновлення надання життєво важливих функцій/послуг.

Узагальнену модель ВОІ в системі БСКІ наведено в *табл. 3.1*, завдання суб'єктів державної системи захисту критичної інфраструктури – у *табл. 3.2*.

Інструментом формалізації функціонування державної системи БСКІ виступатиме *Національний план захисту критичної інфраструктури*, який зафіксує завдання, послідовність дій та механізм координації всіх залучених суб'єктів у різних режимах функціонування державної системи.

Пропозиції щодо структури та змісту Національного плану захисту критичної інфраструктури, сформовані відповідно до запропонованої моделі функціонування державної БСКІ в Україні, наведено в *Додатку 2*.

Деталізація запропонованої моделі та засади правового врегулювання функціонування системи захисту критичної інфраструктури відображені в *Додатку 3* «Пропозиції до проекту Закону України "Про критичну інфраструктуру"».

Таблиця 3.1. **Узагальнена модель взаємодії та обміну інформацією в системі безпеки та стійкості критичної інфраструктури**

Суб'єкт	Отримує «знизу» (від об'єктів критичної інфраструктури)	Отримує «зверху» (від суб'єктів системи захисту КІ)	
Оператор критичної інфраструктури	Інформацію щодо оцінки загроз та стану системи захисту. Інформацію щодо ситуації на об'єктах. Запити щодо ресурсного забезпечення системи захисту. Запит про допомогу у випадку кризи	Інформацію щодо включення об'єктів до Переліку КІ (та Реєстру КІ). Вимоги законодавства щодо захисту КІ. Запит на інформацію щодо стану захисту; щодо загроз. Надання допомоги	
Секторальний орган влади (Міненерговугілля, Мінінфраструктури та ін).	Пропозиції щодо включення об'єктів до секторального переліку об'єктів КІ. Проекти планів операторів КІ щодо запобігання, реагування та відновлення КІ. Інформацію щодо ситуації на об'єктах. Запит про допомогу у випадку кризи	Інформація про включення об'єктів до переліку КІ (та Реєстру КІ). Вимоги законодавства щодо захисту КІ в частині вимог до оператора КІ. Вимоги законодавства до секторального органу в частині захисту КІ. Запит на інформацію щодо стану захисту об'єктів КІ; щодо оцінки загроз КІ. Доручення щодо реагування в кризовому режимі функціонування. Надання допомоги	
Функціональний орган влади (ДСНС, СБУ та ін.)	Проекти паспортів безпеки об'єктів КІ. Проекти планів операторів КІ щодо запобігання та реагування на загрози КІ. Інформацію щодо ситуації на об'єктах. Запит на інформацію щодо оцінки загроз стосовно КІ. Запит про допомогу у випадку кризи	Вимоги законодавства щодо захисту КІ, у т. ч. до функціонального органу в частині захисту КІ. Запит на інформацію щодо стану захисту об'єктів КІ, оцінки загроз КІ. Надання доручень щодо реагування у кризовому режимі функціонування.	

	Вихідна дія/інформація/документ	Здійснює
	Пропозиції щодо включення до переліку об'єктів КІ (Реєстру КІ). Інформація щодо стану захисту відповідно до вимог законодавства. Запит на інформацію щодо загроз. Запити до секторального та функціональних органів влади щодо ресурсного забезпечення системи захисту. Запит до секторального органу влади про допомогу у випадку кризи	Затвердження корпоративних вимог щодо організації захисту КІ відповідно до вимог законодавства. Розробку та затвердження Паспорта безпеки об'єктів КІ. Розробку планів запобігання, реагування та відновлення КІ. ВОІ із іншими суб'єктами системи захисту
	Секторальний перелік об'єктів КІ, пропозиції щодо включення до Реєстру КІ. Пропозиції щодо врахування потенційних загроз КІ та наслідків їх реалізації. Запит на інформацію щодо загроз до Урядового центру та функціональних органів влади. Запити до Уряду та інших суб'єктів системи захисту КІ щодо ресурсного забезпечення системи захисту КІ. Запити до Уряду про допомогу у випадку кризи. Інформаційні повідомлення в рамках системи ВОІ залежно від режиму функціонування системи захисту КІ	Розробку та затвердження секторальних вимог законодавства щодо організації захисту КІ. Погодження паспортів безпеки об'єктів КІ. Затвердження планів операторів КІ щодо запобігання, реагування та відновлення КІ. Організацію обміну інформацією у секторі, здійснення її аналізу та оцінку загроз і ризиків у рамках секторального СКЦ. Організацію ВОІ із іншими суб'єктами системи захисту. Розроблення проекту Секторальної проектної загрози. Затвердження Плану взаємодії на випадок кризової ситуації. Затвердження Плану відновлення функціонування секторальної КІ
	Пропозиції щодо включення до секторальних переліків об'єктів КІ та Реєстру КІ. Розвідувальні оцінки щодо загроз КІ та наслідків їх реалізації. Інформаційні повідомлення в рамках системи ВОІ залежно від режиму функціонування системи захисту КІ	Розробку та затвердження функціональних вимог законодавства щодо організації захисту КІ. Погодження паспортів безпеки об'єктів КІ. Погодження планів операторів КІ щодо запобігання та реагування на загрози КІ. Формування пропозицій до Національної та секторальних проектних загроз. Організацію ВОІ із іншими суб'єктами державної системи захисту КІ. Контроль за дотриманням вимог законодавства у своїй сфері

Суб'єкт	Отримує «знизу» (від об'єктів критичної інфраструктури)	Отримує «зверху» (від суб'єктів системи захисту КІ)	
Урядовий центр безпеки і стійкості	Пропозиції щодо включення об'єктів до Реєстру КІ. Проекти паспортів безпеки об'єктів КІ. Проекти секторальних планів, Секторальної проектної загрози. Проекти секторальних планів взаємодії на випадок кризової ситуації. Проекти секторальних планів відновлення функціонування КІ	Вимоги законодавства щодо захисту КІ. Запит на інформацію щодо стану захисту об'єктів КІ; щодо оцінки загроз КІ. Запит на інформацію щодо розвитку ситуації в кризовій ситуації	
Кабінет Міністрів України	Інформацію щодо ситуації на об'єктах. Запит на інформацію щодо оцінки загроз стосовно КІ. Запити щодо зміни режимів функціонування системи захисту КІ. Запит про допомогу у випадку кризи	Вимоги законодавства щодо захисту КІ	
Рада національної безпеки і оборони України	Інформацію щодо ситуації на об'єктах. Запит на інформацію щодо оцінки загроз стосовно КІ. Запити щодо зміни режимів функціонування системи ЗКІ	Вимоги законодавства щодо захисту КІ	

Джерело: складено автором.

Продовження табл. 3.1

	Вихідна дія/інформація/документ	Здійснює
	Вимоги щодо побудови та функціонування системи захисту КІ. Запит на інформацію щодо стану та загроз КІ. Оцінка загроз та ризиків КІ. Сценарне прогнозування розвитку ситуації. Запити до Уряду та інших суб'єктів системи захисту КІ щодо ресурсного забезпечення системи захисту. Запити до Уряду щодо зміни режимів функціонування системи захисту КІ	Затвердження Реєстру КІ. Розробку проекту Національної проектної загрози КІ. Затвердження секторальних проектних загроз. Погодження паспортів безпеки об'єктів КІ. Погодження секторальних планів взаємодії на випадок КС. Погодження секторальних планів відновлення функціонування КІ. Контроль за дотриманням вимог законодавства у сфері захисту КІ
	Ресурсна допомога щодо забезпечення захисту КІ	Затвердження Національного плану захисту критичної інфраструктури
	Розвідувальні оцінки та сценарне прогнозування загроз КІ	Координацію дій сектору безпеки і оборони. Контроль за дотриманням вимог законодавства. Затвердження Національної проектної загрози

Таблиця 3.2. **Основні завдання щодо забезпечення суб'єктів БСКІ та ВОІ в окремих режимах функціонування критичної інфраструктури**

Режим функціонування	Основні завдання з реагування	Основні заходи реагування	
Нормальний режим функціонування	Моніторинг поточного безпекового стану. Аналіз безпекових процесів і тенденцій, прогнозування їх коротко-, середньо- і довгострокових наслідків. Подальший розвиток та вдосконалення процедур і механізмів ВОІ в рамках НМ СКЦ	Обмін інформацією і даними про поточний стан безпекових індикаторів, незначні безпекові інциденти, зміни у механізмах та процедурах взаємодії, нормативно-правовій базі, регламентах, протоколах тощо. Проведення аналізу та вивчення процесів і тенденцій на міжнародному, регіональному і національному рівнях, підготовка аналітичних матеріалів для їх передачі на вищі рівні системи управління; аналіз стану безпеки щодо окремих типів загроз; аналіз стану безпеки окремих типів об'єктів. Планування, підготовка й участь у проведенні навчань об'єктового, місцевого, регіонального і національного рівнів; підготовка пропозицій для удосконалення систем взаємодії	

	Основні завдання з обміну інформацією та взаємодії	Основні заходи з інформування та інформаційні потоки
	Створення мережі обміну інформацією, запровадження механізмів та інструментів взаємодії всередині мережі. Розроблення й запровадження планів, механізмів, процедур, протоколів обміну інформацією між ситуаційно-кризовими центрами, а також державними органами та іншими організаціями (у т. ч. у приватному секторі). Забезпечення інформування підрозділів сектору безпеки і оборони, служб безпеки та аварійних служб операторів про загрози та ризики кризових ситуацій. Надання та регулярне оновлення інформації для сил реагування щодо безпекових умов, що можуть вплинути на ефективність реагування у кризовій ситуації. Проведення навчань і тренувань об'єктового, місцевого, регіонального та національного рівнів для відпрацювання процедур і механізмів ВОІ. Підготовка спеціалістів та визначення алгоритмів (процедур) для інформування населення, ЗМІ та експертів у кризовій ситуації	Розвідувальна інформація від правоохоронних органів та спецслужб про наявні та потенційні загрози (може передаватися через СБУ, центри правоохоронних органів). Інформація про поточний безпековий стан об'єктів, систем, ресурсів, віднесених до критичної інфраструктури, передається до органів регулювання безпеки та спецслужб через відповідні центри та служби. Надання політичному керівництву держави інформаційно-аналітичних матеріалів стратегічного значення. ВОІ на відомчому рівні на регулярній основі у форматі щомісячних безпекових брифінгів. Передача технологічних даних з нижнього рівня на відомчий

Режим функціонування	Основні завдання з реагування	Основні заходи реагування	
Готовності та запобігання реалізації загроз	Запобігання реалізації загроз будь-якого виду; якщо неможливо – приведення до максимальної готовності системи захисту та реагування до реалізації загроз. Створення команди для прийняття оперативних рішень. Забезпечення первинного реагування. Забезпечення вчасного, ефективного та збалансованого інформування всіх суб'єктів реагування. Забезпечення виваженого інформування населення, ЗМІ та експертів	Обробка, аналіз та оцінка розвідувальної інформації про загрози і формулювання висновків щодо ймовірності реалізації загроз. Оцінка можливих сценаріїв розвитку кризової ситуації. Приведення державної системи захисту критичної інфраструктури (у т. ч. у пов'язаних секторах) до режиму готовності. Приведення сил сектору безпеки і оборони, визначених у планах захисту та реагування відповідних секторів критичної інфраструктури, у режим «підвищеної готовності». Інформування суб'єктів реагування, передача інформації в НМ СКЦ. Активація відповідних планів реагування та взаємодії для активації додаткових функціональних можливостей країни	

Продовження табл. 3.2

	Основні завдання з обміну інформацією та взаємодії	Основні заходи з інформування та інформаційні потоки
	На першому етапі здійснюється обмін інформацією між розвідувальними і правоохоронними органами, спецслужбами; формулюються висновки про достовірність загрози. Інформування вищого політичного керівництва держави (Президента, РНБОУ, КМУ) за встановленими процедурами. Прийняття рішення щодо зміни режимів функціонування державної системи захисту критичної інфраструктури та пов'язаних систем відповідно до загроз. Доведення інформації щодо зміни режимів систем до залучених учасників. Інформування операторів критичної інфраструктури та сил, що забезпечують охорону та захист (охорона оператора, підрозділи Нацгвардії, місцеві та регіональні управління СБУ, МВС, Нацполіції тощо). Інформування інших залучених органів державної влади, відповідальних за функціонування пов'язаних систем захисту та реагування (ДСНС, Міноборони, Держспецзв'язок, Держприкордонслужба). Відповідні суб'єкти системи захисту готують повідомлення для ЗМІ з метою інформування населення	Передача аналітичних матеріалів на вищий політичний рівень. Підготовка й отримання політичних та урядових рішень. Доведення оцінки розвідувальної інформації до суб'єктів системи захисту критичної інфраструктури (до відповідальних за захист суб'єктів). Доведення висновків з оцінки розвідувальної інформації до суб'єктів забезпечення, пов'язаних систем захисту та реагування. Надання звітів за результатами оцінки готовності сил та засобів реагування. Інформування населення та органів державної влади, міжнародного співтовариства щодо потенційних загроз та вжитих заходів

Режим функціонування	Основні завдання з реагування	Основні заходи реагування	
Реагування на виникнення кризової ситуації	Обмеження масштабу інциденту та стабілізація ситуації на місці подій. Забезпечення безпеки громадян та членів команд реагування. Попередня оцінка масштабів реалізації загроз, потреб у додаткових ресурсах (залучення додаткових сил та засобів сектору безпеки і оборони). Розгортання повномасштабної системи управління кризою (Міжвідомчого штабу). Забезпечення управління в режимі кризової ситуації. Недопущення ескалації кризи. Мобілізація всіх ресурсів для нейтралізації можливих загроз національній безпеці. Забезпечення стратегічної комунікації	Оповіщення про кризову ситуацію та введення в дію планів реагування. Первинне реагування силами та засобами персоналу ОКІ та зовнішніх сил, залучених відповідно до затвердженого плану. Здійснення попередньої оцінки ситуації (характеру інциденту та рівня кризової сиутації) та прийняття рішення щодо активізації Плану взаємодії із іншими силами сектору безпеки і оборони. Активація Урядового кризового центру (у разі потреби) та кризових центрів суб'єктів системи, залучених до плану реагування. Переведення державної системи захисту критичної інфраструктури (у відповідному секторі критичної інфраструктури та пов'язаних із ним секторах) до режиму реагування на кризову ситуацію. Збирання та передавання інформації для аналізу кризи, оцінювання можливих сценаріїв її розвитку в рамках мережі обміну інформацією. Разом зі здійсненням заходів із реагування секторальні органи влади забезпечують: аналіз поточної ситуації та можливих сценаріїв її розвитку; оцінку варіантів виходу з кризи; коротко-, середньо-, та довгострокове прогнозування наслідків розвитку кризи; підготовку заходів, спрямованих на захист національної безпеки; своєчасне, виважене та об'єктивне інформування вищого керівництва держави, населення, ЗМІ та експертного середовища, міжнародних структур про розвиток кризи і вжиті заходи. Документування управлінських рішень та фіксація основних подій. Здійснення запиту (за необхідності) щодо допомоги від міжнародного співтовариства	

Продовження табл. 3.2

	Основні завдання з обміну інформацією та взаємодії	Основні заходи з інформування та інформаційні потоки
	У результаті оцінки ситуації за встановленою процедурою приймається рішення про оповіщення державних органів. У результаті попередньої оцінки рівня та масштабів інциденту оператор ОКІ приймає рішення та надсилає відповідне повідомлення щодо: рівня кризової ситуації, перевищення рівня проектної загрози; необхідності залучення зовнішніх сил сектору безпеки і оборони. У результаті розгортання сил і засобів учасників плану реагування на КС створюються чотири рівні управління кризовою ситуацією: *оперативний* – на базі об'єкта КІ; *тактичний* – на базі оператора КІ, на якому здійснюється мобілізація ресурсів оператора, координація дій залучених сил і засобів реагування в рамках плану реагування; *стратегічний* – на базі СКЦ здійснюється прогнозування розвитку подій, координація дій органів влади, готуються пропозиції щодо можливих політичних рішень; *політичний* – на базі Урядового кризового центру здійснюється стратегічна оцінка ситуації, координації дій органів державної влади, інформування та взаємодія із міжнародним співтовариством. ВОІ спрямовується на: забезпечення інформаційно-аналітичної підтримки сил реагування; інформування керівництва держави; інформування населення та ЗМІ. Забезпечення інформаційно-аналітичної підтримки прийняття рішень на стратегічному і політичному рівнях управління кризою з метою нейтралізації загроз національній безпеці. Виконання необхідних заходів з підготовки до можливого переходу до режиму надзвичайного або воєнного стану	Збирання і передавання первинної оперативної інформації усіма суб'єктами системи про розвиток ситуації та загрози життю людей та довкіллю. Горизонтальний обмін інформацією між підрозділами реагування та системами реагування. Оповіщення про розвиток ситуації керівництва операторів, підрозділів первинного реагування та аварійно-рятувальних служб, залучених до реагування, підрозділів сектору безпеки і оборони. Передавання інформації від оператора ОКІ, залучених органів та сил сектору безпеки і оборони. Інформаційний обмін для забезпечення підготовки першого повідомлення для населення та ЗМІ. Регулярне інформування вищого політичного керівництва держави про розвиток кризової ситуації. Забезпечення інформаційно-аналітичної підтримки діяльності системи управління кризою (Міжвідомчий оперативний штаб; СКЦ; Урядовий центр з питань захисту КІ; Головний ситуаційний кризовий центр при РНБОУ). Підготовка заяв Президента та Уряду щодо кризової сиутації, підготовка інформаційних повідомлень для ЗМІ

Режим функціонування	Основні завдання з реагування	Основні заходи реагування	
Відновлення штатного функціонування	Відновлення нормального функціонування ОКІ. Продовження виконання заходів із пом'якшення та/або ліквідації довгострокових наслідків кризової ситуації, у т. ч. надання комплексної допомоги населенню. Аналіз наслідків кризової (надзвичайної) ситуації, планування заходів з підвищення рівня безпеки, захищеності та стійкості ОКІ	Оцінка можливості та скасування режиму кризового реагування. Прийняття рішення про поетапний перехід до відновлення функціонування безпекових систем держави у нормальному (штатному) режимі. Завершення роботи секторального Міжвідомчого штабу реагування на кризову ситуацію. При переході до етапу відновлення основна координуюча роль передається до ДСНС України або секторального органу влади. За потреби подальше управління ліквідацією довгострокових наслідків кризової ситуації передається до Державної комісії з питань техногенно-екологічної безпеки та надзвичайних ситуацій. Правоохоронні органи та спецслужби зосереджуються на розслідуванні інциденту (теракту/диверсії), аналізі причин та наслідків, а також уроків, які слід винести з цих подій	

Джерело: складено автором.

Продовження табл. 3.2

	Основні завдання з обміну інформацією та взаємодії	Основні заходи з інформування та інформаційні потоки
	Рішення про перехід до режиму відновлення приймається на політичному рівні (Урядовий центр з питань захисту КІ або Головний ситуаційний кризовий центр) на основі оцінки розвідувальної інформації, інформації від правоохоронних органів та спецслужб, а також інформації секторальних органів державної влади щодо ліквідації кризової ситуації. Правоохоронні органи, спецслужби, розвідувальні та контррозвідувальні органи держави обмінюються інформацією та даними з метою аналізу причин і наслідків інциденту (теракту/диверсії), готують пропозиції щодо вдосконалення безпекових заходів з метою зниження ризиків повторення кризової ситуації. Залучені до реагування на кризову ситуацію готують узгоджені повідомлення для інформування населення через ЗМІ, а також експертного середовища. Здійснюється інформування міжнародного співтовариства	На основі інформації (звітів, рекомендацій, інформаційно-аналітичних матеріалів) секторальних та функціональних органів влади приймається рішення про перехід до режиму відновлення та ліквідації наслідків кризової ситуації. Обмін інформацією між залученими учасниками захисту критичної інфраструктури здійснюється відповідно до запитів та форм, визначених в системі ліквідації наслідків кризових (надзвичайних) ситуацій. Обмін розвідувальною та аналітичною інформацією щодо загроз із залученням технічних експертів, узагальнення уроків, підготовка міжвідомчими групами рекомендацій та пропозицій щодо удосконалення заходів із забезпечення безпеки та стійкості критичної інфраструктури. Надання населенню виваженої, правдивої інформації про наслідки кризи, проведення брифінгів для ЗМІ та експертів. Надання звітів до міжнародних організацій щодо різних аспектів кризової ситуації

3.2. Ситуаційно-кризові центри в системі забезпечення безпеки та стійкості критичної інфраструктури

Ситуаційно-кризовий центр має функціонувати як постійно діючий окремий підрозділ органу державної влади, відповідального за формування політики у визначеному секторі критичної інфраструктури.

У загальному випадку СКЦ оперативно, в цілодобовому режимі «24/7» має здійснювати функції, пов'язанні із задачами з підтримки прийняття рішень у системі забезпечення стійкості функціонування визначеного сектору [143].

Центр має здійснювати постійний моніторинг можливих кризових (надзвичайних) ситуацій та взаємодіяти (що стане невід'ємною частиною його діяльності) з мережею національних, відомчих та корпоративних ситуаційно-кризових центрів (ситуаційних, кризових, інформаційно-кризових, інформаційно-аналітичних, центрів управління у кризових чи надзвичайних ситуаціях тощо).

Режими роботи СКЦ мають визначатись залежно від:

- *рівня загроз* – наявності інформації про загрози будь-якого характеру, у т. ч. різного ступеня достовірності;
- *етапу розвитку кризової ситуації* – первинного реагування, функціонування під час кризової (надзвичайної) ситуації, періоду відновлення (ліквідації наслідків);
- *правового стану в державі* – надзвичайний стан, особливий стан, воєнний стан.

Загалом СКЦ має здійснювати свою діяльність у чотирьох режимах функціонування БСКІ (нормальний, підвищеної готовності, кризової ситуації та відновлення нормального функціонування), а також функціонування в умовах надзвичайного (особливого) стану в державі або на окремій її території. Відповідно функції та завдання СКЦ щодо реагування на загрози, запобігання їх реалізації та ліквідації наслідків будуть змінюватись:

- нормальний режим функціонування (базовий рівень) – здійснюється обробка технологічної інформації та моніторинг стану безпеки (проводиться аналіз загроз та ризиків); можуть проводитися перевірки готовності систем до реагування;

[143] Принципи та завдання інформаційного обміну в рамках функціонування системи захисту критичної інфраструктури розкито у *підрозділі 2.4*.

- режим підвищеної готовності – інформування окремих суб'єктів системи взаємодії, попередження аварійних та охоронних підрозділів; також можуть проводитися перевірки готовності систем до реагування;
- режим функціонування в кризовій ситуації – моніторинг реалізації планів реагування та взаємодії, ліквідація кризової (надзвичайної) ситуації;
- відновлення нормального функціонування – інформаційно-координаційна підтримка ліквідації наслідків КС та відновлення життєво важливих функцій/послуг.

У зазначених режимах необхідно буде залучати ресурси та суб'єкти різних державних систем реагування та захисту, що визначатиме і вимоги до інформаційного обміну (*див. табл. 3.1, 3.2*) та, відповідно, технічного забезпечення СКЦ.

Рішення про зміну режимів функціонування СКЦ має приймати керівник органу державної влади, відповідального за реалізацію державної політики захисту КІ (секторального органу) на підставі інформації, отриманої від суб'єктів існуючих державних систем захисту та реагування (ЄДСЦЗ, ЄСЗРПТА та ДСФЗ) та з урахуванням режиму функціонування державної системи БСКІ.

З метою максимального використання ресурсів та бази діючих систем, формування механізму врегулювання наявних неузгодженостей, уникання дублювання функцій та охоплення всіх типів загроз в рамках СКЦ доцільно визначити *постійно діючу частину* (штатні працівники) та *тимчасову частину* (оперативний міжвідомчий центр), яка активується лише в окремих режимах та координує дії всіх залучених сторін.

Постійно діюча частина являє собою визначену кількість постійного персоналу, який має забезпечити функціонування СКЦ у штатному режимі та готовність технічного оснащення, необхідного для функціонування СКЦ в усіх інших режимах.

Відповідно до режиму функціонування БСКІ Урядовий ситуаційно-кризовий центр та секторальні ситуаційно-кризові центри (ССКЦ) мають забезпечити відповідні зміни режимів своєї роботи.

Для розбудови в Україні державної системи БСКІ слід, враховуючи фінансові та ресурсні обмеження України, використовувати чинні системи та механізми ВОІ для побудови мережі ситуаційно-кризових центрів. На вершині піраміди ситуаційно-кризових центрів

має перебувати Урядовий ситуаційно-кризовий центр, який має взаємодіяти із ССКЦ.

У свою чергу, ССКЦ, які взаємодіють із іншими ССКЦ та СКЦ операторів КІ, мають забезпечити оперативне опрацювання інформації та приведення її до формату, необхідного для обговорення на вищому рівні прийняття рішень.

Конкретні завдання ССКЦ щодо інформаційно-аналітичної підтримки діяльності суб'єктів державної системи БСКІ визначатимуться вимогами законодавства у сфері захисту критичної інфраструктури (див. *Додатки 1–3*), а також секторальним галузевим законодавством.

Для прикладу, у сфері енергетики ССКЦ при Міненерговугілля [144] (як органу державної влади, що визначений відповідальним за функціонування енергетичної критичної інфраструктури) має забезпечити взаємодію та обмін інформацією між залученими учасниками щодо виконання таких завдань:

- організація збирання, накопичення, аналізу та узагальнення інформації про загрози об'єктам критичної енергетичної інфраструктури, прогнозування можливого перебігу подій з метою відповідного реагування та контролю;
- проведення ризик-аналізу критичної енергетичної інфраструктури;
- забезпечення фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання та пов'язаних з ними об'єктів [145];
- забезпечення діяльності функціональних підсистем Міненерговугілля ЄДСЦЗ, реагування на аварійні ситуації [146];

---

[144] Про затвердження Положення про Міністерство енергетики та вугільної промисловості України: Постанова Кабінету Міністрів України від 29.03.2017 № 208 // База даних «Законодавство України»/ВР України. URL: http://zakon5.rada.gov.ua/laws/show/208-2017-%D0%BF

[145] Про затвердження Порядку функціонування державної системи фізичного захисту: Постанова Кабінету Міністрів України від 21.12.2011 № 1337 // База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/1337-2011-%D0%BF

[146] Про затвердження Положення про функціональну підсистему безпеки електроенергетичного та ядерно-промислового комплексів Міненерговугілля України єдиної державної системи цивільного захисту: Наказ Міненерговугілля від 11.09.2015 № 591 // База даних «Законодавство України»/ВР України. URL: https://zakon.rada.gov.ua/rada/show/v0591732-15

- розроблення та здійснення узгоджених заходів Державного плану взаємодії на випадок вчинення диверсії [147], зокрема підтримки роботи міжвідомчого оперативного штабу (який створюється відповідно до законодавства);
- залучення додаткових сил і засобів, а також відповідних сил допомоги ззовні (правоохоронні органи, підрозділи спеціального призначення, підрозділи ЗСУ, інші, утворені відповідно до законів України військові формування) у разі виникнення на об'єктах критичної енергетичної інфраструктури загрози, що перевищує об'єктову проектну загрозу;
- організації роботи підприємств, установ та організацій паливно-енергетичного комплексу в особливий період; забезпечення функціонування паливно-енергетичного комплексу, технічного прикриття та відбудови його об'єктів в особливий період [148];
- забезпечення кібербезпеки об'єктів енергетики[149];
- інформування в установленому порядку Президента України, Кабінету Міністрів України та Ради національної безпеки і оборони України про розвиток подій щодо забезпечення стійкості функціонування критичної енергетичної інфраструктури;
- забезпечення взаємодії диспетчерських служб енергетичного сектору щодо інформування та оповіщення про загрозу або виникнення кризових ситуацій, порушень у роботі об'єктів енергетики, що можуть спричинити кризові ситуації [150];

---

[147] Про затвердження державного плану взаємодії центральних та місцевих органів виконавчої влади на випадок вчинення диверсій щодо ядерних установок, ядерних матеріалів, інших джерел іонізуючого випромінювання у процесі їх використання, зберігання або перевезення, а також щодо радіоактивних відходів у процесі поводження з ними: Постанова Кабінету Міністрів України від 24.07.2013 № 598 // База даних «Законодавство України»/ВР України. URL: http://zakon0.rada.gov.ua/laws/show/598-2013-%D0%BF

[148] Про функціонування паливно-енергетичного комплексу в особливий період: Закон України від 02.11.2006 № 307-V // База даних «Законодавство України»/ВР України. URL: http://zakon5.rada.gov.ua/laws/show/307-16

[149] Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України // База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/96/2016

[150] Про затвердження Інструкції про організацію діяльності диспетчерських служб при виникненні порушень у роботі підприємств паливно-енергетичного комплексу України: Наказ Міністерства енергетики та вугільної промисловості України від 02.02.2012 № 68 // База даних «Законодавство України»/ВР України. URL: https://zakon.rada.gov.ua/go/v0068732-12

- забезпечення енергопостачання в умовах надзвичайного стану, особливого періоду та у разі надзвичайних ситуацій в Об'єднаній енергетичній системі України [151];
- здійснення моніторингу безпеки електропостачання [152];
- запровадження спеціальних режимів функціонування газотранспортних (транзитних) систем України з урахуванням узгоджених режимів спільної роботи країн ЄС та України [153];
- сприяння у питаннях щодо забезпечення готовності сил і засобів, що залучаються до проведення антитерористичних операцій та забезпечення належного рівня захисту та охорони об'єктів можливих терористичних посягань [154];
- аналітичного забезпечення Президента України, Кабінету Міністрів України та Ради національної безпеки і оборони України, інших залучених суб'єктів до реагування на кризові ситуації щодо оцінки наслідків кризової (надзвичайної) ситуації та їх вплив на енергетичну та національну безпеку в частині створення єдиної системи ситуаційних центрів державних органів, що входять до сектору безпеки і оборони, а також інших органів державної та місцевої влади відповідно до Концепції розвитку сектору безпеки і оборони України [155].

ССЦК має стати організаційно-технічним майданчиком аналітичного супроводу та координації дій різних суб'єктів реагування на кризові та надзвичайні ситуації як у частині активації Міжвідомчого оперативного штабу при Міненерговугілля, так і сприяння роботі

[151] Про електроенергетику: Закон України від 16.10.1997 № 575/97-ВР // База даних «Законодавство України»/ВР України. URL: http://zakon0.rada.gov.ua/laws/show/575/97-%D0%B2%D1%80

[152] Про затвердження Правил про безпеку постачання електричної енергії: Наказ Міністерства енергетики та вугільної промисловості України від 27.08.2018 № 448 // База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/z1076-18

[153] Про затвердження Національного плану дій: Наказ Міненерговугілля від 02.11.2015 № 687 // База даних «Законодавство України»/ВР України. URL: http://zakon2.rada.gov.ua/laws/show/z1458-15#n16

[154] Про затвердження Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків: Постанова Кабінету Міністрів України від 18.02.2016 № 92 // База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/92-2016-%D0%BF

[155] Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України»: Указ Президента України від 14.03.2016 № 92/2016 // База даних «Законодавство України»/ВР України. URL: http://zakon5.rada.gov.ua/laws/show/92/2016

СКЦ інших існуючих системи захисту та реагування, а також для підтримки Спеціальної урядової комісії (яка може бути створена за відповідного рівня загроз).

3.3. Ризик-аналіз у системі забезпечення безпеки та стійкості критичної інфраструктури

Вагомим елементом функціонування державної системи БСКІ є оцінка наслідків реалізації загроз та їх впливу на безперервність надання життєво важливих функцій та послуг суспільству та державі, а також оцінка спроможностей щодо недопущення розвитку негативних сценаріїв.

Управління ризиками є визнаним у світі комплексним підходом, що передбачає відпрацювання відповідних цілеспрямованих заходів, які можуть виявлятися в найрізноманітніших формах.

Загалом цей підхід передбачає виконання на рівні держави відповідних завдань, найбільш важливим із яких є визначення відповідних заходів та їх включення у документи державного планування. Кінцевою метою при цьому є запобігання виникненню нових і зниження відомих ризиків негативного розвитку ситуації шляхом здійснення комплексних заходів на місцевому, регіональному і загальнодержавному рівнях з урахуванням таких пріоритетів [156]: розуміння ризику; удосконалення організаційно-правових рамок управління ризиком; інвестиції в заходи зі зниження ризику з метою зміцнення потенціалу протидії; підвищення готовності до криз для забезпечення ефективного реагування та впровадження принципу «Зробити краще, ніж було» в діяльність із відновлення, реабілітації та реконструкції.

Позитивний досвід багатьох країн свідчить про те, що створення системи управління ризиком матиме низку переваг, серед яких: поліпшення координації зусиль із сусідніми державами, залучення ресурсів приватних компаній та міжнародних організацій, обмін досвідом з різними країнами світу, а також підвищення позитивного іміджу нашої держави через запровадження визнаних у світі ризик-орієнтованих підходів для підвищення стійкості держави до впливу кризових і надзвичайних ситуацій різного походження.

[156] Sendai Framework for Disaster Risk Reduction 2015–2030. URL: http://www.unisdr.org

Необхідність такого елементу в діяльності державної системи БСКІ [157] зумовлена тим, що порушення функціонування КІ призведе до порушення надання життєво важливих функцій/послуг та настання негативних наслідків для людини та довкілля, суспільства та держави. Слід зазначити, що у провідних країнах світу виходять із необхідності забезпечення БСКІ від усіх видів загроз (all hazards approach).

Розуміння неможливості забезпечити однаково високий рівень ЗКІ від усіх можливих загроз зумовило розвиток підходу, який зосереджений на вибірковому захисті конкретного об'єкта КІ від обмеженого набору відомих та відносно прогнозованих загроз, при цьому пріоритет надається тій або тій інфраструктурі залежно від ступеня її «критичності», основною мірою якої виступає *ризик* [158].

Існують різні підходи до визначення ризику [159]. Узагальнений підхід до оцінки ризиків КІ включає:

- ідентифікацію загроз, оцінку частості реалізації кожної загрози (події);
- оцінку вразливості стосовно кожної загрози, що з урахуванням її частості визначає ймовірність завдання шкоди;
- оцінку наслідків (шкоди) для найгіршого сценарію розвитку подій.

Слід зазначити, що подібний ризик-орієнтований підхід широко використовується в Україні як в управлінні техногенно-екологічною безпекою, так і іншими галузями – лідерами у сфері оцінки загроз і ризиків, зокрема в:

- авіаційній галузі при аналізі та задля забезпечення авіаційної безпеки;
- ІТ галузі при аналізі та задля забезпечення кібербезпеки;
- ядерній галузі при аналізі та задля забезпечення фізичної ядерної безпеки.

---

[157] Орієнтовні вимоги щодо структури та змісту ризик-аналізу наведено в *Додатку 1.3*.

[158] Giannopoulos, G., Filippini, R., Schimmer, M. (2012). Risk assessment methodologies for critical infrastructure protection. Part I: a state of the art. Luxembourg: Joint Research Centre of Institute for the Protection and Security of the Citizen. 70 p.

[159] Згідно з ДСТУ 2293-99 «ризик – це ймовірність заподіяння шкоди з урахуванням її тяжкості». Державний російський стандарт ГОСТ Р 52448-2005 дає таке визначення ризику: це «поєднання ймовірності завдання шкоди внаслідок того, що визначена загроза реалізована через наявність вразливості».

Так, у глобальній заяві Міжнародної організація цивільної авіації (The International Civil Aviation Organization, ICAO) про контекст ризику [160] наводиться опис картини ризику для авіаційної безпеки. На основі методики, розробленої експертами ICAO, опрацьована *мапа процесу оцінки ризику*, яка включає виявлення характерних проблем, оцінку залишкового ризику та підготовку рекомендацій. Під час цього процесу ризики оцінюються шляхом визначення: 1) загрози для конкретного об'єкта, а також засобів та методів можливого нападу; 2) ймовірності виникнення загрози; 3) наслідків нападу; 4) вразливостей; 5) залишкового ризику.

У сфері ІТ розроблені та широко впроваджуються методики оцінки загроз і ризиків, зокрема Національного інституту стандартів та технологій США (The National Institute of Standards and Technology, NIST); методологія аналізу факторів ризиків інформаційних технологій (FAIR) тощо. Узагальнена *мапа процесу аналізу ІТ ризиків* [161] містить: 1) ідентифікацію активів та визначення їхньої цінності; 2) оцінку загроз; 3) оцінку вразливостей; 4) оцінку ризиків; 5) визначення контрзаходів; 6) аналіз захищеності; 7) оцінку залишкового ризику; 8) план захисту.

Заходи, передбачені в рамках Державної системи фізичного захисту ядерних установок та ядерних матеріалів, включають увесь ланцюжок дій – від оцінки загроз та категоризації об'єктів системи до встановлення конкретних вимог щодо систем фізичного захисту (залежно від категорії об'єкта), оцінки вразливості об'єктів, оцінки ризиків наслідків, проведення перевірок систем фізичного захисту та планів взаємодії. Зазначені підходи доцільно розповсюдити і на систему захисту критичної інфраструктури [162].

Слід зазначити, що подібні ризик-орієнтовані підходи широко використовуються і в провідних країнах світу. Так, у ЄС 2015 р. розроблено документ «Методи оцінки ризику для захисту критичної

---

[160] Глобальное заявление ИКАО о контексте риска. URL: http://www.icao.int/Meetings/avsecconf/Documents/Risk%20Context%20Statement/Risk%20Context%20Statement%20-%20Abridged%20Version.Published.RU.pdf

[161] Ткаченко В. Сучасні підходи до оцінки ризиків інформаційних технологій. URL: http://slidegur.com/doc/1615456/suchasn%D1%96-p%D1%96dhodi-do-oc%D1%96nki-rizik%D1%96v-%D1%96nformac%D1%96jnih-tehnolog%D1%96j

[162] Проблеми оцінки терористичної вразливості та формування паспортів безпеки об'єктів енергетики: аналітична записка. Київ: НІСД, 2016. URL: http://www.niss.gov.ua/content/articles/files/pasport_bezpeki-3d468.pdf

інфраструктури. Частина II. Новий підхід» [163], який базується на аналізі загроз та ризиків.

При цьому в країнах ЄС з метою проведення національної оцінки ризику (National Risk Assessment) для КІ рекомендується використовувати матрицю ризику залежно від відносних наслідків впливу визначених загроз («Relative Impact») та їх імовірності («Relative Likelihood»), що використовується у ЄС і для захисту КІ.

Зазвичай для оцінки наслідків реалізації загроз та їх імовірності у ЄС використовується матриця (*рис. 3.3*) розмірністю 5 х 5, у якій наслідки оцінюються від незначних до катастрофічних, а їх імовірність/частість – від низької до високої. Для наглядного

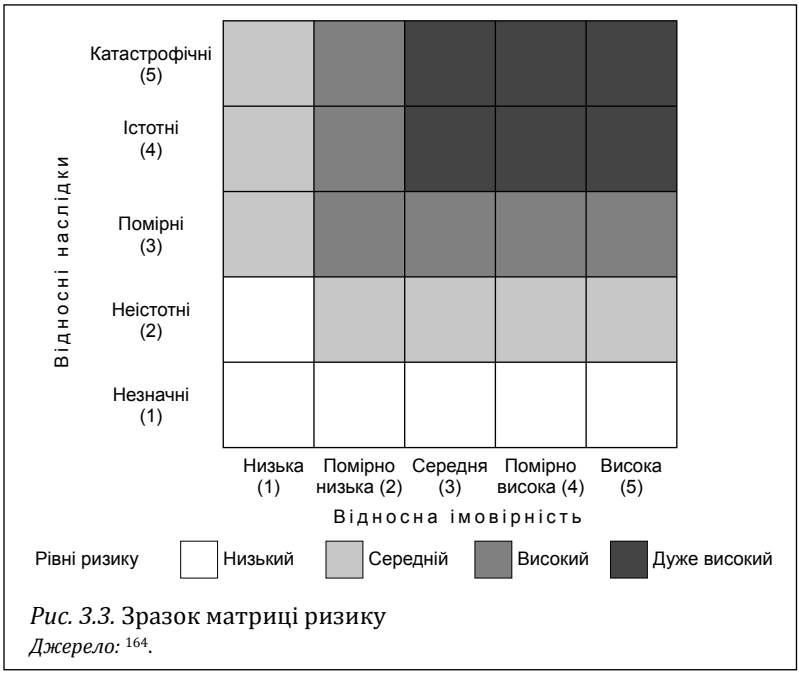


Рис. 3.3. Зразок матриці ризику
Джерело: [164].

[163] Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. URL: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/risk-assessment-methodologies-critical-infrastructure-protection-part-ii-new-approach

[164] Там само.

представлення рівня ризиків застосовується чотиридіапазонна кольорова шкала: низький рівень ризику – зелений колір; середній – жовтий; високий – помаранчевий; дуже високий – червоний.

Інколи окремі країни ЄС використовують ще дуже низький рівень ризику, що позначається блакитним кольором за шкалою кольорів, або ж різні градації відтінків сірого кольору.

У Європейському Союзі кожна країна має проводити оцінку ризиків для різних загроз і, відповідно, будувати різні матриці ризику при проведенні оцінки ризиків для КІ. При цьому особливої уваги потребують взаємозв'язки та взаємозалежності між загрозами природного походження, коли виникнення одних небезпечних явищ призводить до формування нових через механізм каскадних ефектів.

Серед усіх загроз різного походження для безпеки КІ найбільш важливими визначено такі:

- *природні* (незловмисні): повені, екстремальні погодні явища, лісові пожежі, землетруси, епідемії та пандемії, епізоотії;
- *техногенні* (незловмисні): промислові аварії, ядерні/радіологічні аварії, аварії на транспорті;
- *зловмисні*: кібератаки, терористичні атаки, втрата критично важливої інфраструктури.

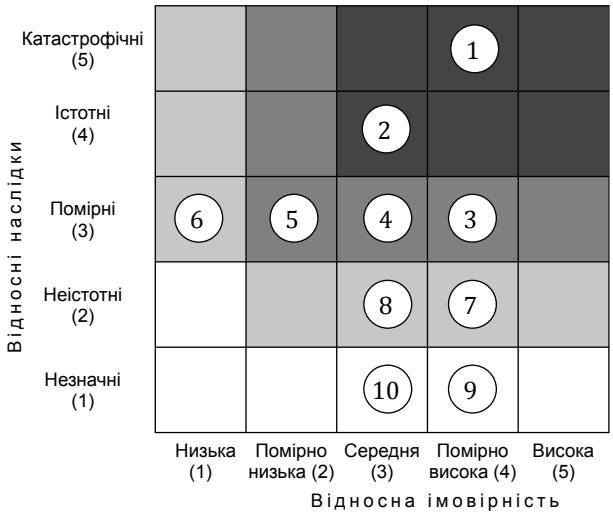
Ризик-аналіз в окремих країнах став важливим елементом у системі забезпечення національної безпеки. Відтак щорічно здійснюється публікація окремого документа «Національна оцінка ризиків» (National Risk Assessment).

Прикладом застосування такого інструменту підвищення національної стійкості є ризик-аналіз, який проводиться у Великій Британії. Уряд країни щорічно готує *Національну оцінку ризиків*, у межах якої забезпечується виконання низки важливих елементів системи забезпечення національної стійкості, а саме:

- *передбачення* (визначення ризиків) – здійснюється широкий пошук інформації для встановлення того, де може виникнути проблема, які існують потенційні загрози;
- *формування реєстру ризиків* – здійснюється визначення найбільш імовірних загроз, реалізація яких може спричинити найбільш тяжкі наслідки для країни у наступні п'ять років (ґрунтується на аналізі інформації, аналітичних та наукових судженнях і розвідданих про ймовірність і наслідки реалізації загроз);

- *оцінка ризиків* – власне формування розуміння комплексу ризиків, на запобігання яким має бути налаштована система національної стійкості що формує загальну національну оцінку ризику.

РИЗИКИ РІЗНОГО ХАРАКТЕРУ



Події:
1. Епідемії грипу.
2. Повені у прибережній смузі, ефузивні виверження вулканів.
3. Аномальні температури, магнітні бурі, снігопади.
4. Епідемії, річкові повені.
5. Великі техногенні катастрофи.
6. Великі транспортні аварії.
7. Виверження вулканів, шторми і шквали.
8. Епізоотії, посухи, громадські заворушення.
9. Халатність на промислових об'єктах.
10. Сильні лісові пожежі.

Рівні ризику: Низький, Середній, Високий, Дуже високий

Примітка: під якісною оцінкою ймовірностей розуміється:
(1) низька – від 1/20000 до 1/2000;
(2) помірно низька – від 1/2000 до 1/200;
(3) середня – від 1/200 до 1/20;
(4) помірно висока – від 1/20 до 1/2;
(5) висока – більше ніж 1/2.

Результатом такої роботи є *Національний реєстр ризиків*, який раз на два роки оприлюднює уряд Великої Британії (*рис. 3.4*) [165].

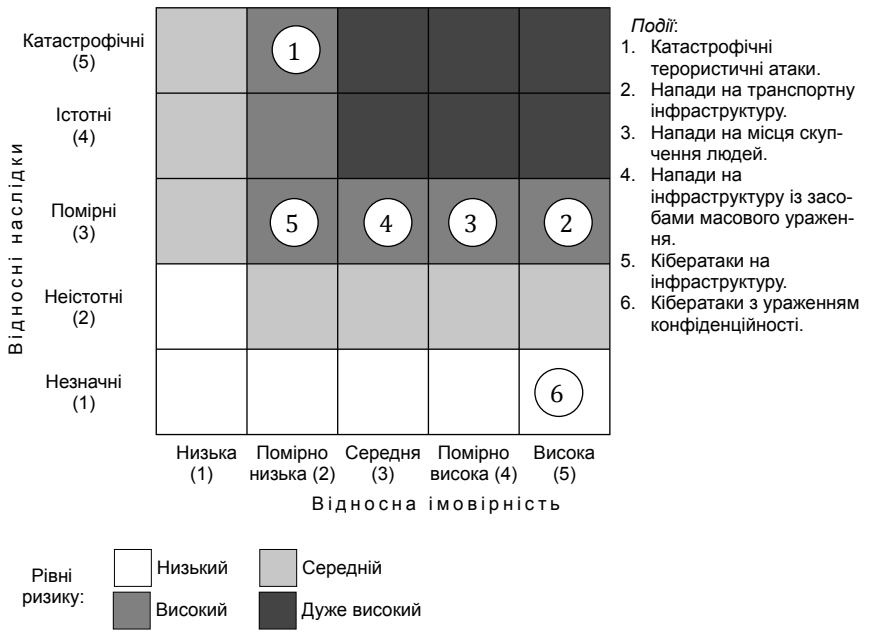


Рис. 3.4. Національна оцінка ризиків Великої Британії

Джерело: за даними Національного реєстру ризиків Великої Британії [166].

[165] National Risk Register of Civil Emergencies, 2015. UK Cabinet Office. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/419549/20150331_2015-NRR-WA_Final.pdf

[166] Там само.

Подібний підхід використовується й у США [167]. Він базується на аналізі загроз (Threat), вразливостей (Vulnerability) та наслідків (Consequence). При цьому ризики КІ оцінюються на основі експертних оцінок за п'ятибальною шкалою (інколи за трибальною) – від низького рівня до катастрофічного. Зокрема, заінтересованість викликає оцінка ризиків для окремого сектору критичної інфраструктури – електроенергетики, зроблена Центром аналізу та обміну інформацією в електроенергетиці (Electricity Information Sharing and Analysis Center, E-ISAC) [168].

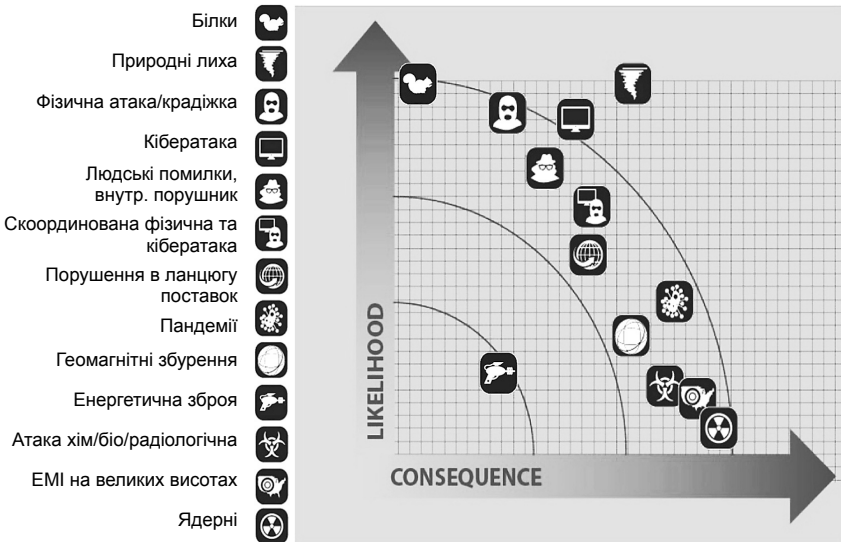


Рис. 3.5. Основні загрози електроенергетиці США (за оцінкою E-ISAC)
Джерело: за даними E-ISAC [169].

[167] Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach. URL: https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf

[168] Electricity Information Sharing and Analysis Center. URL: https://www.eisac.com/

[169] The Electricity ISAC. URL: https://www.frcc.com/Compliance/EducationalMaterials/Educational%20Materials/Workshops%20-%20Workshop%20Event%20Materials/2016-11%20-% 20Fall%20Compliance%20Workshop/November%209%20-%202016%20-%20CIP%20Presentations/TLP%20GREEN%20EISAC_FRCC_FINAL-11-1-16.pdf

Так, за цими даними найбільшу загрозу для електроенергетики в США становлять природні лиха та кібератаки (*рис. 3.5*), що підтверджується й українським досвідом.

Узагальнений досвід управління ризиками знайшов своє відображення в міжнародному стандарті IEC/ISO 31010:2009 Risk management – Risk assessment techniques (Керування ризиком. Методи загального оцінювання ризику) [170] та у відповідному національному стандарті України ДСТУ IEC/ISO 31010:2013 [171]. І хоча цей міжнародний стандарт розроблявся Міжнародною електротехнічною комісією (International Electrotechnical Commission, IEC), тобто первісно призначався для електричних, електронних та інших суміжних технологій, його впровадження Міжнародною організацією зі стандартизації (International Organization for Standardization, ISO) свідчить про доцільність використання цього стандарту будь-якою організацією, яка стикається у своїй діяльності з низкою ризиків різноманітного характеру, які можуть впливати на досягнення цілей, поставлених організацією. Значення цього стандарту ще й у тому, що в ньому достатньо повно описані практично всі методи, які використовуються при аналізі ризиків [172].

Загальне оцінювання ризиків має надати відповіді на такі питання:

- Що може трапитись і чому?
- Які можуть бути наслідки?
- Якою є ймовірність їх виникнення в майбутньому?
- Як пом'якшити наслідки або знизити їх імовірність?
- Чи є рівень ризику допустимим (прийнятним), чи треба та як його обробляти у подальшому?

Відповідно до ДСТУ IEC/ISO 31010:2013 «Керування ризиком», загальний процес оцінювання ризику включає такі етапи:

- ідентифікація ризику – процес виявлення, усвідомлення та реєстрування ризиків, що, у свою чергу, охоплює визначення причин і джерел ризику, аналіз подій, ситуацій та обставин, які можуть мати вплив на функціонування організації та

[170] IEC/ISO 31010:2009 Risk management – Risk assessment techniques. URL: https://www.iso.org/standard/51073.html

[171] ДСТУ IEC/ISO 31010:2013. Керування ризиком. Методи загального оцінювання ризику. URL: http://khoda.gov.ua/image/catalog/files/dstu%2031010.pdf

[172] Додаток В до ДСТУ IEC/ISO 31010:2013.

досягнення поставлених нею цілей, а також характер цього впливу;

- аналізування ризику, яке передбачає аналіз причин і джерел ризику, аналіз вразливостей, аналіз наслідків, кількісне оцінювання та прогнозування ймовірностей виникнення цих наслідків (зауважимо, що для прогнозування та оцінки ймовірності можуть використовуватися різноманітні методи, як-от: експертне оцінювання, метод Дельфі, метод парних порівнянь, дерева відмов, дерева подій, дерева рішень, імітаційне моделювання методом Монте-Карло тощо);
- оцінювання ризику, що має на меті порівняння оцінених рівнів ризику з критеріями ризику, визначеними під час установлення оточення, та слугує для прийняття рішень щодо подальших дій.

Втім кількісно оцінити та адекватно зіставити ризики КІ далеко не завжди можливо. Це пов'язано як із невизначеністю, зокрема неточністю та неповнотою інформації, яка необхідна для коректної оцінки частості загроз (найбільше це позначається на невизначеності терористичних загроз), так і з багатовимірністю та незіставністю можливих наслідків [173].

Окрім того, ключовою особливістю оцінки ризиків для КІ є необхідність урахування численних взаємозв'язків та взаємозалежностей, які можуть бути як очевидними (функціональна залежність), так і розмитими (коли стан однієї системи визначає функціональний стан іншої).

З іншої сторони, коли йдеться про захист КІ, важливо визначити не лише те, «від чого захищатись», а й те, «що захищати»: об'єкт чи функцію. Слід зазначити, що захист цих елементів КІ має відмінності, оскільки щодо *об'єктів* він спрямований передусім на зниження рівня загроз та вразливості об'єктів, мінімізацію наслідків, а щодо *функцій* – на безперервність їх надання та швидке відновлення у разі переривання. У цьому аспекті у нагоді можуть стати сучасні технології управління кризовими ситуаціями, побудовані на системі управління безперервністю бізнесу [174].

---

[173] Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. *Стратегічні пріоритети*. 2015. № 4 (37).

[174] ISO 22301:2012. Societal security – Business continuity management systems – Requirements. URL: https://www.iso.org/standard/50038.html

3.4. Методологія віднесення інфраструктурних об'єктів і систем до критичної інфраструктури

Оцінюючи рівень критичності ОКІ, слід ураховувати, що параметри (критерії) оцінки мають різну природу та характеризують вплив кризової ситуації на ОКІ (її наслідки) з різних боків. Передусім – це масштаб та тяжкість наслідків від якоїсь події у низці безпекових сфер (економіка, безпека життєдіяльності та здоров'я людини, державна безпека, обороноздатність тощо). Відповідно, залежно від наявних даних вони можуть бути представлені в *якісному*, *напівкількісному* або *кількісному вигляді* [175].

Для визначення множини параметрів оцінки рівня критичності об'єкта інфраструктури розглянемо фактори та критерії, які використовуються у ЄС, США, Ізраїлі та РФ.

Так, при визначенні потенційних елементів європейської КІ Директива 2008/114/ЄС [176] визначає необхідність аналізу таких критеріїв (як наскрізних, тобто таких, які враховують взаємозалежність та взаємний вплив об'єктів КІ, так і секторальних):

- масштаб впливу (поширюється щонайменше на дві держави – члени ЄС);
- тривалість збою та/або відновлення;
- наявність альтернатив (для інфраструктури, що надає основну послугу чи виконує життєво важливу функцію);
- істотність впливу (тяжкість можливих наслідків) за наведеними *наскрізними критеріями*: нещасних випадків (оцінюється потенційна кількість смертельних випадків або отриманих травм); економічних результатів (оцінюється значущість економічних втрат та/або погіршення продуктів чи послуг, у т. ч. потенційні екологічні наслідки); суспільних наслідків (оцінюється вплив на суспільну довіру, фізичні страждання, порушення повсякденного життя, у т. ч. ненадання основних послуг).

[175] ДСТУ IEC/ISO 31010:2013. Керування ризиком. Методи загального оцінювання ризику.

[176] Директива Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту // База даних «Законодавство України»/ВР України. URL: http://zakon2.rada.gov.ua/laws/show/984_002-08

При визначенні потенційних елементів КІ у США, як і в ЄС, використовуються подібні параметри:

- масштаб;
- взаємовплив елементів інфраструктури;
- тривалість впливу;
- час на відновлення;
- тяжкість можливих наслідків у таких основних групах: економіка; фінанси; оточуюче середовище; безпека життєдіяльності та здоров'я людей; технологічне середовище.

Окрім того, враховується символічна значущість об'єктів, заподіяна шкода національній обороні та можливі вторинні проблеми для національної безпеки.

Слід відзначити, що США в загальнонаціональну базу для аналізу критичності включено близько 33 тис. об'єктів інфраструктури, з яких близько 2 тис. було віднесено до КІ. Ці об'єкти розділені на *три категорії*: *життєво важливі* (АЕС, великі гідроспоруди та ГЕС, сховища стратегічних запасів нафти та газу, небезпечні хімічні та нафтохімічні виробництва, сховища ядерних матеріалів та боєприпасів); *вкрай важливі* (крупні системи енергозабезпечення, метрополітен, мережі водопостачання та каналізації, магістральні трубопроводи); *важливі* (морські порти, очисні споруди, магістральні автомобільні та залізничні дороги, крупні аеропорти, центри зв'язку тощо). Загалом, при оцінці критичності об'єктів у США зазвичай визначаються її ступені, зокрема високий ступінь критичності об'єктів, середній та низький. Водночас наразі в США від категоризації ОКІ перейшли до їх пріоритизації [177].

Вартим уваги є підхід до ранжування об'єктів військово-промислового комплексу у США – модель визначення пріоритетності об'єктів ВПК (The Asset Prioritization Model) [178]. Усі об'єкти оцінюються за 16 факторами, яким присвоєні вагові коефіцієнти від 16 до 1, з діапазоном оцінок «важливості» об'єкта від 1 до 3 (інколи 5), та розраховується сумарний індекс «ризикованості» об'єкта. Ці фактори враховують: вплив на великосерійні програми виробництва;

[177] Presidential Policy Directive – Critical Infrastructure Security and Resilience. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[178] Баранник А., Клементьев С. Организация обеспечения безопасности критической инфраструктуры в США. *Зарубежное военное обозрение*. 2009. № 8. С. 3–10.

на бойові можливості (значущість продукції); фінансові можливості компанії, економічну живучість; можливості відновлення; кількість населення, що проживає поряд; супутні втрати від враження хімічними/біологічними/радіаційними та вибуховими речовинами, які використовувалися при атаці, та ін. Цікавим є й те, що в 2007 р. найбільш критичними визнані об'єкти, на яких виконуються великосерійні програми виробництва для ВПК, тоді як раніше такими об'єктами вважалися ті, які мають найбільший вплив на сучасні бойові можливості.

Подібний набір параметрів використовується й у РФ [179]. При цьому показники розподілені на два рівні, коли кожний показник 1-го рівня розкривається через показники 2-го рівня: значущість об'єкта для економіки держави, нанесення шкоди престижу держави, можливі загрози населенню та територіям.

В Ізраїлі при ідентифікації ОКІ враховуються такі критерії [180]:

- символічна (ідеологічна, історична або культурна) значущість об'єктів;
- залежність основних процесів життєзабезпечення суспільства від інфраструктури (енергетика, водопостачання, каналізація, телекомунікації);
- наявність складних взаємозв'язків та залежностей між об'єктами інфраструктури.

Цікавим є те, що об'єкти культурної спадщини Ізраїлю (музеї, архіви, культові споруди та інші пам'ятки) віднесені до числа об'єктів, які повинні бути захищені в першу чергу.

Ураховуючи наведене, можна побудувати таку ієрархічну модель критеріїв визначення рівня критичності інфраструктури (*табл. 3.3*).

Слід зазначити, що запропонований підхід не є абсолютним, оскільки визначені ним критерії не є повністю незалежними одне від одного. Наприклад, критерій «збиток здоров'ю і життю людей» пов'язаний з іншими параметрами оцінки критичності, зокрема

[179] Методика отнесения объектов государственной и негосударственной собственности к критически важным для национальной безопасности Российской Федерации. Нормативный документ МЧС России. URL: http://central.mchs.ru/upload/site4/files/bea08465669b520c2603f73058fe188a.pdf

[180] Гриняев С. О взгляде на проблему безопасности критической инфраструктуры в государстве Израиль. *Центр стратегических оценок и прогнозов*. URL: http://csef.ru/ru/oborona-i-bezopasnost/265/o-vzglyade-na-problemu-bezopasnosti-kriticheskoj-infrastruktury-v-gosudarstve-izrail-3229

Таблиця 3.3. **Ієрархічна модель критеріїв визначення рівня критичності інфраструктури**

1-й рівень	2-й рівень	3-й рівень
Взаємозв'язок між елементами КІ та наявність альтернатив	Каскадні ефекти	Зниження обсягу функцій залежних систем. Настання тяжких негативних екологічних, економічних, соціально-політичних наслідків. Унеможливлення ліквідації наслідків кризової ситуації (ускладнення роботи аварійно-рятувальних служб, надання екстреної допомоги населенню тощо)
	Взаємозамінність (диверсифікованість), наявність альтернативи	Можливість постачання послуг/ресурсів з інших джерел (іншими шляхами)
	Резервування	Наявність резервних виробництв/ресурсів
Масштаб впливу	Територіальне поширення	Локальне, район, регіон, уся територія держави, глобальне
	Масштаб інциденту в організаційному аспекті	На рівні процесу, підприємства, галузі економіки, загальний для держави або групи держав
Часовий ефект впливу	Час, через який з'являються негативні наслідки	Негайно, через кілька годин, тижнів, місяців
	Тривалість впливу	До кількох годин, діб, тижнів, місяців, років
	Час на відновлення	Кілька годин, діб, тижнів, місяців, років
Тяжкість можливих наслідків	Збиток здоров'ю і життю людей	Кількість постраждалих, травмованих, загиблих, евакуйованих
	Ступінь порушення нормальних умов життєдіяльності людей	Енергопостачання. Водопостачання. Каналізація та вивезення сміття. Постачання товарів першої необхідності (продуктів харчування, засобів гігієни тощо). Послуги з охорони здоров'я. Транспортне сполучення

Продовження табл. 3.3

1-й рівень	2-й рівень	3-й рівень
Тяжкість можливих наслідків	Економічна шкода	Вплив на ВВП. Розмір економічних втрат, як прямих, так і непрямих. Чисельність персоналу та населення, які пов'язані з діяльністю об'єкта. Частка продукції об'єкта в загальнодержавному її випуску/споживанні
	Ступінь порушення безперервності надання функцій із забезпечення виробничої діяльності стратегічних підприємств	Зупинка безперервних виробництв. Частка продукції об'єкта в загальнодержавному її випуску/споживанні
	Ступінь впливу на фінансову та банківську систему	Частка об'єкта в загальнодержавному обсязі банківських чи фінансових послуг
	Екологічна шкода	Вплив на населення (забрудненість повітря, води, продуктів харчування тощо). Вплив на навколишнє природне середовище
	Соціально-політична шкода	Нанесення шкоди авторитету держави. Рівень панічних, протестних та антидержавних настроїв. Суспільна тривога, втрата впевненості в дієздатності влади, розбрат. Символічна значущість об'єктів (історичні та культурні цінності)
	Ступінь впливу на безпеку держави та обороноздатність	Порушення керованості держави або регіону. Масові порушення правопорядку. Зниження боєготовності та боєздатності збройних сил. Вплив на бойові можливості (значущість продукції/послуг). Розкриття державних секретів, конфіденційної науково-технічної та комерційної інформації

Джерело: складено автором.

з такими, як: екологічна шкода, порушення нормальних умов життєдіяльності, обороноздатність, масові порушення правопорядку тощо.

Окрім того, запропонований підхід дозволяє оцінити взаємозалежності об'єктів інфраструктури лише спрощено, тобто у першому наближенні.

Для коректної оцінки рівня критичності об'єкта потрібно (як того і вимагає Директива 2008/114/ЄС) коректно врахувати численні взаємозв'язки та взаємний вплив ОКІ – наскрізно оцінити наслідки міжсекторальних залежностей. Проте це врахування взаємного впливу об'єктів КІ доцільно проводити більш глибоко лише для вже визначених ОКІ, які віднесені до І та ІІ категорій критичності – критично-важливих та життєво важливих об'єктів інфраструктури. Результати оцінки взаємозалежностей мають бути представлені в *паспорті безпеки об'єкта КІ*.

Проте використання критеріїв, наведених у *табл. 3.3*, для первісної оцінки та ранжування об'єктів інфраструктури за рівнем критичності є прийнятним, оскільки дозволяє достатньо просто оцінити рівень критичності будь-якого об'єкта інфраструктури, використовуючи, відповідно до ДСТУ IEC/ISO 31010:2013, *напівкількісні методи*, коли наслідки, ймовірність та рівень ризику оцінюються за допомогою числових шкал з обмеженою кількістю можливих значень параметрів оцінки та нескладних формул.

Узявши за основу підхід ЄС «Методи оцінки ризику для захисту критичної інфраструктури. Частина ІІ. Новий підхід» [181], для оцінки наслідків та їх ймовірності використовується п'ятидіапазонна шкала, в якій наслідки оцінюються від незначних до катастрофічних, а їх імовірність/частість – від дуже малоймовірних/дуже рідкісних до дуже ймовірних/частих. Ризик також оцінюється за п'ятидіапазонною кольоровою шкалою: дуже низький (блакитний), низький (зелений), середній (жовтий), високий (помаранчевий) та дуже високий (червоний).

[181] Risk assessment methodologies for critical infrastructure protection. Part II: A new approach. URL: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/risk-assessment-methodologies-critical-infrastructure-protection-part-ii-new-approach

Розглянемо ***Методику віднесення об'єктів інфраструктури до критичної*** [182]. У її основу покладений апарат *нечіткої логіки* та *метод експертних оцінок* [183], який базується на представницькій процедурі опитування фахівців (експертів) та подальшій обробці результатів для визначення нормованого інтегрального показника критичності об'єкта інфраструктури. Методика може бути використана для будь-якого сектору інфраструктури.

Визначення параметрів оцінки критичності. Множина параметрів оцінки критичності об'єктів/функцій інфраструктури сформована на основі параметрів ієрархічної моделі критеріїв (*табл. 3.3*), для зручності та простоти використання згорнутої до 20 параметрів (*табл. 3.4*).

Визначення ваги параметрів. Для кожного з параметрів за методом експертної оцінки Дельфі визначена його вага (значимість) від 0 до 100 % (від 0 до 1,0); при цьому сума ваги всіх параметрів дорівнює 100 % (1,0).

Параметри оцінки критичності та вагові коефіцієнти значимості кожного з них, визначені експертами, наведені в *табл. 3.4*. При визначенні групової оцінки використовувалося середнє арифметичне оцінок усіх експертів, округлене до 1 % [184].

Визначення значень параметрів. Методом експертної оцінки Дельфі визначається нечітке значення кожного параметра об'єкта, який оцінюється.

Для оцінки рівня критичності ОКІ (ризиків від припинення надання ними життєво важливих послуг та функцій, а також ризиків, пов'язаних з аваріями на них, зумовлених будь-якими причинами) використовується лінгвістична зміна з 5 термів:

- несуттєвий (голубий чи кількісно 1);
- незначний (зелений чи кількісно 2);

---

[182] Слід зазначити, що на сьогоднішній день методика віднесення об'єктів інфраструктури до критичної в Україні відсутня. Далі йдеться про методику, запропоновану фахівцями НІСД.

[183] Бобро Д. Г. Методологія оцінки рівня критичності об'єктів інфраструктури. *Стратегічні пріоритети*. 2016. № 3 (40). С. 77–86. URL: http://www.niss.gov.ua/public/File/Str_prioritetu/SP_3_40_16.pdf

[184] Експертне опитування було проведено серед фахівців НІСД. У результаті були визначені коефіцієнти значимості для параметрів 1-ї групи та обраної групи з 20 параметрів 2-го та 3-го рівнів. Обрана група дозволяє достатньо просто оцінити рівень критичності об'єктів будь-якого сектору КІ. Втім для конкретного сектору КІ цей перелік може бути уточнено.

- значимий (жовтий чи кількісно 3);
- значний (помаранчевий чи кількісно 4);
- критичний (червоний чи кількісно 5).

При визначенні групової оцінки використовується середнє арифметичне оцінок усіх експертів, округлене до найближчого цілого.

Визначення рівня критичності ОКІ. Нормований рівень критичності ОКІ (приведений у діапазон від 0 до 1,0, де 1,0 відповідає найкритичнішому об'єкту) визначається як сума добутку ваги параметра на його нечітке значення для цього об'єкта, розділене на 5 (кількість термів).

Таблиця 3.4. **Параметри оцінки рівня критичності та їх вагові коефіцієнти значимості**

№ п/п	Параметри 1-го рівня	Вага, %	Параметри оцінки критичності	Вага, %
1	Взаємозв'язок ОКІ та наявність альтернатив	32	Каскадні ефекти	22
2			Диверсифікованість (альтернативи)	7
3			Резерви	3
4	Масштаб впливу	10	Територіальний масштаб впливу	7
5			Масштаб впливу в організаційному аспекті	3
6	Часові ефекти впливу	5	Тривалість впливу	3
7			Час на відновлення	2
8	Тяжкість можливих наслідків	53	Збиток здоров'ю та життю людей	8
9			Енергопостачання	4
10			Водопостачання	2
11			Каналізація та вивезення сміття	2
12			Постачання товарів першої необхідності	2
13			Послуги з охорони здоров'я	2
14			Транспортне сполучення	2
15			Економічна шкода	7
16			Порушення роботи стратегічних підприємств	5
17			Фінанси та банківська сфера	5
18			Екологічна шкода	2
19			Соціально-політична шкода	6
20			Обороноздатність	6
Загалом		100	Загалом	100

Джерело: складено автором.

Для візуалізації [185] рівня критичності об'єкта, що оцінюється, будується пелюсткова діаграма, де ширина пелюстки відповідає вазі (значимості) параметра, а його значення дорівнює нечіткому значенню для цього об'єкта – середнє арифметичне оцінок експертів, визначених із використанням вищезгаданої лінгвістичної зміни з 5 термів та округлене до ближчого цілого. Приклад візуалізації результатів оцінки рівня критичності АЕС наведений на *рис. 3.6*. Для оцінки використано 20 параметрів *табл. 3.4*, які відображені за ходом часової стрілки у порядку від 1-го до 20-го.

Рис. 3.6. Приклад оцінки рівня критичності АЕС

Джерело: складено автором.

[185] Не є обов'язковим. Слугує для наочності зробленої оцінки рівня критичності об'єкта КІ. При цьому обчислений рівень критичності відповідає площі пелюсткової діаграми.

Категоризація (пріоритизація) об'єктів інфраструктури. Ранжування усіх інфраструктурних об'єктів з розбивкою на чотири категорії критичності проводиться за обчисленими значеннями нормованого інтегрального показника критичності. Попередні результати подібного ранжування для двох рівнів загроз, властивих звичайному та воєнному стану, як приклад наведені на *рис. 3.7*.

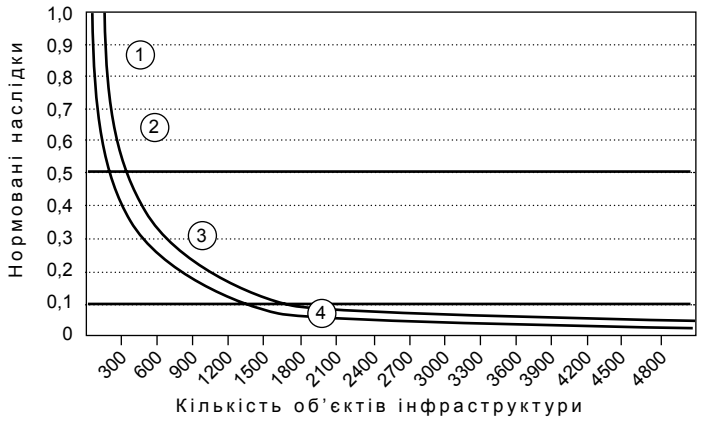


Рис. 3.7. Приклад ранжування об'єктів інфраструктури за рівнем критичності для двох рівнів загроз – звичайного та воєнного стану
Джерело: складено автором.

Розбивка об'єктів інфраструктури на групи проведена так:

І категорія критичності – критично-важливі об'єкти (нормований коефіцієнт критичності понад 0,8). Це об'єкти, які мають загальнодержавне значення, розгалужені зв'язки та значний вплив на іншу інфраструктуру, заходи з відновлення яких вимагають значних ресурсів та часу. На таких об'єктах має бути створена адекватна загрозам система фізичного захисту (наприклад, на АЕС, нафтопереробних заводах, великих гідроспорудах тощо). Відповідальність за захист цієї КІ має консолідовано нести держава та оператори (власники) з чітким регламентуванням відносин та взаємодії. Зазначені об'єкти включаються до переліку ОКІ, формуються вимоги щодо забезпечення їхнього захисту;

II категорія критичності – життєво важливі об'єкти (нормований коефіцієнт критичності від 0,5 до 0,8), порушення функціонування яких призведе до кризової ситуації регіонального значення. На таких об'єктах потрібно реалізувати як заходи з фізичного захисту, так і передбачити можливість скорішого відновлення функцій за рахунок диверсифікації та резервів (наприклад, крупні нафтобази, підземні сховища газу, електричні підстанції, мостові переходи, крупні елеватори, джерела питної води тощо). Відповідальність за захист цієї КІ мають нести оператори (власники) та держава на основі державно-приватного партнерства при жорсткому контролі з боку держави за дотриманням вимог та правил з безпеки. Зазначені об'єкти включаються до переліку ОКІ, формуються вимоги щодо розмежування завдань і повноважень органів державної влади та операторів критичної інфраструктури, спрямованих на забезпечення їхнього захисту та відновлення функціонування;

III категорія критичності – важливі об'єкти (нормований коефіцієнт критичності від 0,1 до 0,5). Пріоритетом захисту такої інфраструктури є забезпечення швидкого відновлення функцій за рахунок диверсифікації та резервів. Відповідальність за стійкість функціонування об'єктів несуть оператори при встановлених законодавством вимогах щодо взаємодії із органами державної влади, яка має забезпечити наявність умов для диверсифікації та резервування;

IV категорія критичності – необхідні об'єкти (нормований коефіцієнт критичності до 0,1). Об'єкти інфраструктури, безпосередній захист яких є відповідальністю оператора, який повинен мати план реагування на кризову ситуацію.

Слід зазначити, що прийняті у цьому прикладі граничні показники критичності (0,1, 0,5 та 0,8) визначені експертами попередньо та мають бути уточнені за результатами оцінки основної частини інфраструктурних об'єктів, у т. ч. ураховуючи спроможності держави.

3.5. Проектна загроза у системі забезпечення безпеки та стійкості критичної інфраструктури

Методологічно державна система БСКІ будується на аналізі ризиків, які несе в собі дестабілізація роботи ОКІ, спричинена будь-якими чинниками природного чи техногенного характеру, а також протиправними діями. Саме проаналізувавши наявні загрози та небезпеки,

зробивши їх відсів за результатами аналізу ризиків, можна сформувати перелік загроз (небезпек), на захист від яких має бути розрахована система захисту критичної інфраструктури. Цей перелік і буде *проектною загрозою* – основою, яка визначатиме, від *кого* та від *чого* потрібно захищатися[186].

3.5.1. Модель порушника та модель загрози протиправних дій

У межах державної системи фізичного захисту передбачені заходи, що включають увесь ланцюжок дій: від оцінки загроз протиправних дій (у т. ч. визначення проектної загрози) та категоризації об'єктів системи до встановлення конкретних вимог щодо систем фізичного захисту, оцінки вразливості об'єктів, ймовірності завдання шкоди, проведення перевірок систем фізичного захисту (ФЗ) та планів взаємодії. Подібні підходи можуть бути використані також при розбудові в Україні державної системи БСКІ.

Слід зазначити, що визначення проектної загрози [187] ядерним установкам та ядерним матеріалам в Україні ґрунтується на рекомендаціях МАГАТЕ з фізичної ядерної безпеки [188] та аналізі сучасного безпекового середовища, яке враховує суттєві зміни безпекової ситуації внаслідок агресії РФ [189]. При цьому основою проектної загрози в системі ФЗ є *модель порушника*, на основі якої будується

[186] Детальна структура Проектної загрози ОКІ наведена в *Додатку 1.6*.

[187] Відповідно до рекомендацій МАГАТЕ проектна загроза (design basis threat) – це «ознаки та характеристики потенційних внутрішніх та/або зовнішніх порушників, що можуть вчинити спробу несанкціонованого вилучення або саботажу (диверсії), для протидії яким створюється та оцінюється система фізичного захисту». Аналогічне визначення міститься й в Правилах фізичного захисту ядерних установок та ядерних матеріалів, розроблених Держатомрегулювання України: «Проектна загроза – визначені в установленому порядку характеристики потенційних правопорушників, які могли б здійснити спробу несанкціонованого вилучення ядерних матеріалів або вчинення акту ядерного тероризму, для протидії яким визначається, створюється та оцінюється система фізичного захисту». Деякі відмінності згаданих визначень зумовлені дещо різним міжнародним трактуванням таких термінів, як-от «саботаж (диверсія)», «акт тероризму», та їх визначеннями в українському законодавстві.

[188] Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок (INFCIRC/225/Revision 5). URL: http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481r_web.pdf

[189] Нині в Україні діє редакція Проектної загрози ядерним установкам, ядерним матеріалам, радіоактивним відходам, іншим джерелам іонізуючого випромінювання, схвалена рішенням РНБО України від 16 жовтня 2012 р. (зі змінами, внесеними Указом Президента України від 27 серпня 2015 р. № 521/2015). Цей документ є таємним.

модель загрози. Обидві моделі є вихідною інформацією для розроблення політики безпеки і проектування будь-яких систем захисту.

Подібні підходи в оцінці загроз використовуються і в США. Зокрема, у документі «Політика Міністерства енергетики щодо проектної загрози» (DOE O 470.3C, Design Basis Threat Policy) [190] визначено загрози, які стосуються аспектів захисту ядерної зброї (зміст зазначеного документа утаємничений), а в документі Комісії з ядерного регулювання США (US NRC 10 CFR) [191] у загальному вигляді (без конкретизації кількісних показників) визначено характеристики порушників щодо цивільних ядерних об'єктів та ядерних матеріалів, а також при транспортуванні ядерних матеріалів. Так, у разі диверсії (в оригіналі – *sabotage*) використовується така модель порушника:

(i) одиночна група, що атакує через одну точку входу; декілька груп, що атакують через декілька точок входу; комбінація груп та окремих нападників, що атакують через декілька точок входу з такими атрибутами, підтримкою та оснащенням:

A. добре підготовлені (включаючи військову підготовку та навички) особи, віддані справі та готові убивати чи бути вбитими, з достатніми знаннями для визначення конкретного обладнання чи місць для успішного нападу;
B. внутрішня допомога – активна (допомога для входу/виходу, відключення сигналів тривоги та засобів зв'язку, участь у нападі) чи пасивна (надання інформації) або те й інше;
C. відповідна зброя, у т. ч. ручна автоматична зброя, оснащена глушниками, яка має ефективну дальність і точність;
D. ручне оснащення, у т. ч. для нейтралізації (несмертельна зброя), вибухівка для входу або підриву реакторного обладнання;
E. наземні та водні транспортні засоби;

а також:

(ii) внутрішня загроза;

(iii) напад із застосуванням замінованого наземного транспортного засобу;

[190] DOE O 470.3C, Design Basis Threat Policy (U) / U.A. Department of Energy. URL: https://www.directives.doe.gov/directives-documents/400-series/0470.3-BOrder-c

[191] Purpose and Score. NRC Regulations. Part Index / U.A. NRC. URL: https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0001.html

(iv) напад із застосуванням замінованого водного транспортного засобу, які можуть бути скоординовані із зовнішнім нападом;

(v) кібератака.

Щодо інших країн, то, наприклад, в Австралії у проектній загрозі ядерним об'єктам, окрім згаданих вище характеристик порушників, в якості оснащення розглядаються ще й дрони, а модель загроз включає ще й напад на ядерний об'єкт за допомогою літака, який може бути скерований на об'єкт як імпровізований вибуховий пристрій [192].

У Росії формування базових проектних загроз об'єктам енергетики здійснюється відповідно до низки нормативно-правових актів, а сама базова проектна загроза [193] містить відомості про:

- цілі здійснення актів незаконного втручання – критичні елементи, що підлягають захисту, можливі засоби та способи їх пошкодження (руйнування);
- сценарії здійснення актів незаконного втручання, у т. ч. вживані тактики досягнення поставлених цілей, маршрути та часові характеристики дій порушника відносно кожного з критичних елементів об'єкта;
- розрахункові моделі порушника, у т. ч. чисельність, склад, розподіл нападників за елементами бойового ладу, озброєння, оснащення, екіпіровки, ступені обізнаності із виробничо-технологічним циклом і систем фізичного захисту об'єкта, спроможності санкціонованого доступу;
- виробничі особливості об'єкта, його географічне, соціальне та криміногенне оточення.

Зазначені дані включаються до Паспорта безпеки об'єкта енергетики, який відображає не лише характеристики цього об'єкта з точки зору його потенційної небезпеки (категорії небезпеки, отриманої з урахуванням властивостей небезпечних речовин, що використовуються на об'єкті, та за впливом вражаючих факторів, що можуть мати місце у разі аварії на об'єкті), а й можливі наслідки в результаті незаконного втручання у функціонування об'єкта, оцінку стану

[192] Australian National Design Basis Threat Approved Declassification / Australian Safeguards and Non-Proliferation Office. URL : http://dfat.gov.au/international-relations/security/asno/Documents/design-basis-threat.pdf

[193] Обоснование базовой проектной угрозы объекту. URL : http://iteration.su/danger.html#section_2

систем інженерно-технічного та фізичного захисту, заходи із забезпечення антитерористичної захищеності [194].

Таким чином, в аспекті фізичного захисту об'єктів модель загроз будується на моделі порушника та розробляється для того, щоб встановити:

- від кого захищатися;
- яка мета потенційного порушника (причини та мотиви, цілі на об'єкті);
- хто може бути потенційним порушником (одна людина чи група осіб), він є зовнішнім або внутрішнім порушником, чи, можливо, вони діють у зговорі;
- якими знаннями та навичками володіє порушник (як щодо об'єкта, включно із системою його фізичного захисту, так і щодо використання зброї, засобів зв'язку та розвідки, наприклад, дронів, транспорту тощо);
- якими методами та засобами користується порушник (озброєння, технічна оснащеність, засоби зв'язку, розвідки, пересування тощо);
- яку тактику дій може використати порушник (сценарії дій).

При цьому загрози критичній інфраструктурі слід розглядати також і з точки зору виокремлення елементів об'єкта захисту, на які ці загрози спрямовані:

- *фізичні елементи*, зокрема технологічне обладнання та ресурси об'єктів;
- *системи управління*, зокрема системи автоматичного управління та регулювання технологічними процесами, системи зв'язку, охорони (у т. ч. контролю доступу, інженерно-технічні засоби охорони тощо);
- *персонал* об'єктів, зокрема диспетчерський, оперативний, який безпосередньо забезпечує функціонування критичної інфраструктури, персонал охорони тощо.

Проте подібні моделі загроз та сформована на їхній основі проектна загроза, заснована лише на моделі порушника, не дає можливості побудувати систему захисту критичної інфраструктури від загроз усіх типів – будь-якого походження та спрямованості.

[194] Проблеми оцінки терористичної вразливості та формування паспортів безпеки об'єктів енергетики: аналіт. записка. URL : http://www.niss.gov.ua/content/articles/files/pasport_bezpeki-3d468.pdf

3.5.2. Модель загроз та проектна загроза критичній інфраструктурі

Слід зазначити, що моделі загроз та порушника широко використовуються у світі також і в рамках захисту інформаційних ресурсів і кіберзахисту ОКІ. Причому саме в цій сфері був здійснений перехід від розгляду лише загроз зловмисних (чи, точніше, протиправних) дій до ширшого кола загроз.

Так, у РФ при аналізі джерел загроз безпеці інформації аналізуються як антропогенні джерела (особи, які здійснюють протиправну діяльність), так і природні та техногенні джерела [195]. Модель порушника включає їхні типи (зовнішній/внутрішній) та види (спецслужби держав, терористичні чи екстремістські угруповання, кримінальні структури, конкуренти, розробники, адміністратори, обслуговуючий персонал, користувачі тощо), можливі цілі та мотивацію порушників, їхній потенціал.

Якщо звернутися до досвіду західних країн, то, наприклад, під час аналізу загроз електроенергетичному сектору США [196] бачимо, що відповідна модель включає:

- загрози природного характеру (торнадо, повені, землетруси тощо);
- людські помилки та інші техногенні аварії;
- протиправні дії (кримінальні та терористичні угруповання, активісти екстремістських груп різного спрямування, хакери тощо).

Загалом же при розгляді моделей загроз КІ США на національному рівні в рамках підходу *all hazards approach* розглядається низка загроз природного та техногенного характеру, а також зловмисних дій, пов'язаних у т. ч. з використанням як зброї літаків, актів ядерного, радіологічного, хімічного та біологічного тероризму [197].

---

[195] ФСТЭК России. Методика определения угроз безопасности информации в информационных системах. URL: http://fstec.ru/component/attachments/download/812

[196] Integrating Electricity Subsector Failure Scenarios into a Risk Assessment Methodology. EPRI. 3002001181. Decr 2013. (2014). URL: https://energy.gov/sites/prod/files/2014/05/f15/IntegratingElectricitySubsectorFailureScenariosIntoARiskAssessmentMethodology_1.pdf ; Electric Grid Security and Resilience. Establishing a Baseline for Adversarial Threats. June 2016. (2017). URL: https://energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf

[197] 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

Таким чином, в аспекті захисту КІ модель загроз для неї є більш широким (відносно моделі в системі ФЗ в ядерній галузі) поняттям та базується на пошуку відповіді на питання: «Які фактори можуть завдати шкоди функціонуванню ОКІ?» А це означає необхідність аналізу не тільки потенційних порушників, а й самого ОКІ:

- де він розташований (у т. ч. географічні, кліматичні умови, сейсмічні показники);
- які потенційно-небезпечні технології на цьому об'єкті використовуються; де та як розміщене обладнання, як до нього можна дістатися, що може вплинути на його роботу;
- які інші об'єкти розташовані поряд із об'єктом, що аналізується, та можуть потрапити під дію вражаючих факторів;
- яке місце цей об'єкт посідає у виробничих ланцюжках; хто є споживачем його продукції (тобто взаємозалежність з іншими господарськими об'єктами) тощо.

Водночас модель загроз буде неповною без *моделювання соціально-політичної обстановки*, в якій об'єкт КІ функціонує, оскільки від цього залежить можливість реалізації низки загроз воєнного та соціально-політичного характеру.

Отже, адекватна модель загроз об'єкта КІ має включати модель порушника, модель об'єкта та модель обстановки [198]. Зважаючи на зазначене, модель загроз можна представити графічно (*рис. 3.8*).

У цій моделі відповідно до підходу *all hazards approach* враховано загрози (небезпеки) будь-якого походження:

- природного й техногенного характеру (ураховуються при опрацюванні моделі об'єкта);
- соціально-політичного та воєнного характеру (ураховуються при опрацюванні моделі обстановки);
- протиправні дії – кіберзагрози та загрози диверсійно-терористичного характеру (ураховуються в моделях порушника).

[198] Бояринцев А., Редькин В. Центр анализа уязвимости ЗАО «НПП «ИСТА-Системс». Определение и ранжирование угроз объектам. URL: http://mx1.algoritm.org/arch/71/71_5.pdf ; Мошкова Р. А. Критерии системы управления экономической безопасностью предприятия железнодорожного транспорта. URL: http://publishing-vak.ru/file/archive-economy-2016-6/6-moshkova.pdf ; Петрищев И. О., Смагин А. А. Построение моделей угроз и расчетных показателей эффективности комплексной системы безопасности при анализе уязвимости складов нефтепродуктов. URL: http://www.apu.npomars.com/images/pdf/21_4.pdf

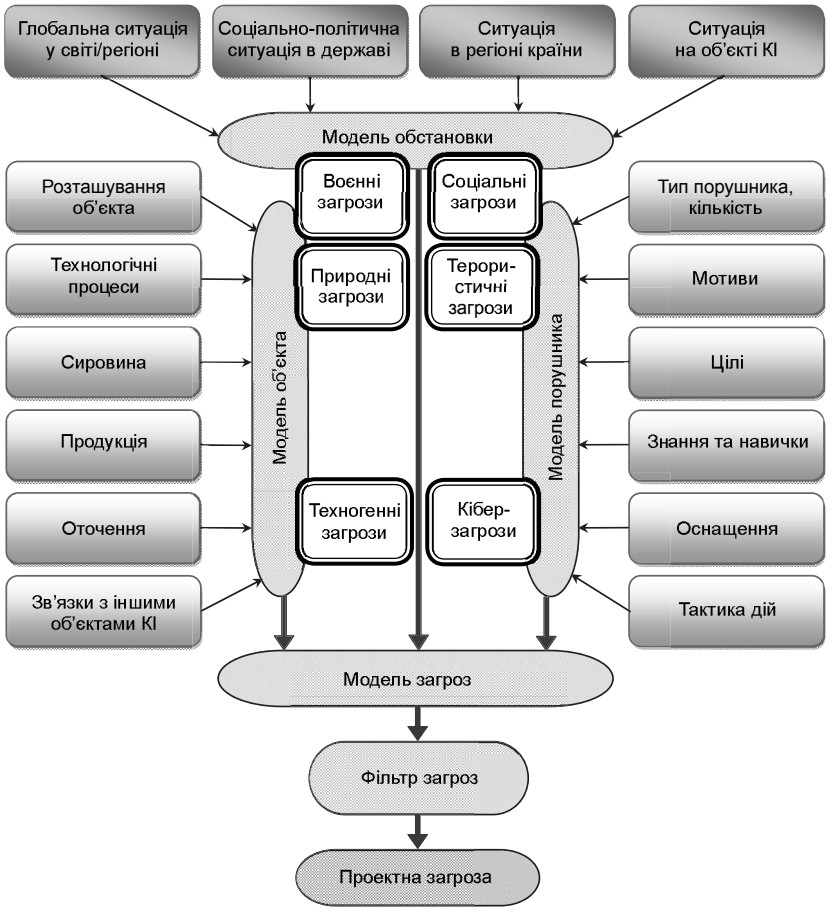


Рис. 3.8. Модель загроз та проектна загроза об'єктам критичної інфраструктури

Джерело: складено автором з урахуванням [199].

[199] Бояринцев А., Редькин В. Центр анализа уязвимости ЗАО «НПП «ИСТА-Системс». Определение и ранжирование угроз объектам ; Мошкова Р. А. Критерии системы управления экономической безопасностью предприятия железнодорожного транспорта ; Петрищев И. О., Смагин А. А. Построение моделей угроз и расчетных показателей эффективности комплексной системы безопасности при анализе уязвимости складов нефтепродуктов.

При цьому варто зазначити, що перелічені вище моделі (обстановки, об'єкта, порушника) є взаємопов'язаними та взаємозалежними. Так, наприклад, модель об'єкта є основою для визначення потенційних цілей порушника (у т. ч. щодо кібератак), а соціально-політична ситуація в державі, регіоні та на об'єкті впливає на мотиви (протестні настрої тощо) та дії (наприклад, перекриття доріг тощо) порушників.

Завдяки моделюванню формується *модель загроз*, яка містить перелік можливих загроз (небезпек) для об'єкта КІ, що впливають на його безпечне функціонування [200]. Проте, як уже згадувалося, забезпечити однаково високий рівень захисту всієї критичної інфраструктури від усіх можливих загроз неможливо. Потрібно провести фільтрацію та ранжування загроз. Дослідники з Центру аналізу вразливості пропонують для цього використовувати їх імовірність (відсів малоймовірних), величину (відсів тих, вплив яких на функціонування об'єкта КІ не виходить за припустимі межі) та потенційні втрати (відсів тих загроз, втрати від реалізації яких є прийнятними). Вважаємо, що ці підходи є слушними, проте більш коректно здійснювати відсів загроз за ризиками, оскільки саме ризик, оцінений для різних сценаріїв розвитку подій, є мірою критичності об'єкта КІ. При цьому навіть малоймовірні події (з частістю 10^{-5} на рік і нижче) мають ураховуватися в моделі загроз, якщо їх наслідки (а з урахуванням вразливості об'єкта вони й становитимуть ризик) є суттєвими.

Варто наголосити на тому, що означений підхід до відсіву загроз є відсівом «знизу», а потрібно провести ще й відсів «зверху» – тобто розподілити загрози на ті, що включаються до проектної загрози, та на позапроектні загрози, нейтралізація яких є відповідальністю держави (наприклад, загрози бойових дій чи нападу із застосуванням важкої зброї). Такий підхід (щодо розподілення відповідальності між оператором КІ та державою) є одним із основоположних

[200] Слід зауважити, що, окрім відомих (прогнозованих) загроз (небезпек), існує ще й безліч інших загроз, а для відомих загроз є безліч можливих сценаріїв їх реалізації. Тому побудувати абсолютну систему захисту КІ неможливо. Проте і за цих умов невизначеності та реалізації неврахованих загроз є можливість забезпечити стійкість критичної інфраструктури шляхом швидкого відновлення її функцій, у т. ч. за рахунок диверсифікації та резервів.

принципів МАГАТЕ щодо встановлення та підтримки режиму фізичного захисту [201]. Це розмежування щодо захисту КІ можна представити у вигляді схеми (*рис. 3.9*).

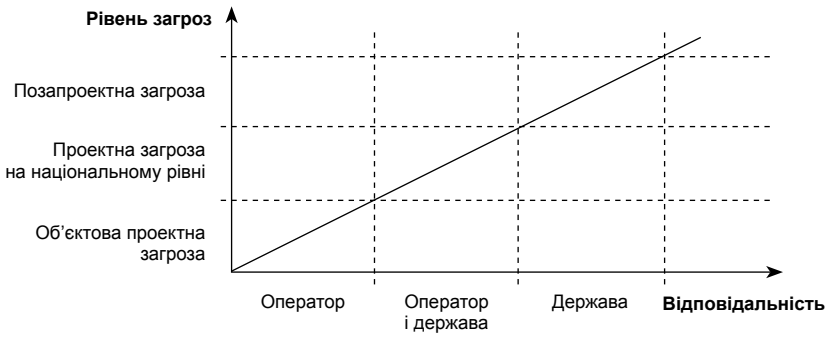


Рис. 3.9. Схема розподілення відповідальності між оператором КІ та державою

Джерело: складено автором.

Можна навести такий приклад класифікації розмежування відповідальності, яка залежить від характеристик моделювання порушника та загроз:

- *відповідальність оператора* – внутрішній порушник, що діє через образу на керівництво об'єкта, не має зброї чи інших активних засобів впливу (вибухівки тощо), але може втрутитись у керування технологічними процесами на об'єкті, через що може статися збій у функціонуванні ОКІ або аварія;
- *відповідальність держави та оператора* – внутрішній порушник, що діє на критично- чи життєво важливому об'єкті КІ у зговорі з диверсійно-терористичною групою, оснащення якої не перевищує показників, встановлених проектною загрозою на національному рівні;

[201] Відповідно до рекомендацій МАГАТЕ визначено низку основоположних принципів щодо встановлення та підтримки режиму фізичного захисту, зокрема щодо відповідальності: держави (принципи A та B), органу регулювання безпеки (принцип D), операторів (принцип E), проведення державою оцінки загрози (принцип G) тощо.

- *відповідальність держави* – незаконне збройне формування, що має на озброєнні важку військову техніку (позапроектна загроза).

При цьому роль держави полягає не тільки в нейтралізації позапроектних загроз чи участі в нейтралізації проектних загроз КІ, а й у: розробці та впровадженні єдиних методологічних підходів, на основі яких мають бути проаналізовані загрози КІ, сформована модель загроз, підготовлена проектна загроза КІ на національному рівні (залежно від категорії критичності об'єктів інфраструктури); наданні методологічної підтримки операторам КІ в розробці об'єктових проектних загроз, планів їх попередження та нейтралізації; оцінці ефективності діяльності у сфері захисту критичної інфраструктури.

3.6. Паспорти безпеки об'єктів критичної інфраструктури

3.6.1. Нормативно-правові засади формування вимог до захисту об'єктів критичної інфраструктури

У Концепції створення державної системи захисту критичної інфраструктури [202], серед проблем, що потребують розв'язання, йдеться і про необхідність розроблення методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядку їх паспортизації та категоризації.

В існуючих сьогодні функціональних системах забезпечення безпеки галузевих об'єктів частково передбачено врегулювання цих аспектів, щоправда, лише для окремих типів загроз. Так, у сфері цивільного захисту відповідно до Закону України «Про об'єкти підвищеної небезпеки» [203] передбачено декларування безпеки об'єкта підвищеної небезпеки шляхом підготовки документа, в якому наводяться результати аналізу ступеня небезпеки та оцінки рівня

[202] Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету Міністрів України від 06.12.2017 № 1009-р // База даних «Законодавство України»/ВР України. URL: http://zakon3.rada.gov.ua/laws/show/1009-2017-%D1%80

[203] Про об'єкти підвищеної небезпеки: Закон України від 18.01.2001 № 2245-III // База даних «Законодавство України»/ВР України. URL: http://zakon0.rada.gov.ua/laws/show/2245-14

ризику цього об'єкта. Також цей документ визначає комплекс заходів, що вживаються суб'єктом господарської діяльності з метою запобігання аваріям, а також для забезпечення готовності до локалізації, ліквідації аварій та їхніх наслідків.

У системі фізичної ядерної безпеки діє Порядок проведення оцінки вразливості ядерних установок та ядерних матеріалів [204]. Дія цього документа поширюється на експлуатуючі організації та інших ліцензіатів, що визначають, створюють і підтримують безперервне функціонування системи фізичного захисту ядерних установок та ядерних матеріалів або системи фізичного захисту ядерних матеріалів I та II категорій при їх перевезенні. Завдання проведення цієї оцінки вразливості такі: виявлення вразливих цілей правопорушників; аналіз потенційних радіаційних наслідків вчинення протиправних дій щодо вразливих цілей правопорушників; оцінка ризиків; розроблення рекомендацій щодо приведення стану системи фізичного захисту ядерної установки та ядерних матеріалів, системи фізичного захисту ядерних матеріалів при їх перевезенні у відповідність до вимог чинного законодавства.

Стосовно антитерористичної захищеності об'єктів критичної інфраструктури треба зазначити, що в рамках державної системи фізичного захисту за результатами оцінки вразливості формуються документи, що певною мірою відповідають паспорту потенційно небезпечного об'єкта (ПНО), але є значно ширшими з точки зору оцінки загроз [205]. Так, Звіт з оцінки вразливості, окрім загальних даних про об'єкт та виявлені джерела небезпеки, містить опис загроз, сценарії дій правопорушників та оцінює здатність системи фізичного захисту та об'єктового плану взаємодії протистояти визначеним загрозам [206].

---

[204] Про затвердження Порядку проведення оцінки вразливості ядерних установок та ядерних матеріалів: Наказ Державного комітету ядерного регулювання України від 30.11.2010 № 16 // База даних «Законодавство України»/ВР України. URL: http://zakon2.rada.gov.ua/laws/show/z1309-10

[205] Про затвердження Порядку функціонування державної системи фізичного захисту: Постанова Кабінету Міністрів України від 21.12.2011 № 1337 // База даних «Законодавство України»/ВР України. URL: http://zakon0.rada.gov.ua/laws/show/1337-2011-%D0%BF

[206] Про затвердження Порядку проведення оцінки вразливості ядерних установок та ядерних матеріалів: Наказ Держатомрегулювання України від 30.11.2010 № 169 // База даних «Законодавство України»/ВР України. URL: http://zakon2.rada.gov.ua/laws/show/z1309-10

Аналогічні заходи передбачені й у РФ, зокрема щодо забезпечення безпеки об'єктів енергетики [207]. Водночас паспорт безпеки об'єкта енергетики в Росії відображає не лише характеристики цього об'єкта з точки зору його потенційної небезпеки (категорії небезпеки, отриманої з урахуванням властивостей небезпечних речовин, що використовуються на об'єкті, та за впливом уражаючих факторів, що можуть мати місце у разі аварії на об'єкті), а й можливі наслідки в результаті незаконного втручання у функціонування об'єкта, оцінку стану систем інженерно-технічного та фізичного захисту, заходи із забезпечення антитерористичної захищеності. При цьому інформація, яка міститься в паспорті безпеки, віднесена до інформації з обмеженим доступом.

У частині формування бази даних щодо стану захисту об'єктів, то на сьогодні найбільш пристосованим до вирішення завдань БСКІ є підхід до паспортизації потенційно небезпечних об'єктив, що здійснюється Державною архівною службою України.

Відповідно до «Положення про паспортизацію потенційно небезпечних об'єктів» [208] проводиться ідентифікація та паспортизація цих об'єктів шляхом підготовки і надання паспорта потенційно небезпечного об'єкта. Паспорт потенційно небезпечного об'єкта є документом визначеної форми, що містить структуровані дані про окремий потенційно небезпечний об'єкт. Це насамперед загальна інформація про об'єкт, дані про небезпечні природні умови та технологічні процеси, дані щодо основних джерел небезпеки та об'єктів впливу надзвичайних ситуацій, аварійно-рятувальна документація тощо. Форми паспортів ПНО відповідають певному виду господарської діяльності, у т. ч. шахти, гідротехнічні об'єкти, магістральні трубопроводи, родовища корисних копалин. Ідентифікація потенційно небезпечного об'єкта є процедурою виявлення на об'єкті джерел та чинників небезпеки, на підставі яких об'єкт визнається потенційно небезпечним.

Реєстрація потенційно небезпечних об'єктів в Україні розпочалася після прийняття Постанови Кабінету Міністрів України «Про

[207] О безопасности объектов топливно-энергетического комплекса: Федеральный закон РФ от 21.07.2011 № 256-ФЗ // ИПС «Закон». URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102149573&rdk=&backlink=1

[208] Про затвердження Положення про паспортизацію потенційно небезпечних об'єктів: Наказ Міністерства України з надзвичайних ситуацій від 18.12.2000 № 338 // База даних «Законодавство України»/ВР України. URL: http://zakon2.rada.gov.ua/laws/show/z0062-01

затвердження Положення про Державний реєстр потенційно небезпечних об'єктів» [209]. Нині Реєстр ПНО є автоматизованою інформативно-довідковою системою, що забезпечує облік та обробку інформації щодо потенційно небезпечних об'єктів. База даних Реєстру містить актуальну інформацію про понад 26 тис. потенційно небезпечних об'єктів, що включають підприємства, родовища нафти та газу, магістральні трубопроводи та відгалуження, гідротехнічні об'єкти, вугільні шахти, автозаправні станції, кар'єри, мости, віадуки, шляхопроводи, сухопутні тунелі, підземні станції та тунелі метро тощо.

Ураховуючи викладене вище, зазначимо, що формалізація вимог щодо оцінки готовності власників ОКІ, щоб забезпечити їхню безпеку та стійкість функціонування, є цілком можливою. Понад те, паспортизація ОКІ є одним із ключових елементів розбудови в Україні державної системи БСКІ.

3.6.2. Основні вимоги до розробки паспортів безпеки об'єктів критичної інфраструктури

Паспорт безпеки ОКІ має стати документом визначеної форми, що містить структуровані дані про окремий ОКІ та визначає комплекс заходів, які вживаються оператором з метою забезпечення захисту цього об'єкта.

Метою формування паспортів безпеки ОКІ є визначення загроз та оцінки можливих ризиків негативних наслідків їхнього прояву для КІ, визначення напрямів забезпечення їхньої безпеки для подальшої розробки на цій основі заходів із запобігання та попередження прояву загроз для ОКІ.

При формуванні паспортів безпеки ОКІ необхідно враховувати всі типи загроз. При цьому серед усіх загроз різного походження для безпеки критичної інфраструктури найбільш актуальними можна вважати такі [210]:

---

[209] Про затвердження Положення про Державний реєстр потенційно небезпечних об`єктів: Постанова Кабінету Міністрів України від 29.08.2002 № 1288 // База даних «Законодавство України»/ВР України. URL: http://zakon5.rada.gov.ua/laws/show/1288-2002-%D0%BF

[210] Risk assessment methodologies for critical infrastructure protection. Part II: A new approach.

- *природні*: повені, екстремальні погодні явища, лісові пожежі, землетруси, епідемії та пандемії, епізоотії;
- *техногенні*: а) *незловмисні*: промислові аварії, ядерні/радіологічні аварії, аварії на транспорті, втрата критично важливої інфраструктури; б) *зловмисні*: кібератаки, терористичні атаки.

Формуючи паспорти безпеки ОКІ, загрози КІ слід також розглядати не тільки з точки зору характеру їх походження, а й з точки зору визначення елементів КІ, на які ці загрози спрямовані: фізичні елементи; системи управління та комунікації; персонал об'єктів, який безпосередньо забезпечує функціонування критичної інфраструктури.

Встановлення спрямованості дії загроз методологічно дозволяє більш системно підійти до формування державної політики та організації системи БСКІ. У планах захисту КІ, розроблених операторами, погоджених і схвалених відповідними державними органами, мають бути докладно описані заходи протидії загрозам за такими *напрямами захисту*:

- фізичний захист – спрямований на забезпечення захищеності ОКІ від несанкціонованого доступу, попередження та припинення диверсій, крадіжки або будь-якого іншого незаконного вилучення обладнання, пристроїв та матеріалів;
- технічний захист – забезпечення технологічної безпеки, підвищення відмовостійкості та живучості систем, функціональне резервування;
- персонал – підготовка та перевірка персоналу, контроль його здатності до виконання визначених функцій, захищеність персоналу;
- інформаційні технології – захист інформації, систем зв'язку і управління;
- юридичний – врегулювання питань функціонування інфраструктури у кризових ситуаціях, закріплення розподілу відповідальності у нормативних і правових документах, розробка керівництв та інструкцій для персоналу, у т. ч. щодо взаємодії в умовах кризової ситуації;
- відновлення – створення планів, резервів та сервісів для швидкого відновлення втрачених функцій.

Особливої уваги потребують взаємозв'язки та взаємозалежності між окремими елементами КІ, коли виникнення одних небезпечних явищ призводить до формування нових через механізм каскадних

ефектів. Усвідомлення каскадних ефектів сучасних загроз є досить складним через взаємозв'язок об'єктів інфраструктури та їх вплив на забезпечення виконання життєво важливих функцій суспільства та держави. Цей аспект має знайти відображення вже на етапі аналізу загроз на нижчому, об'єктовому рівні та повинен бути окремо виділений у паспорті безпеки ОКІ.

Загалом паспорт безпеки ОКІ має включати інформацію щодо загальних відомостей про об'єкт, природно-кліматичних і географічних умов місця розташування ОКІ, зв'язків з іншою інфраструктурою, впливу об'єкта на забезпечення життєво важливих функцій чи послуг, готовності персоналу до дій в умовах виникнення загроз чи кризової ситуації, вимоги до організації охорони та фізичного захисту ОКІ, характеристики основних джерел небезпеки, взаємодії із іншими суб'єктами тощо [211].

Паспорт безпеки, окрім ідентифікації загроз ОКІ та заходів щодо його захисту, має також передбачити узгодження дій оператора із діями інших суб'єктів державної системи БСКІ. Цей аспект має бути відображений через врахування наявності планів запобігання, реагування, взаємодії та відновлення ОКІ.

Нижче наведено види планів, які також розробляються оператором КІ, і зміст того, що в них повинно враховуватися.

- *План запобігання*: заходи зі зниження рівня загроз; заходи зі зниження вразливості; заходи з мінімізації можливої шкоди; заходи з підвищення технічної надійності; навчання та тренування.
- *План реагування*: аварійний план; план взаємодії на випадок диверсії; план протидії кіберзагрозам; план безперервності ведення бізнесу.
- *План відновлення*: заходи з відновлення; заходи з диверсифікації (наявності альтернатив); заходи з резервування (наявності резервних виробництв та/або ресурсів).

Паспорти безпеки ОКІ разом із планами запобігання, реагування, взаємодії та відновлення мають надати системну базу для складання Національного плану захисту критичної інфраструктури [212], у якому має бути визначена система взаємодії суб'єктів захисту

[211] Детальна структура Паспорта безпеки ОКІ наведена в *Додатку 1.5*.

[212] Пропозиції щодо структури та змісту Національного плану захисту критичної інфраструктури наведені в *Додатку 2*.

критичної інфраструктури та розподіл ресурсів на загальнодержавному рівні для запобігання загрозам, пом'якшення можливих наслідків, реагування на реалізовані загрози та відновлення КІ.

Загалом паспорт безпеки має містити висновок щодо достатності сил і засобів для виконання заходів забезпечення безпеки та стійкості ОКІ та в разі необхідності перелік додаткових заходів з удосконалення та усунення виявлених недоліків із зазначенням термінів їх виконання.

Паспорти безпеки мають готуватися операторами ОКІ та надаватися на погодження до суб'єктів захисту, відповідальних за сектори критичної інфраструктури. Форма Паспорта безпеки ОКІ, порядок його розробки, наповнення, зміст і строки подання має встановлювати Кабінет Міністрів України.

Після проведення паспортизації має відбутися внесення даних Паспорта безпеки ОКІ до Реєстру критичної інфраструктури об'єктів. Враховуючи те, що інформація, яка міститься у паспорті безпеки, може бути віднесена до інформації з обмеженим доступом, порядок ведення Реєстру, а також особливості надання інформації з Реєстру мають встановлюватися Кабінетом Міністрів України.

Слід відзначити, що паспортизація є одним з етапів проведення обліку ОКІ, який включатиме виконання комплексу заходів із забезпечення збирання, накопичення та актуалізації необхідної інформації щодо характеристик ОКІ, формування та адміністрування бази даних, а також забезпечення інформаційної підтримки суб'єктів державної системи БСКІ. Ураховуючи важливість інформації щодо об'єктів критичної інфраструктури для забезпечення національної безпеки держави, інформація, що використовується для обліку об'єктів критичної інфраструктури, може бути віднесена до інформації з обмеженим доступом або взагалі бути закритою. Зважаючи на важливість інформації, паспорт безпеки має бути погоджено з відповідальними органами за сектори захисту критичної інфраструктури та спеціальними службами сектору безпеки і оборони України.

Отже, паспортизація об'єктів критичної інфраструктури є складовим етапом створення державної системи БСКІ, що потребує дієвої взаємодії операторів, які мають формувати паспорти безпеки об'єктів критичної інфраструктури, секторальних органів виконавчої влади і спецслужб.

3.7. Проведення навчань і тренувань

Одними із організаційних заходів, спрямованих на захист і забезпечення стійкості КІ, є періодичні перевірки готовності до реагування на кризові ситуації, які здійснюються під час проведення різного роду навчань та тренінгів.

Метою розгляду готовності й планування є визначення того, що держава (регіон)/сектор КІ (галузь)/об'єкт КІ мають достатню нормативну базу, відповідні плани, кваліфікований та підготовлений персонал, оснащення та ресурси для дій у кризовій ситуації, координують свої плани й регулярно перевірять готовність шляхом навчань і тренувань.

Світова практика визначила цілий набір інструментів для проведення такої підготовки. Так, у США запропонована модель проведення комплексу навчальних (тренінгових) заходів, що передбачають [213]:

- *семінари* (Seminars) та *воркшопи* (Workshops). Семінари проводяться як активна форма залучення слухачів до ідентифікації окремих проблем у відповідній сфері чи обговорення нових підходів щодо діяльності в цій сфері, роз'яснення нових правил та процедур реагування тощо. У свою чергу, воркшоп передбачає активне залучення слухачів до вироблення спільної позиції щодо вирішення якої-небудь проблеми, розробки процедур реагування, планів дій тощо, тобто йдеться про спільний пошук шляхів вирішення проблеми;
- *настільні вправи* (Tabletop Exercises, TTX), під час яких обговорюються та відпрацьовуються шляхи реагування на якісь гіпотетичні події. Передбачається, що учасники в процесі дискусії здійснюють оцінку існуючих процедур, планів, регламентів щодо дій окремих інституцій за різними сценаріями. Фактично цей вид навчання передбачає визначення проблем у законодавстві і не спрямовується на оцінку дій персоналу;
- *ігри* різного роду (Games), під час яких також моделюються якісь гіпотетичні ситуації, але вже за участю різних команд, які протидіють та/або виступають союзниками у грі та діють відповідно до чинних правил;

[213] The Homeland Security Exercise and Evaluation Program / FEMA. URL: https://www.fema.gov/media-library/assets/documents/32326

- *функціональні вправи* (Functional Exercises), які здебільшого використовують для відпрацювання оцінки функціональності та ефективності існуючих процедур, планів реагування на сценарії розвитку ситуації. Цей вид навчання спрямований на перевірку спроможності персоналу діяти у визначених ситуаціях за встановленими планами та процедурами;
- *спеціалізоване (вузько спрямоване) навчання* (Drills), що проводиться в реальному часі в реалістичному оточенні, проте рух сил та засобів реагування відбувається лише в обмеженому обсязі, який визначається функціональною спрямованістю вправи. Такий вид навчання спрямований на перевірку спроможності персоналу діяти у визначених ситуаціях за встановленими планами та процедурами (приклад, евакуація у разі пожежі);
- *повномасштабні вправи* (Full-Scale Exercises), які проводяться в реальному часі в реалістичному оточенні та до яких залучаються реальні сили та засоби реагування у повному обсязі.

Для більшості цих навчальних і тренувальних заходів в українській інтерпретації відсутні аналоги, які повністю відповідають сутності цих понять. Водночас ці навчально-тренувальні заходи за сутністю відповідають заходам із підготовки та перепідготовки персоналу, під час яких слухачі набувають теоретичних знань (лекції, семінари, практичні заняття, колоквіуми тощо), та заходам із набуття практичних навичок – це протиаварійні, командно-штабні (штабні) і тактико-спеціальні (у т. ч. спеціальні об'єктові) навчання і тренування.

При цьому в українській практиці слід розрізняти різні види навчань/тренувань: спрямовані на отримання та закріплення *теоретичних знань*, на здобуття та закріплення *практичних навичок*, у т. ч. щодо взаємодії та відпрацювання злагодженості дій залучених сил. Проте в Україні термін «навчання» охоплює обидва ці напрями підготовки.

Слід зазначити, що в Україні проведення навчань передбачено для окремих державних систем захисту та реагування, зокрема ЄДСЦЗ [214],

[214] Відповідно до ст. 92 Кодексу цивільного захисту підготовка до дій за призначенням органів управління цивільного захисту здійснюється під час проведення командно-штабних (штабних) та інших навчань і тренувань (див.: URL: http://zakon0.rada.gov.ua/laws/show/5403-17/page5).

ЄСЗРПТА [215], ДСФЗ [216], НСК [217]. Найбільш детально методичні аспекти підготовки та проведення навчань (тренувань) в Україні висвітлені в низці відповідних документів ЄДСЦЗ [218] та ДФСЗ [219].

Поряд із тим слід відзначити, що практика проведення подібних навчань обмежується переважно рівнем оцінки дій персоналу щодо дотримання планів реагування на власних об'єктах, або ж підрозділів сил окремих державних систем захисту та реагування. Фактично тренування на загальнодержавному рівні, які б потребували залучення різних рівнів управлінської вертикалі й секторів КІ та спрямовувались на пошук неврегульованих проблем системи БСКІ, удосконалення законодавства, в Україні не проводилися.

---

[215] Відповідно до Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків (п. 4) передбачена взаємодія шляхом організації і проведення командно-штабних та тактико-спеціальних навчань і тренувань з використанням сил і засобів суб'єктів боротьби з тероризмом (див.: URL: http://zakon5.rada.gov.ua/laws/show/92-2016-%D0%BF).

[216] Відповідно до Закону України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» (ст. 16, 17, 22) у рамках Державного плану взаємодії центральних та місцевих органів виконавчої влади на випадок вчинення диверсій передбачені тренування (навчання), підготовка та перепідготовка персоналу (див.: URL: http://zakon5.rada.gov.ua/laws/show/2064-14).

[217] Відповідно до Стратегії кібербезпеки України (п. 4.1) та Закону України «Про основні засади забезпечення кібербезпеки України» (ст. 8) проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі віднесені до пріоритетних напрямів забезпечення кібербезпеки (див.: URL: http://zakon5.rada.gov.ua/laws/show/96/2016 ; http://zakon2.rada.gov.ua/laws/show/2163-19).

[218] Порядок підготовки до дій за призначенням органів управління та сил цивільного захисту: Постанова Кабінету Міністрів України від 26.06.2013 № 443 // База даних «Законодавство України»/ВР України. URL: http://zakon0.rada.gov.ua/laws/show/443-2013-%D0%BF ; Методичні рекомендації щодо підготовки та проведення командно-штабних навчань органів управління цивільного захисту: Наказ ДСНС України від 29.01.2014 № 44 // База даних «Законодавство України»/ВР України. URL: www.dsns.gov.ua/files/2014/1/30/Metod_rekom_khn.doc ; Рекомендації щодо проведення спеціальних об'єктових навчань і тренувань: Лист ДСНС України від 26.04.2017 № 16-6361/161 ; Порядок здійснення навчання населення діям у надзвичайних ситуаціях: Постанова Кабінету Міністрів України від 26.06.2013 № 444 // База даних «Законодавство України»/ВР України. URL: http://zakon0.rada.gov.ua/laws/show/444-2013-%D0%BF

[219] Про затвердження Вимог до об'єктового плану взаємодії у разі вчинення диверсії: Наказ Держатомрегулювання від 22.11.2010 № 163 // База даних «Законодавство України»/ВР України. URL: http://zakon5.rada.gov.ua/laws/show/z1264-10 ; Про затвердження Положення про державну систему професійної підготовки, перепідготовки та підвищення кваліфікації фахівців з фізичного захисту, обліку та контролю ядерних матеріалів: Постанова Кабінету Міністрів України від 21.03.2012 № 263 // База даних «Законодавство України»/ВР України. URL: є http://zakon5.rada.gov.ua/laws/show/263-2012-%D0%BF

Саме тому широкого резонансу в Україні набуло проведення у 2017 р. навчань національного рівня із залученням широкого кола суб'єктів державної системи БСКІ на загальнодержавному рівні COHERENT RESILIENCE 2017 (CORE 17), спрямованих на оцінку чинних планів та процедур реагування на загрози критичній електроенергетичній інфраструктурі [220].

На основі отриманого досвіду з організації та проведення зазначених навчань, а також використовуючи досвід країн НАТО, можна виокремити такі узагальнені підходи до навчань і тренувань, які доцільно розповсюдити на всі сектори КІ:

1) навчання залежно від масштабу та сфери охоплення можна поділити на багатонаціональні, загальнодержавні (національні), регіональні та місцеві (у межах областей та районів, у межах міст та районів у містах), секторальні або галузеві (у межах сектору КІ), корпоративні (у межах оператора КІ) та об'єктові (у межах ОКІ);

2) залежно від залучених на навчання сил та засобів суб'єктів захисту КІ, а також завдань, що відпрацьовуються на навчаннях/тренуваннях, їх можна поділити на командно-штабні (штабні) та тактико-спеціальні (у т. ч. спеціальні об'єктові) навчання і тренування;

3) мета навчань і тренувань полягає в отриманні комплексної оцінки відповідності державної системи БСКІ загрозам, що існують, та стану готовності суб'єктів державної системи БСКІ до дій, спрямованих на запобігання та реагування на кризові ситуації, а також відновлення після кризи. У свою чергу, комплексність оцінки досягається шляхом перевірки:

- достатності законодавчої бази у сфері БСКІ, відсутності в ній пробілів, неузгодженостей та суперечностей;
- наявності та продуманості відповідних планів запобігання кризи, реагування на кризу та відновлення після кризи;
- наявності кваліфікованого та підготовленого персоналу, достатності оснащеності, матеріальних та фінансових ресурсів для дій у кризовій ситуації;
- злагодженості дій залучених сил;

Загалом процес підготовки та проведення навчань/тренувань (управлінський цикл) включає: етап підготовки; етап проведення;

[220] Sukhodolia, O. (2018). Training as Tool of Fostering a CIP Concept Implementation: Results of Table Top Exercise on Critical Energy Infrastructure Resilience. *Information & Security: An International Journal*. Vol. 40. Issue 2.

етап розбору (етап аналізу та підготовки звіту за результатами навчань/тренувань).

Етап підготовки. Визначаються вихідні дані та розробляється пакет документів з навчань/тренувань, які, відповідно, містять на концептуальному рівні чи у більш деталізованому форматі: *концепцію (задум)* та *специфікацію навчань/тренувань*, які, у свою чергу, містять (концепція – на концептуальному рівні, специфікація – у більш детальному форматі):

а) тематику навчань/тренувань;

б) мету (aim) та цілі (objectives) навчань/тренувань;

в) етапи навчань/тренувань;

г) вимоги щодо: учасників навчальних/тренувальних груп; фасилітаторів/модераторів (координаторів спільної роботи учасників у навчальних/тренувальних групах); оцінки та аналізу результатів; зовнішньої підтримки, включно й адміністративної; логістичного, матеріально-технічного та фінансового забезпечення; розробки документів з навчань/тренувань, а саме такі: організаційно-розпорядчі документи (накази): організаційні вказівки з розподілом завдань та осіб, відповідальних за їх виконання (група з планування; сценарна група; група оцінки; група підтримки проведення); склад учасників навчальних/тренувальних груп, послідовність їх залучення та на який термін; перелік спостерігачів;

ґ) навчально-методичні документи: опис передісторії та інфраструктури – змодельованої вихідної геостратегічної ситуації, на фоні якої відбуваються події, передбачені сценарієм навчання/тренування, та інфраструктурної ситуації на території, на якій під час навчань/тренувань моделюються події; сценарій та підсценарії розвитку подій (в англомовній інтерпретації – віньєтки (vignettes), а також загальні ввідні, перелік питань для учасників (*примітка*: ці дані доводяться до учасників навчальних/тренувальних груп завчасно; при цьому з урахуванням принципу «нарощування обстановки» доцільно виокремити різні етапи моделювання розвитку кризової ситуації: передкризова ситуація; криза/конфлікт різного ступеня інтенсивності; посткризова стабілізація та відновлення); ввідні, які виносяться на опрацювання учасників навчальних/тренувальних груп (*примітка*: з метою внесення в хід навчань/тре-

нувань елементів напруженості та раптовості ці дані стають відомими учасникам груп лише безпосередньо під час навчань/тренувань та можуть відрізнятися від тих, що передбачені віньєтками); керівництво для фасилітаторів/модераторів з переліком питань за кожною віньєткою/ввідною для спрямування процесу обговорення в групах;

д) документи з планування: план-календар основних заходів з підготовки та проведення навчань/тренувань; програма навчань/тренувань (*примітка*: в цьому документі визначаються фасилітатори/модератори, відповідальні за організацію обговорення ввідних в навчальних/тренувальних групах, та представники групи оцінки, які відповідальні за аналіз та оцінку роботи учасників у групах; ця програма доводиться до всіх учасників навчань/тренувань); план опрацювання сценарію та доведення ввідних (*примітка*: цей документ доводиться лише до фасилітаторів/модераторів та групи оцінки).

Слід зазначити, що на етапі підготовки навчань/тренувань ключовою є роль групи з планування та сценарної групи. Важливо, щоб плани, як і сценарій, були реалістичними та правдоподібно відображали ситуацію. Водночас при опрацюванні ввідних учасникам доцільно зосереджуватися не на причинах, а на наслідках подій, які моделюються під час навчань/тренувань [221]. Для цього доцільно використовувати медіа (як при підготовці ввідних, так і при їх доведенні до учасників).

Зокрема, у сценарії при описі віньєток/ввідних повинні бути наведені такі дані про подію:

- *коли* відбулася подія (дата і час);
- *де* це сталося (місце події);
- *що* сталося (характер події);
- *хто* постраждав (первісні наслідки: кількість загиблих, постраждалих тощо);
- *як* це сталося (остання інформація про причини, а не про наслідки, є допоміжною та наводиться лише для того, щоб запобігти недовірі учасників до змодельованої ситуації).

[221] Інколи учасники навчань/тренувань оспорюють події, які моделюються ввідними, як неможливі. Одне із завдань фасилітаторів і полягає у припиненні подібних спорів та концентрації уваги учасників на наслідках цих подій.

Усі ці дані про подію мають бути достатньо реалістичними, щоб не викликати в учасників недовіру, яка може вплинути на хід обговорення та на його спрямування.

До ввідних доцільно включати події різного типу за походженням [222]:

- *стихійні лиха та екстремальні природні явища* (наприклад: землетруси; зсуви; провалля; сильне налипання снігу; дуже міцний мороз або сильна спека; сильний вітер; високі рівні води; посуха; пожежі тощо);
- *події техногенного характеру* (аварії на виробництві або під час перевезення; аварії, пожежі, вибухи, не пов'язані з протиправними діями; раптове руйнування споруд; катастрофи, наслідком яких може стати ураження об'єкта);
- *події, пов'язані з протиправними діями* (проникнення правопорушників на об'єкт, вчинення пожежі або вибуху; розсіювання небезпечних речовин; втручання у роботу технологічного обладнання (у т. ч. шляхом кібератак); вивід з ладу засобів системи фізичного захисту; напад на об'єкт із застосуванням транспорту; збройний напад чи обстріл об'єкта; підбурювання до та проведення масштабних акцій протесту, захоплення адміністративних будівель, перекриття доріг, переривання залізничного сполучення тощо).

З урахуванням сучасних безпекових викликів згаданий перелік потребує розширення, що і було враховано при підготовці підрозділу 3.5 пропонованої аналітичної доповіді.

Етап проведення навчань/тренувань. На цьому етапі здійснюються заходи, передбачені програмою та планом: з метою поглиблення теоретичних знань проводяться теоретичні заняття (лекції, семінари, воркшопи), під час яких учасників навчань доцільно ознайомити з кращою світовою практикою та логікою прийняття рішень щодо запобігання кризовій ситуації, реагування на неї та відновлення після кризи.

[222] Досить детальний перелік подій, що можуть призвести до кризової ситуації, наведений у Спільному наказі Міненерговугілля та МНС України від 15.09.2011 № 501/1001, зареєстрованому в Міністерстві юстиції України 06.10.2011 за № 1147/19885, що має назву «Про затвердження Вимог до визначення порядку дій персоналу підрозділу фізичного захисту, персоналу підрозділу обліку та контролю ядерних матеріалів в умовах надзвичайних і кризових ситуацій».

Під час етапу тренувань з метою прищеплення практичних навичок учасниками опрацьовується сценарій та ввідні. При цьому важливо, щоб учасники усвідомили весь задум навчань, надзавдання, а не реагували на окремі ввідні. Доцільно заохочувати ініціативу, самостійність і творчий підхід учасників щодо пропонованих і прийнятих ними рішень. Саме в цьому полягає роль фасилітаторів і групи оцінки. Перші разом зі своїми помічниками мають скеровувати дискусію в групах у плідне русло (зокрема, використовуючи і питання/підказки, наведені в керівництві для фасилітаторів), а члени групи оцінки – не втручаючись у хід дискусії, детально фіксувати хід обговорення, підстави, на яких приймаються рішення, та самі рішення, пропоновані та прийняті учасниками. У разі нестачі інформації для прийняття рішень слід дозволяти учасникам робити розумні припущення. Водночас потрібно стримувати фантазії учасників щодо того, «що було б, якби…». Учасникам потрібно сконцентруватися на поставленій перед ними проблемі, на наслідках змодельованої ситуації та не намагатися переробити сценарій, віньєтки чи ввідні.

З метою зняття психологічної напруги в учасників навчань/тренувань доцільно запевнити їх, що за результатами навчань будуть оцінюватися не конкретні люди (тобто самі учасники), а стан справ із захистом КІ на відповідному рівні, недосконаліть системи захисту, що дозволить знайти проблемні питання та розв'язати проблему на системному рівні.

Етап розбору. Проводиться аналіз навчань/тренувань та готується звіт за їх результатами. Розбір є заключною частиною навчання/тренування і відіграє велику навчально-виховну роль та має значення з точки зору виявлення проблемних питань і пошуку шляхів їх вирішення. Основою розбору є висновки групи оцінки.

Окрім того, доцільним є й проведення опитування учасників стосовно їхніх вражень від навчань/тренувань, виявлених проблемних питань та пропозицій щодо шляхів вирішення останніх.

Під час аналізування дій учасників навчання/тренування розглядаються:

- особливості проведеного навчання/тренування, вимоги, що пред'являлися до його учасників, відповідність учасників цим вимогам;
- уміння аналізувати дані та адекватно оцінювати ситуацію;

- хід обговорення та рішення учасників, їхня об'єктивність та неупередженість, своєчасність прийняття та розуміння наслідків прийнятих рішень;
- здатність до командної роботи та взаємодії.

У звіті про проведення навчань/тренувань наводиться:

- тема навчання/тренування;
- склад та аналіз дій учасників (за кожною віньєткою/ввідною з розбивкою за відомствами/органами, які учасники представляли);
- ступінь досягнення цілей;
- основні шляхи вирішення виявлених проблемних питань у сфері захисту КІ, у т. ч.: пропоновані заходи з розробки та вдосконалення нормативно-правової бази; основні напрями підвищення готовності до дій у кризовій ситуації за призначенням, у т. ч. злагодженості та взаємодії.

Подібні підходи були використані при підготовці та проведенні в 2017 р. командно-штабних навчань з питань захисту критичної електроенергетичної інфраструктури та реагування на загрози порушення стійкості її функціонування на загальнодержавному рівні COHERENT RESILIENCE 2017 (CORE 17) (Tabletop Exercise за класифікацією НАТО) [223].

Командно-штабні навчання CORE 17 проводилися в рамках виконання річної програми співробітництва Україна – НАТО на 2017 р. Співорганізаторами навчань виступили Міністерство енергетики та вугільної промисловості України, Центр передового досвіду НАТО з питань енергетичної безпеки (NATO ENSEC COE, м. Вільнюс, Литва) та НІСД (м. Київ). До підготовки та проведення навчань була залучена Військово-морська вища школа США (Naval Postgraduate School, NPS). Представники НІСД, NATO ENCEK COE та NPS брали участь в оцінюванні навчань та спільно підготували відповідний звіт.

Участь у навчаннях взяли понад 80 українських представників від різних міністерств та відомств, у т. ч. правоохоронних та воєнних, а також енергетичних компаній України, і приватних включно.

[223] Проведено командно-штабні навчання з питань захисту критичної електроенергетичної інфраструктури та реагування на загрози порушення стійкості її функціонування на загальнодержавному рівні –COHERENT RESILIENCE 2017 (CORE 17). URL: http://www.niss.gov.ua/articles/2718/

Безпосередньо етап проведення навчань включав три фази:

- академічний семінар у Національному інституті стратегічних досліджень (16–17 жовтня 2017 р.);
- командно-штабні навчання на базі НЕК «Укренерго» (18–19 жовтня 2017 р.);
- попередній аналіз результатів навчань на базі НЕК «Укренерго» (20 жовтня 2017 р.).

На етапі аналізу та звітності групою з оцінки були підготовлені попередній та фінальний звіти з оцінки.

Загальною *метою* навчань CORE 17 було виявлення проблемних питань забезпечення ефективності управління захистом критичної електроенергетичної інфраструктури на національному рівні в умовах виникнення та реалізації комплексних загроз цій інфраструктурі.

Цілі навчань: оцінити ефективність чинних у державі систем реагування та захисту, а також можливості стратегічної інформаційної комунікації держави в умовах виникнення кризової ситуації, зокрема щодо:

- наявності процедур запобігання та реагування на загрози електроенергетичній інфраструктурі різних типів (природного та техногенного характеру, неправомірних дій, включаючи кібер- та терористичні загрози); наявності планів та процедур забезпечення стійкості функціонування електроенергетичної системи в умовах кризи/особливого періоду;
- ефективності взаємодії різних існуючих державних систем запобігання та реагування на загрози КІ, наявності механізмів координації дій персоналу різних установ та організацій, що беруть участь у роботі зазначених систем; виявлення проблемних питань взаємодії існуючих державних систем запобігання та реагування на загрози інфраструктурі;
- достатності та ефективності механізмів захисту ОКІ із залученням сил сектору безпеки та оборони;
- достатності та ефективності функціонування інформаційно-комунікаційної системи з донесення необхідних повідомлень до адресатів (населення, органів влади, міжнародного співтовариства) в умовах кризи;
- обміну досвідом у сфері захисту КІ із НАТО.

Сценарій навчань охоплював розвиток подій та розгортання конфліктної ситуації між двома вигаданими країнами – Краєм та Остландом, які утворилися внаслідок колапсу колишньої Ост Імперії.

Основна ідея сценарію, географічне розміщення, інфраструктурно-технологічна складова взаємовідносин, а також політико-економічні відносини цього регіону мали безпосередню схожість із ситуацією в Південно-Східній частині України у 2014–2017 рр.

Розвиток подій за сценарієм охоплював чотири етапи:

1) передконфліктний період;

2) конфлікт низького рівня інтенсивності;

3) кризова ситуація;

4) постконфліктна стабілізація.

Ситуація на кожному етапі уточнювалася додатковими підсценаріями (віньєтками), які відображали перебіг подій за окремими предметними напрямами навчань (типами загроз) та відповідно до яких проводилася дискусія щодо реагування.

Деталізація сценарію, формування окремих ввідних здійснювалися з урахуванням необхідності застосування планів реагування на загрози будь-якого походження (природного та техногенного характеру, неправомірних дій), включно й непередбачувані.

Головний висновок навчань CORE 17: у рамках кожної з чинних державних (національних) систем захисту та реагування (воєнної організації держави, системи правоохоронних органів, системи цивільного захисту, системи боротьби з тероризмом, системи фізичного захисту, системи кіберзахисту) визначені об'єкти захисту та суб'єкти, що забезпечують їхній захист. У рамках кожної державної системи налагоджена взаємодія сторін, залучених до заходів із кризового реагування. Проте вищезазначене стосується лише загроз, на протидію яким спрямовані зазначені системи.

Гострота проблеми захисту критичної інфраструктури полягає в тому, що жодна з перелічених вище систем не призначена для реагування на всі види/типи загроз (природного, техногенного, соціального та воєнного характеру, включно й кібер- та терористичні загрози). Не передбачено також системи взаємодії на випадок загроз, які носять комплексний характер. Окрім того, жодна з цих систем не опікується питаннями *стійкості* об'єктів КІ та можливістю скорішого *відновлення функцій* КІ. Зазначене зумовлює відсутність

системного підходу до забезпечення БСКІ на національному рівні, який мав би враховувати численні взаємозв'язки її елементів.

Окрім того, в наявних державних системах захисту/реагування пріоритет надається захисту *об'єкта* та відсутнє розуміння необхідності збереження чи відновлення *цільової функції* більшої системи, елементом якої є такий об'єкт.

За результатами навчань CORE 17 була опрацьована низка рекомендацій Уряду країни та органам виконавчої влади щодо напрямів розбудови в Україні державної системи захисту критичної інфраструктури. Зокрема, запропоновано врахувати позитивний досвід ядерної галузі у сфері забезпечення безпечної експлуатації ядерних установок та протидії загрозам тероризму [224]. Крім того, потрібно враховувати, що забезпечення стійкості критичної інфраструктури має здійснюватися як шляхом реалізації заходів з охорони та оборони ОКІ, так і шляхом посилення готовності та своєчасного реагування на загрози природного й техногенного характеру, а також швидкого відновлення. При цьому пріоритет щодо відновлення має надаватися не відбудові конкретного об'єкта, а необхідності збереження чи відновлення *цільової функції* більшої системи, елементом якої є цей об'єкт.

Загалом на прикладі навчань COHERENT RESILIENCE 2017 можна зробити висновок про те, що командно-штабні навчання є достатньо ефективним елементом із розбудови в Україні державної системи безпеки критичної інфраструктури.

[224] Заходи, передбачені в рамках державної системи фізичного захисту, включають увесь ланцюжок дій – від оцінки загроз та категоризації об'єктів системи до встановлення конкретних вимог до систем фізичного захисту (залежно від категорії об'єкта), оцінки вразливості об'єктів, оцінки ризиків наслідків (зокрема, радіаційних), проведення перевірок систем фізичного захисту та планів взаємодії. Зазначені підходи доцільно розповсюдити й на систему захисту критичної інфраструктури, яка наразі створюється в Україні.

ПІСЛЯМОВА

Авторський колектив сподівається, що включені до збірника матеріали, підготовлені в НІСД упродовж останніх років, викличуть інтерес у науковців та фахівців-практиків, чия професійна діяльність пов'язана з проблематикою критичної інфраструктури, її захистом і стійкістю, а також із загальними питаннями національної безпеки та національної стійкості.

У своїх матеріалах автори приділили увагу різним аспектам проблематики забезпечення безпеки і стійкості критичної інфраструктури з тим, щоб продемонструвати читачеві все розмаїття комплексних проблем, які необхідно розв'язати для побудови державної системи захисту критичної інфраструктури України: від ролі вищого політичного керівництва держави у кризових ситуаціях, пов'язаних з критичною інфраструктурою, до безпосередньої «діяльності на місцях» щодо практичного реагування на загрози окремих об'єктів; від нагальної потреби у підвищенні рівня взаємодії та обміну інформацією між існуючими системами безпеки і кризового реагування до узгодження термінології, яка використовується в кожній із систем; від необхідності проведення регулярних міжвідомчих навчань і тренувань для відпрацювань процедур реагування до запровадження культури безпеки на виробничих об'єктах та в місцях масового перебування людей тощо.

Зведена в одне видання інформація про стан запровадження сучасної концепції захисту та стійкості критичної інфраструктури, забезпечення її безпеки та стійкості дає можливість оцінити обсяг і масштаби проблем, які стоять перед залученими суб'єктами у цій сфері, виокремивши такі основні напрями зусиль, що спрямовані на їх розв'язання:

1. Створення організаційно-правових засад державної системи забезпечення захисту (безпеки) та стійкості критичної інфраструктури стосовно усіх видів фізичних загроз та кіберзагроз на принципах управління відповідними ризиками, що передбачає, серед іншого, таке:

- у короткостроковій перспективі – завершення розробки і подання до Парламенту України проекту профільного Закону України «Про критичну інфраструктуру та її захист»;
- у середньостроковій перспективі – визначення (створення) державного органу, відповідального за координацію дій, взаємодію та обмін інформацією між усіма заінтересованими сторонами; розроблення методологічних, нормативних та організаційних засад урегулювання діяльності суб'єктів системи захисту критичної інфраструктури;
- у довгостроковій перспективі – завершення створення сучасної державної системи забезпечення захисту критичної інфраструктури, інтегрованої до системи забезпечення національної безпеки, оборони та стійкості України.

2. Розроблення й запровадження механізмів та інструментів, необхідних для підтримки сталого та ефективного функціонування державної системи захисту критичної інфраструктури, у т. ч.:

- розвиток науково-теоретичних та методологічних засад створення державної системи захисту критичної інфраструктури;
- побудова національної мережі системи кризових, ситуаційних та інформаційно-аналітичних центрів для підтримки процесу прийняття рішень щодо критичної інфраструктури;
- запровадження та розвиток державно-приватного партнерства, розвиток партнерських стосунків між усіма заінтересованими сторонами;
- розвиток науково-методологічної та технологічної бази для виконання заходів щодо безпеки та стійкості критичної інфраструктури;
- інтегроване по вертикалі та горизонталі планування заходів (діяльності) щодо безпеки та стійкості критичної інфраструктури;
- створення системи підготовки кадрів та освіти населення щодо безпеки та стійкості критичної інфраструктури.

При цьому слід ураховувати, що внаслідок надскладних безпекових, соціально-політичних і фінансово-економічних умов поточного розвитку країни, ускладнення безпекової ситуації на міжнародному рівні, а також рівня сучасних викликів та загроз національній безпеці Україна потребує якнайшвидше завершити процеси реформування сектору національної безпеки. Тому стосовно критичної інфраструктури в найближчій перспективі доцільно максимально швидко та послідовно використати кращу практику організації діяльності та передовий зарубіжний досвід у в цій сфері.

Авторський колектив переконаний, що це видання, де напрацьовані теоретичні та методологічні підходи до забезпечення безпеки і стійкості критичної інфраструктури, допоможе суб'єктам системи захисту критичної інфраструктури розробити необхідну правову основу для всієї подальшої роботи у цій сфері та забезпечити виконання рішення РНБОУ та Указу Президента України № 8/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури».

ДОДАТКИ

Додаток 1

ІНСТРУМЕНТИ ФОРМАЛІЗАЦІЇ ДІЯЛЬНОСТІ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Додаток 1.1

План захисту критичної інфраструктури (на прикладі плану запобігання виникненню криз у системах енергопостачання) [225]

1. Опис системи (критичної інфраструктури):
- сукупність об'єктів, мереж та ресурсів, поєднаних цільовою функцією (забезпечення споживачів енергією).

2. Висновки проведеного ризик-аналізу:
- оцінки ризиків критичній інфраструктурі (ризик = загроза × вразливість × наслідки) відповідно до встановленої методології [226]. Загалом виокремлюють загрози: a) політичні (у т. ч. воєнні); b) технологічні; c) комерційні (ринкові); d) соціальні; e) природні;
- оцінка узагальнених сценаріїв розвитку кризових ситуацій (відповідно до встановлених критеріїв).

3. Відповідність стандартам інфраструктури:
- визначення критичних елементів інфраструктури, зокрема найбільшого елементу інфраструктури (критерій *N-1*);
- засоби, обсяги та потужності, спроможні вчасно компенсувати втрату найбільшого елементу інфраструктури (критерій *N-1*) та забезпечити стандарти постачання (відповідно до встановлених вимог);
- інші запобіжні заходи, такі як підвищення взаємозамінності елементів інфраструктури та можливості забезпечити диверсифікацію енергопостачання (джерел та маршрутів).

4. Відповідність стандартам безпеки постачання:
- визначення заходів запобігання та реагування на кризу, що можуть бути реалізовані не ринковими механізмами (не порушуючи нормальний режим функціонування інфраструктури);

[225] На основі узагальнення вимог Регламенту ЄС № 1983/2017, проекту Регламенту щодо готовності електроенергетичної інфраструктури та положень Концепції створення державної системи захисту критичної інфраструктури в Україні.

[226] Детальніше див. *Додаток 1.3*.

– визначення заходів запобігання та реагування на кризу, що потребують застосування неринкових заходів (запровадження обмежень на діяльність учасників) з урахуванням чіткого визначення критеріїв та процедур їх запровадження та відміни;
– визначення заходів щодо безпеки постачання захищених категорій споживачів.

5. Заходи запобігання виникненню кризи:
– заходи, спрямовані на запобігання ризиків відповідно до ризик-аналізу (у т. ч. їх територіальний вимір, очікувану ефективність та результативність, економічні наслідки для споживачів);
– склад та структура інфраструктури та заходи забезпечення відповідності вимогам стандартів безпеки постачання та інфраструктурним стандартам;
– встановлення вимог до операторів інфраструктури в частині забезпечення захисту та надійності;
– встановлення вимог щодо проведення тренувань на випадок кризових ситуацій.

6. Подальший розвиток системи (інфраструктурні проекти):
– оцінка взаємовпливу існуючих та будівництва майбутніх об'єктів, мереж, міжсистемних зав'язків (інтерконекторів) на безпеку постачання на випадок виникнення кризових ситуацій.

7. Зобов'язання в частині безпеки постачання (у т. ч. безпека постачання захищених категорій споживачів):
– визначення захищених категорій споживачів та вимог щодо їх енергозабезпечення;
– зобов'язання, що накладаються на операторів інфраструктури або відповідних служб, щодо постачання споживачів, включно й вимоги щодо безпеки функціонування інфраструктури.

8. Узгодженість дій учасників:
– визначення ролі та повноважень компетентного органу, відповідального за координацію учасників системи;
– визначення кризового менеджера, його завдань та повноважень у кризовому реагуванні;
– встановлення процедур реагування учасників на випадок криз, у т. ч. регламент обміну інформацією, забезпечення захисту чутливої інформації;
– встановлення процедур інформування споживачів.

9. Регіональні аспекти безпеки постачання:
– розроблення механізмів співпраці з іншими постачальниками (послуг на рівні операторів інфраструктури, регіонів (країн));
– встановлення процедури звернення по допомогу до інших країн;
– встановлення процедур обміну інформацією щодо запобігання та подолання криз на регіональному та міждержавному рівнях.

Додаток 1.2

План реагування на випадок кризової ситуації [227]
(на прикладі плану реагування в системах енергопостачання)

1. Рівні кризової ситуації:

- опис етапів та вимог до функціонування інфраструктури відповідно до рівня кризи [228] (нормальне функціонування; підвищена увага; кризова ситуація; посткризове відновлення [229]);
- опис ролі та відповідальності учасників реагування відповідно до рівня кризи.

2. Визначення заходів відповідно до рівня кризи:

2.1. ***Нормальне функціонування (аналіз ризиків, оцінка імовірності реалізації загрози):***

- опис заходів, що готуються основними учасниками, залученими до функціонування інфраструктури;
- опис процедур, які застосовуються;
- опис результатів, очікуваних від застосування заходів та процедур для запобігання або підготовки до кризи;
- опис процедур обміну інформацією між залученими учасниками.

2.2. ***Підвищена увага (попередження, запобігання):***

(a) заходи реагування, які мають бути застосовані на цьому етапі (аналогічно до підпунктів попереднього етапу. – *Авт.*)

(b) опис вимог до звітності (інформування) учасників щодо реагування на цей рівень кризи;

2.3. ***Кризова ситуація:***

(a) встановлення переліку наперед визначених заходів, як із боку постачальників, так і споживачів, щодо забезпечення енергією споживачів у

[227] На основі узагальнення вимог Регламенту ЄС № 1983/2017, проекту Регламенту щодо готовності електроенергетичної інфраструктури та положень Концепції створення державної системи захисту критичної інфраструктури в Україні.

[228] *Рівень раннього попередження (попередження):* коли є конкретна, надійна інформація, що подія може статись і, ймовірно, призведе до значного погіршення ситуації з поставками і, швидше за все, призведе до виникнення ситуації високого ризику чи кризової (аварійної) ситуації.

Рівень оповіщення ризику (оповіщення): коли трапляється порушення поставок або надзвичайно високий попит газу, що має наслідком значне погіршення ситуації з постачанням, але ринок ще може регулювати порушення чи недостатність постачання переривання поставок без необхідності вдаватися до неринкових заходів.

Аварійний рівень (аварійний): у разі виключно високого попиту на газ, значного порушення поставок чи іншого значного погіршення ситуації з поставками та у випадку, коли всі відповідні ринкові механізми запроваджено, але постачання газу є недостатнім для задоволення попиту, то для забезпечення постачання газу (відповідно до встановлених вимог) додатково повинні бути застосовані неринкові механізми.

[229] Відповідно до положень Концепції створення державної системи захисту критичної інфраструктури.

кризовій ситуації, включно й комерційні угоди щодо компенсаційних механізмів у випадку припинення постачання;

(b) деталізація застосування заходів реагування на кризу, що можуть бути реалізовані неринковими механізмами (не порушуючи нормальний режим функціонування інфраструктури);

- короткий опис заходів і залучених учасників реагування;
- опис процедур, що застосовуються;
- опис результатів, очікуваних від застосування заходів та процедур для пом'якшення кризи;
- опис процедур обміну інформацією між залученими учасниками;
- заходи забезпечення нерозголошення отриманої комерційної інформації, захисту чутливої інформації;

(c) деталізація заходів реагування на кризу, що потребують застосування неринкових заходів [230]:

- короткий опис заходів та залучених учасників реагування;
- оцінка необхідності застосування заходів обмеження ринкових механізмів для подолання кризи та рівень (обсяг) їхнього застосування;
- детальний опис процедур імплементації заходів цього рівня (*хто* і *які* заходи буде застосовувати, *хто* має приймати рішення щодо їх запуску та відміни);
- визначення внеску неринкових заходів, які мають застосовуватись на етапі кризової ситуації, на доповнення до заходів ринкового регулювання (включно й компенсаційні механізми на випадок припинення постачання);
- оцінка результативності застосування неринкових заходів;
- обґрунтування відповідності заходів із положеннями щодо обмеження негативного впливу прийнятих заходів: на енергопостачання (потоки) на енергетичному ринку; на ситуацію в інших країнах ЄС; на доступ до транскордонної інфраструктури (відповідно до планів реагування на кризу);
- опис процедур обміну інформацією залучених учасників на цьому етапі;
- заходи забезпечення нерозголошення отриманої комерційної інформації, захисту чутливої інформації;

(d) вимоги щодо звітності учасників стосовно вжитих заходів.

[230] Орієнтовний перелік неринкових заходів (наводиться у Регламенті ЄС № 1983/2017) для застосування у кризовій ситуації: (a) з боку постачання: використання стратегічних запасів; використання альтернативних джерел енергії; генерування електроенергії на інших технологіях (видах первинного палива); термінове збільшення виробництва тощо; (b) з боку споживання: оперативні заходи зниження енергоспоживання; переведення на резервні види/джерела енергозабезпечення; застосування переривних контрактів; графіки відключення тощо.

2.4. ***Посткризове відновлення (відновлення та адаптація інфраструктури до нових умов):***

(a) встановлення переліку заходів, як з боку постачальників, так і споживачів, щодо відновлення нормального режиму функціонування інфраструктури;

(b) визначення заходів щодо адаптації інфраструктури до нових умов функціонування з урахуванням отриманих уроків;

(c) вимоги щодо звітності учасників щодо вжитих заходів.

3. Спеціальні заходи, спрямовані на безпеку систем життєдіяльності населення (у регламенті – сфера теплопостачання. – *Авт.*);

– визначення заходів та дій, необхідних для пом'якшення негативного впливу припинення газопостачання на інші системи життєзабезпечення;

– деталізація обсягів енергопостачання, що мають постачатися захищеним категоріям споживачів, та заходів забезпечення таких поставок.

4. Кризовий менеджер або кризова команда:

– визначення ролі та встановлення детальної процедури діяльності кризового менеджера відповідно до рівня кризової сиутації;

– встановлення детальної процедури та заходів, які необхідно вжити за різними рівнями кризових ситуацій, також ідеться й про схему взаємодії та обміну інформацією.

5. Ролі та відповідальність учасників плану реагування:

– визначення ролі та відповідальності операторів інфраструктури і споживачів, а також їх взаємодії із відповідними органами влади у випадку виникнення кризових ситуацій відповідно до встановлених рівнів;

– визначення ролі та відповідальності відповідних органів влади, інших служб відповідно до задач плану реагування на різні рівні кризової ситуації.

6. Заходи щодо запобігання порушенню встановлених режимів постачання незахищених категорій споживачів:

– процедури та режими (обсяги) постачання споживачів відповідно до рівня кризи;

– заходи контролю за режимами споживання споживачів відповідно до рівня кризи.

7. Кризове тестування:

– встановлення вимог та графіків проведення тестувань на випадок кризових ситуацій.

8. Регіональний вимір: заходи відповідно до типу та рівня кризової ситуації; механізми взаємодії та взаємодопомоги; механізми солідарності між країнами:

– формування механізму забезпечення співпраці (солідарності) між країнами за різними рівнями кризової ситуації та обміну інформацією між визначеними компетентними органами.

Додаток 1.3

Проведення ризик-аналізу [231]

1. Опис системи

Опис сукупності мереж, об'єктів та елементів, які забезпечують цілісне функціонування КІ.

2. Стандарти безпеки (інфраструктурні, операційні)

Наводяться вимоги до параметрів нормального режиму функціонування КІ.

3. Ідентифікація загроз:

a) політичні (припинення постачання енергоресурсів з третіх країн з різних причин; політичні протести (у країнах постачальниках чи транзитних країнах); війни (у країнах-постачальниках чи транзитних країнах); тероризм);

b) технологічні (вибухи/пожежі; пожежі на обладнанні; витоки; низький рівень технічного обслуговування; збої та поломки обладнання; відсутність енергоживлення; збої в системі комп'ютерного управління технологічними процесами (програмні збої, Інтернет, проблеми із SCADA тощо); порушення внаслідок ремонтно-будівельних робіт тощо);

c) комерційні/ринкові/фінансові (контрактні зобов'язання з третіми країнами/постачальниками; комерційний спір); контроль енергетичної інфраструктури структурами третіх країн, які можуть нехтувати інвестиціями у розвиток інфраструктури; диверсифікацією; порушенням вимог законодавства ЄС; ринковим ціноутворенням; випадками різкого зростання попиту; іншими ризиками, що призведуть до неадекватного щодо реальної ситуації функціонування інфраструктури);

d) соціальні (страйки (у різних дотичних секторах, що впливають на функціонування КІ (інші галузі енергетики, транспорт тощо), диверсії, вандалізм, крадіжки тощо); кібератаки;

e) природні (землетруси, оповзні, підтоплення, шторми, лавини, екстремальні погодні умови; пожежі (у т. ч. ззовні поблизу об'єктів КІ) тощо).

4. Проведення ризик-аналізу:

– проаналізувати ризик-фактор відповідно до специфіки та актуальності для відповідного сектору КІ (ризик = загроза × вразливість × наслідки);

– опис критеріїв, які використовуватимуться для визначення, чи система підпадає під ризик високого/недопустимого ризику;

[231] На основі узагальнення вимог Регламенту ЄС № 1983/2017, проекту Регламенту щодо готовності електроенергетичної інфраструктури та положень Концепції створення державної системи захисту критичної інфраструктури в Україні.

– визначення набору ризик-сценаріїв відповідно до ризик-фактору та його вірогідності та опис того, як таке визначення було зроблено;

– ризик-сценарії повинні базуватися на врахуванні щонайменше таких ризиків:

(a) екстремальні природні загрози (явища) та такі, що трапляються рідко;

(b) випадкові загрози, що виходять за межі критерію безпеки *N-1*;

(c) побічні загрози, включаючи дефіцит палива;

(d) зловмисні цілеспрямовані атаки;

– при проведенні ризик-аналізу необхідно щонайменше враховувати такі чинники:

(a) розгляд усіх регіональних та національних обставин;

(b) взаємовплив та кореляцію ризиків у транскордонному вимірі;

(c) моделювання одночасних кризових сценаріїв;

(d) ранжування ризиків відповідно до їхньої ймовірності та наслідків;

– при проведенні ризик-аналізу на найближчий період (сезонний, тижневий, денний ризик-аналіз) необхідно щонайменше враховувати такі чинники:

(a) невизначеність даних для аналізу, як-от: імовірність пошкодження потужності передачі енергії, генеруючих потужностей, екстремальність погодних умов, непрогнозованість роботи відновлюваних джерел енергії тощо;

(b) імовірність настання критичних ситуацій;

(c) імовірність настання одночасних кризових ситуацій.

Додаток 1.4

Перелік секторів критичної інфраструктури

Життєво важливі функції/послуги	Елементи забезпечення функції/послуги	Сектор критичної інфраструктури	Підсектори	Відповідальні органи
1	2	3	4	5
Енергозабезпечення	Виробництво та постачання електроенергії, природного газу, нафтопродуктів; мережі передачі та розподілу енергоресурсів; основні генеруючі, видобувні, переробні потужності; значні родовища енергоресурсів; найбільші трансформаторні підстанції; системи технологічного управління роботою об'єктів та мереж, стратегічні резерви енергоресурсів (обладнання) тощо	Паливно-енергетичний комплекс	Електроенергетика Газ та нафта Ядерна енергетика *	Міненерго Міненерго Міненерго + Держатомрегулювання Держрезерв
Транспортування	Транспортна інфраструктура (дороги, центральні вузли перевантажень (вокзали); аеропорти; мости; трубопроводи, канали, фарватери, тунелі, дамби, системи технологічного управління роботою об'єктів та транспортних мереж тощо	Транспорт	Автомобільний Залізничний Авіаційний Водний Підземний (метро)	Мінінфраструктури Мінрегіон
Водопостачання, теплопостачання	Система водопостачання та водовідведення; водозабори, вузли підготовки води, опрацювання стічних вод; системи теплозабезпечення; системи технологічного управління роботою об'єктів та мереж, ресурси питної води тощо	Мережі життєзабезпечення	Теплопостачання Водопостачання	Мінрегіон

* У більшості країн, де використовують ядерну енергію, для неї виділяють окремий сектор. В Україні ядерна енергія відіграє дуже велику роль, тому цілком можливо розглянути її як окремий сектор КІ, у т. ч. враховуючи наявність Чорнобильської зони.

1	2	3	4	5
Продовольче забезпечення	Продовольчі ресурси, запаси продовольчих ресурсів на випадок криз; система якості виробництва та переробки продовольства; окремі об'єкти виробництва продовольчої продукції; великі регіональні зрошувальні системи; стратегічні запаси та резерви тощо	Харчова промисловість та агропромисловий комплекс		Мінагропром Держрезерв
Інформаційно-телекомунікаційна система	Система телекомункацій, поширення телевізійного та радіосигналів; система мобільного зв'язку; система фіксованого зв'язку, система спеціального зв'язку; система електронного врядування, бази даних; національна мережа Internet, програмне забезпечення адміністрування мереж тощо	Телекомунікації та зв'язок		Держспецзв'язок Мінінфраструктури
Фінансово-економічна інституційна основи	Система банків, страхових компаній; система фінансових трансакцій, платіжна система, бази даних тощо	Фінансово-банківський сектор		Міністерство фінансів України, Національний банк України
Охорона прав та законність	Мережа представництв правоохоронних органів та судів, центри надання адміністративних послуг; ситуаційні центри поліції; система зв'язку із правоохоронними органами тощо	Правоохоронна система		МВС, СБУ
Оборона країни та фізичний захист важливих об'єктів	Система органів та сил оборони, система ресурсного забезпечення сил оборони; система комунікацій та транспортного забезпечення сил сектору безпеки і оборони; система оборонних споруд тощо; система забезпечення безпеки (у т. ч. фізичної) найважливіших органів управління державою і відповідних об'єктів, будівель, систем тощо	Сектор безпеки і оборони		Міноборони, СБУ, АТЦ СБУ МВС, Управління державної охорони

1	2	3	4	5
Медичне забезпечення	Мережа поліклінік, лікарень, лабораторій; система швидкої допомоги; станції переливання крові та надання первинної медичної допомоги; аптечна мережа; бази даних, система ресурсного забезпечення (склади ліків) тощо	Служби екстреної допомоги		Міністерство охорони здоров'я Держрезерв
Реагування на випадок виникнення кризових ситуацій	Система органів та сил реагування на загрози природного та техногенного характеру, об'єкти підвищеної небезпеки (зокрема підприємства хімічної промисловості); система зв'язку та повідомлення про надзвичайні ситуації; система об'єктів інженерно-технічного захисту населення та територій тощо	Система цивільного захисту населення і територій		ДСНС України
Урядування	Система ресурсного та технічного забезпечення прийняття рішень; система доведення та контролю за виконанням прийнятих рішень; система суспільної комунікації з питань урядування; бази даних законодавства, державні реєстри, державні архіви; система адміністративних центрів надання послуг населенню, суб'єктам господарювання, окремі об'єкти культури національного значення тощо	Система державного управління		Секретаріат КМУ Державне агентство з питань електронного урядування України Мін'юст, Держархів

Джерело: складено автором.

Додаток 1.5

Паспорт безпеки
об'єкта/системи критичної інфраструктури

1. Загальні відомості про об'єкт

1.1. Довідкові дані: назва, адреса, контактна інформація, вид економічної діяльності, форма власності, підпорядкованість, сектор КІ, керівництво, контактна відповідальна особа.

1.2. Територія: географічні координати, відокремлені площадки, адміністративно-виробничі будівлі та споруди; санітарно-захисна зона, наближеність до інших об'єктів КІ.

1.3. Персонал та режим роботи: чисельність; час роботи, змінність, наявність на об'єкті підрозділу охорони, захисту державної таємниці, вимоги щодо безпеки (обмеження).

1.4. Основні фонди: потужність виробництва, період експлуатації, рівень зносу, балансова вартість.

1.5. Основні споруди і технологічне обладнання: критичні об'єкти, їх характеристики та місце розташування, категорійність (відповідно до існуючих вимог різних систем захисту та реагування), проектно-конструкторська документація та її утримувач, технічний стан (задовільний/незадовільний).

1.6. Особливості: відомості про внесення до державних (галузевих) реєстрів (кадастрів).

2. Зв'язок з іншою критичною інфраструктурою

2.1. Розміщення об'єкта відносно іншої КІ: інших ОКІ; об'єктів військового призначення; житлової забудови та населених пунктів; об'єктів масового скупчення людей; розташування ОКІ відносно іншої КІ (системи/об'єкти транспорту, зв'язку, енергетики тощо).

2.2. Забезпечення діяльності ОКІ: джерела основних ресурсів та шляхи їх постачання (матеріали, енергопостачання, водопостачання, зв'язок); маршрути пересування персоналу, відправлення продукції (послуг); наявні резерви (використовуваних ресурсів, готової продукції); методи утилізації відходів (маршрути їх вивезення).

2.3. Вплив на роботу іншої КІ: ідентифікація іншої КІ, на які може здійснювати вплив цей ОКІ; оцінка потенційного впливу функціонування сусідніх ОКІ; оцінка потенційного впливу на умови життєдіяльності населення навколишньої території, регіону.

3. Природно-кліматичні умови

3.1. Кліматичні умови: роза вітрів, температура; відносна вологість, параметри атмосферних опадів тощо.

3.2. Небезпечні природні умови: геофізичні (сейсмічність); геологічні (зсуви, обвали); гідрологічні (рівні води, розмиви берегів, посуха, припливи, хвилі); метеорологічні (спека або мороз, шквали та смерчі, удари блискавки, ожеледь); пожежі в природних екосистемах.

4. Технологічні процеси

4.1. Технологічний процес/обладнання: категорійність, вид небезпеки (вибухова, пожежна, хімічна, біологічна, ядерна, радіаційна тощо); відомості про речовини та матеріали, що використовуються на ОКІ; технологічні викиди та скиди шкідливих речовин, відповідність вимогам безпеки.

4.2. Оцінка небезпеки: аварії та порушення в роботі, що мали місце на ОКІ протягом останніх 10 років; події техногенного характеру, що можуть вплинути на ОКІ (на пов'язаних виробництвах); транспортна катастрофа; викиди речовин (вибухонебезпечних, горючих, токсичних); вибухи, пожежі, інші аварії, наслідком яких може бути ураження об'єкта, пожежа техногенного характеру, прорив дамб водосховищ.

4.3. Аварійно-рятувальна документація: аварійні плани, сили та засоби ліквідації аварій та їх наслідків; оцінка готовності персоналу до дій в умовах надзвичайних та кризових ситуацій; оснащення персоналу приладами, обладнанням, засобами індивідуального захисту; дані про початкове навчання персоналу, перевірку знань, тренувань учасників аварійного плану ОКІ.

4.4. Захисні споруди цивільного захисту: їхні характеристики.

5. Захищеність ОКІ [232]

5.1. Організація охорони та фізичного захисту ОКІ: опис конфігурації системи ФЗ ОКІ; дані про підрозділ фізичного захисту; дані про підрозділ охорони; дані про організаційно-розпорядчі документи, у т. ч. спільні з іншими органами державної влади; дані про плани взаємодії із залученими суб'єктами та силами, організація пропускного та внутрішнього режимів; рівень підготовки персоналу підрозділів фізичного захисту і охорони.

5.2. Інженерно-технічні засоби охорони: характеристики периметра зони охорони та складу засобів охорони (освітлення, сигналізація, наяв-

[232] Інформація цього розділу може бути віднесена до інформації з обмеженим доступом.

ність засобів радіо- та телефонного зв'язку, техніка контрольно-пропускних пунктів, засоби примусової зупинки транспорту тощо; характеристики засобів виявлення заборонених предметів і речовин; засоби електроживлення інженерно-технічних засобів охорони).

5.3. Об'єктова проектна загроза [233]***:*** вимоги щодо «проектної загрози» [234].

5.4. Оцінка вразливості ОКІ [235]***:*** характеристики ОКІ, важливі з точки зору захисту; цілі правопорушників (як у фізичному, так і кіберпросторі); сценарії дій правопорушників щодо їх цілей; оцінка ймовірності успішного протистояння системи захисту кожному сценарію дій правопорушників; оцінка ризику для ОКІ від здійснення кожного сценарію дій правопорушників; оцінка здатності систем захисту протистояти правопорушникам, оцінка стану культури захищеності на ОКІ.

5.5. Відповідність стану систем захисту ОКІ плану забезпечення захисту ОКІ.

6. Визначення рівня небезпеки та критичності ОКІ

6.1. Види небезпеки [236].

6.2. Реципієнти виникнення кризової ситуації на ОКІ (взаємозв'язок між елементами критичної інфраструктури): визначення рівня впливу на ОКІ різних секторів КІ [237]; оцінка каскадних ефектів (зниження обсягу функцій залежних систем та настання тяжких негативних екологічних, економічних, соціально-політичних наслідків).

6.3. Відсутність/наявність альтернатив та резервів на випадок порушення роботи ОКІ.

6.4. Масштаб впливу: територіальне поширення (локальне, район, регіон, вся держава, глобальне); функціональне (на рівні техпроцесу, ОКІ, галузі економіки, загальний для держави або групи держав).

6.5. Часові ефекти впливу: час появи негативних наслідків, тривалість негативного впливу, час на відновлення.

---

[233] Формується на основні проектної загрози критичній інфраструктурі на національному рівні з урахуванням особливостей ОКІ, технологічних особливостей ОКІ. Ця інформація має бути віднесена до інформації з обмеженим доступом та може бути винесена в окремий додаток.

[234] Див. *Додаток 1.6*.

[235] Ця інформація має бути віднесена до інформації з обмеженим доступом та може бути винесена в окремий додаток. Методологія оцінки вразливості ОКІ може базуватися на методології, визначеній у Порядку проведення оцінки вразливості ядерних установок та ядерних матеріалів, затвердженому Наказом Державного комітету ядерного регулювання України від 30.11.2010 № 169, зареєстрованому в Мінюсті 22.12.2010 за № 1309/18604.

[236] За узагальненими даними розділів 3 та 5 Паспорта безпеки ОКІ.

[237] Див. *Додаток 1.4*.

6.6. Тяжкість можливих наслідків: збиток здоров'ю та життю людей; ступінь порушення нормальних умов життєдіяльності суспільства та держави; економічна шкода; екологічна шкода; соціально-політична шкода; вплив на обороноздатність держави.

6.7. Визначення інтегрального показника критичності ОКІ.

7. Категорія, присвоєна об'єкту

7.1. Категорія об'єкта з цивільного захисту за: пожежною, вибуховою, хімічною, біологічною, радіаційною, ядерною небезпекою.

7.2. Категорія об'єкта за режимом.

7.3. Категорія об'єкта за ступенем критичності (критично важливий об'єкт; життєво важливий об'єкт; важливий об'єкт; необхідний об'єкт).

8. Додатки

8.1. Інформація щодо «Об'єктової проектної загрози».

8.2. Інформація щодо «Звіту з оцінки вразливості».

8.3. Інформація щодо планів запобігання, реагування, взаємодії, відновлення.

Додаток 1.6

Проектна загроза критичній інфраструктурі (на національному рівні)

1. Загальні положення

Базова проектна загроза (***модель загроз***) являє собою ***сукупність моделей (1) обстановки, (2) об'єкта та (3) порушника***, та містить перелік реальних та потенційних загроз критичній інфраструктурі (небезпечних чинників, подій, інцидентів, інших джерел ризику), що впливають на її безпечне функціонування та на захист від яких має бути розрахована державна система захисту критичної інфраструктури. Цей перелік є основою, що визначає, від кого та від чого потрібно захищатися на національному рівні. На його базі розробляються секторальні та об'єктові проектні загрози критичній інфраструктурі.

2. Модель обстановки

Модель обстановки враховує загрози КІ, зокрема [238]:

– дії країни-агресора, зокрема: військова агресія та розвідувально-підривна і диверсійна діяльність; руйнування систем життєзабезпечення; торговельно-економічна війна; монополізація стратегічних галузей національної економіки іноземним капіталом, залежність від монопольних постачань критичної сировини, насамперед енергетичних ресурсів; інформаційно-психологічна війна, пропаганда та інформаційні вкиди, маніпуляції суспільною свідомістю;

– діяльність незаконних збройних формувань, зростання злочинності;

– незадовільний стан економіки, зокрема: монопольно-олігархічна, низькотехнологічна, ресурсовитратна економіка; високий рівень «тінізації» національної економіки; спотворення ринкових механізмів, зокрема в енергетичному секторі; корупція; низька ефективність системи державного регулювання; низька конкурентоспроможність продукції, науково-технологічне відставання, відплив учених, фахівців, кваліфікованої робочої сили;

– незадовільний технологічний стан та низький рівень кіберзахисту: критична зношеність основних фондів об'єктів інфраструктури, відсутність перевірок стану обладнання; уразливість ОКІ та державних інформаційних ресурсів до кібератак, низький рівень підготовки персоналу.

[238] Модель обстановки базується на аналізі актуальних загроз національній безпеці, результати якого наведені в Стратегії національної безпеки.

3. Модель об'єкта

Модель об'єкта враховує загрози природного та техногенного характеру, зумовлені місцем розташування ОКІ, технологічними процесами, що використовуються на ОКІ, його продукцією та зв'язками з іншими об'єктами інфраструктури, та включає такі загрози:

3.1. Події природного характеру [239]**:** землетруси; зсуви; осідання (провалля) земної поверхні; налипання мокрого снігу; сильний мороз; сильна спека; посуха; сильний вітер та смерчі; високі рівні води, повені та підтоплення; пожежі в природних екосистемах; падіння метеорита тощо; епідемії та пандемії.

3.2. Події техногенного характеру: збої та відмова обладнання; помилки персоналу; аварії на виробництві або під час перевезення сировини/палива/робочих середовищ/продукції з викидом небезпечних речовин; пожежі, вибухи, затоплення приміщень об'єкта, не пов'язані з протиправними діями; раптова руйнація споруд та будівель; порушення внаслідок ремонтно-будівельних робіт; авіаційна катастрофа, аварія на залізничному, авто- або водному транспорті, наслідком якої може стати ураження об'єкта; втрата живлення; зниження частоти струму в системі електропостачання чи тиску в мережі газопостачання.

3.3. Переривання виробничих зв'язків: переривання транспортного сполучення (у т. ч. трубопровідного) та перебої з постачанням сировини, матеріалів, води, палива, енергії, викликані будь-якими причинами; розриви контрактів, у т. ч. викликані політико-економічними чинниками; обмеження на використання технологій, у т.ч. програмних продуктів та баз даних; форс-мажорні обставини, що призводять до виникнення обставин непереборної сили.

3.4. Відсутність альтернатив та резервів: відсутність альтернативних джерел та шляхів постачання сировини, матеріалів, води, палива, енергії; відсутність альтернативних технологій; відсутність резервів.

4. Модель порушника

Модель порушника враховує загрози протиправних дій будь-якого характеру, у т. ч. диверсійно-терористичного характеру, кібератаки, та являє собою сукупність якісних та кількісних характеристик порушника, його мотивацію та цілі. Модель порушника включає:

4.1. Опис порушника

Тип порушника: зовнішній; внутрішній; зовнішній, що діє у зговорі з внутрішнім.

[239] У контексті загроз розглядаються як звичайні події, що впливають на функціонування ОКІ (наприклад, випадіння снігу взимку тощо), так і аномальні події (природні лиха, аномальні температури тощо).

Категорії осіб, з числа яких може бути порушник:

– *зовнішні порушники:* терористичні (диверсійно-розвідувальні) групи, у т.ч. що діють під управлінням або за підтримки держави-агресора; кримінальні структури; злочинці, зокрема, вимагачі та шантажисти; хакерські угруповання, у т.ч. що діють під управлінням або за підтримки державних органів; хакери; хактивісти; недобросовісні партнери або конкуренти; незадоволене населення, підбурене до протиправних дій;

– *внутрішні порушники:* працівники ОКІ, що діють під тиском або примусом (через шантаж або загрозу застосування сили до них або їх близьких); завербовані агенти з числа персоналу ОКІ; невдоволений та агресивно налаштований персонал ОКІ.

Чисельність та склад: одиночний порушник; одиночна група у кількості до *N* осіб; кілька груп різної чисельності та складу; комбінація груп та окремих нападників.

4.2. Мотиви порушника: політичні або ідеологічні; економічні (отримання вигоди); особисті: дії через особисту образу, невдоволення, розчарування, в якості помсти тощо; дії заради самоствердження, задля розваги або в якості тренувань та демонстрації власної вправності; дії під впливом психотропних препаратів, наркотичних речовин або алкоголю.

4.3. Потенційні цілі:

– ***критичні фізичні елементи***, зокрема, технологічне обладнання та ресурси ОКІ;

– ***системи управління***, зокрема: системи автоматичного управління технологічними процесами (ОТ-системи, від *англ*. Operational Technology); інформаційно-комунікаційні системи (ІТ-системи та системи зв'язку, від *англ*. Information Technology); системи фізичного захисту;

– ***персонал об'єктів***.

4.4. Припущення щодо:

– ***знань, кваліфікації, практичних навичок, можливостей та налаштованості порушників:*** ступінь обізнаності з об'єктом (включно із системою захисту); можливості внесення змін у роботу систем управління та захисту; практичні навички щодо використання зброї, засобів зв'язку тощо; відданість справі та готовність порушників убивати та/чи бути вбитими.

– ***оснащення та екіпіровки порушника:*** транспортні засоби; засоби розвідки та радіоелектронної боротьби; засоби зв'язку та комунікації; засоби індивідуального захисту; озброєння.

4.5. Тактика дій у фізичному просторі.

Розвідувальні дії: засоби та методи дистанційного спостереження; незаконне приєднання до апаратури та ліній зв'язку, підслуховування та перехоплення даних; аналіз виробничих відходів та офісного сміття; отримання інформації від персоналу ОКІ, зокрема засобами соціального інжинірингу.

Відкриті насильницькі дії: фізичне проникнення на об'єкт, установлення вибухових пристроїв; вчинення пожежі або вибуху на об'єкті; розсіювання радіоактивних, небезпечних хімічних та/або біологічних речовин; напад на об'єкт із застосуванням транспорту; використання безпілотних літальних апаратів (БПЛА); збройний напад на об'єкт; обстріл об'єкта; захоплення та утримання заручників з персоналу об'єкта та охорони; втручання в технологічні процеси ОКІ; проведення диверсії на пов'язаній інфраструктурі.

Обманні та приховані дії: використання підроблених або вкрадених документів, ключів, біометричних даних; проведення операцій прикриття та відволікання уваги на інших об'єктах; крадіжка, зокрема ХБРЯ-матеріалів; викрадення документів.

Дії зовнішніх та внутрішніх порушників у зговорі: активні – допомога для входу/виходу, відключення сигналів тривоги, засобів контролю доступу, спостереження, зв'язку, участь у нападі; пасивні – розголошення або надання інформації про ОКІ, у т. ч. паролів; або те й інше.

Комбіновані дії: поєднання вищезгаданих тактик.

4.6. Тактика дій у кіберпросторі

Втручання в роботу інформаційно-комунікаційних систем, зокрема: порушення конфіденційності інформації (неправомірний доступ); порушення цілісності інформації (неправомірна модифікація чи знищення інформації); порушення доступності інформації (блокування, відмова в обслуговуванні).

Втручання в роботу автоматизованої системи управління технологічними процесами (АСУ ТП), зокрема загрози порушення: цілісності АСУ ТП (неправомірна модифікація процесів (алгоритмів управління) на апаратному та/або програмному рівні); спостережності АСУ ТП: втручання в роботу, що призвело до неможливості фіксації або помилкової фіксації діяльності користувачів і процесів; керованості АСУ ТП: неналежне реагування на команди управління; перехоплення та підміна команд управління та/або даних.

Методи, що використовуються для втручання в роботу IT-OT-систем: несанкціонований доступ, у т. ч. віддалений, неправомірне використання привілеїв; впровадження шкідливого програмного забезпечення; соціальний інжиніринг, спам та фішинг; DoS або DDoS атаки; наявність в програмному забезпеченні прихованих точок входу; цілеспрямовані, підготовлені довготермінові атаки, що використовують всі прийоми кібернападу.

4.7. Сценарії дій порушників мають враховувати реалістичні характеристики порушників та можливість комбінації дій у фізичному та кіберпросторі та розроблятися в рамках об'єктової проектної загрози для всього спектру цілей на ОКІ.

Додаток 2

ПРОПОЗИЦІЇ ДО НАЦІОНАЛЬНОГО ПЛАНУ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Національний план захисту критичної інфраструктури спрямований на формування спроможності країни забезпечити стійке та безперебійне забезпечення надання людині, суспільству та державі життєво важливих функцій (послуг).

Національний план формує механізм координації та спрямування зусиль держави, суспільства, суб'єктів господарювання та населення для забезпечення БСКІ, яка є основою реалізації життєво важливих функцій (послуг).

Національний план безпосередньо визначає організаційно-інституційну модель та механізми взаємодії суб'єктів державної системи БСКІ, а також встановлює їх основні завдання щодо забезпечення її безпеки та стійкості.

Національний план в частині, що стосується поширення чутливої інформації (державна чи комерційна таємниця), є документом з обмеженим доступом. Щорічно оприлюднюється узагальнена відкрита версія плану для забезпечення суспільства та суб'єктів державної системи БСКІ орієнтирами щодо пріоритетів дій та розроблення власних планів.

1. Цілі Національного плану

Стратегічне бачення Плану: безпечна та стійка країна, спроможна забезпечити безперебійне надання життєво важливих послуг та функцій, які є важливими для соціально-економічного розвитку та безпеки держави, суспільства, людини.

Цілі Плану:

- створення системи управління ризиками завдяки запровадженню заходів щодо ідентифікації загроз, їх оцінки та аналізу впливу, оцінки уразливостей та наслідків пошкодження КІ для життєдіяльності країни;
- формування системи забезпечення БСКІ від усіх типів загроз за характером походження (природного, техногенного характеру, викликані протиправними діями (фізичні та кібератаки)) та спрямованості (споруди, обладнання, ресурси, технологічні процеси, системи управління, персонал тощо);

– посилення готовності держави та операторів КІ до мінімізації наслідків виникнення кризових ситуацій завдяки узгодженому плануванню та застосуванню заходів реагування та пом'якшення наслідків реалізації загроз КІ;
– запровадження державно-приватного партнерства для забезпечення БСКІ, враховуючи витрати на захист та використовуючи переваги інвестицій у безпеку;
– формування системи ВОІ для управління ризиками КІ;
– забезпечення постійного розвитку знань та адаптації суб'єктів до появи нових викликів і загроз стійкості національної критичної інфраструктури завдяки формуванню заходів щодо навчання та підготовки персоналу, проведення тренінгів і навчань.

2. Сучасні виклики та пріоритети створення державної системи БСКІ

Для стабільного та безпечного існування сучасне суспільство та держава мають надійно отримувати цілу низку найрізноманітніших продуктів і послуг, мати доступ до важливих ресурсів. Для цього створюються і використовуються певні об'єкти, мережі та системи, які складають КІ забезпечення життєдіяльності суспільства та держави.

Безпекове середовище в країні та світі, що впливає на КІ, значно ускладнилося останнім часом. Захист критичної інфраструктури, що в останні десятиліття будувався з огляду переважно на загрози, пов'язані із фізичними загрозами та стихійними лихами, наразі все більше піддається впливу кіберзагроз та інших протиправних впливів, що постали з розширенням застосування інструментарію гібридних війн.

На сьогодні система захисту критичної інфраструктури має забезпечити спроможність реагування на загрози будь-якого виду та їх комбінацій.

План урегульовує дії суб'єктів системи щодо забезпечення БСКІ, зокрема формування спроможності:
– не допустити критичний негативний вплив загроз будь-якого виду та їх можливих комбінацій на функціонування критичної інфраструктури;
– надійного функціонування критичної інфраструктури у штатному режимі; адаптуватись до умов, що постійно змінюються, протистояти загрозам та швидко відновлюватись після реалізації загроз усіх типів.

План формує систему управління ризиками та зменшення вразливості КІ до загроз будь-якого типу, завдяки чіткій організації та плануванню діяльності суб'єктів системи забезпечення БСКІ, визначенню завдань та порядку ВОІ залучених суб'єктів системи впродовж усього циклу забез-

печення функціонування КІ та ймовірного розвитку кризової ситуації (ідентифікації загроз, запобіганні їх реалізації, кризового управління та відновлення КІ).

У практичному вимірі кінцевий **результат** запровадження Плану **полягає** у **забезпеченні захисту життєво важливих функцій та послуг**, які забезпечуються критичною інфраструктурою.

План визначає, що підтримання життєво важливих функцій життєдіяльності суспільства, захист базових потреб його членів і формування у них відчуття безпеки – базові умови забезпечення національної стійкості. Виділення найважливіших для життєдіяльності країни життєво важливих функцій, і тим самим секторів КІ, є інструментом визначення меж відповідальності та завдань системи БСКІ. Життєво важливі функції/послуги, надання яких забезпечується функціонуванням відповідних секторів КІ, також визначають розподіл та обсяг завдань для органів державної влади, залучених до функціонування системи БСКІ.

План ґрунтується на тому, що основні життєво важливі функції/послуги, підтримання яких має забезпечити відповідно КІ, такі:

- забезпечення належних умов життєдіяльності суспільства, передусім енергозабезпечення, транспортування, водопостачання, продовольче забезпечення;
- гарантованість медичної допомоги членам суспільства;
- розвиненість та ефективність фінансово-економічної інституційної основи національної економіки та життєдіяльності суспільства;
- розвиненість інформаційно-комунікаційної системи суспільства;
- ефективність системи реагування на випадок кризових ситуацій;
- керованість розвитку суспільства та дотримання членами суспільства визначених правил життєдіяльності;
- забезпечення оборони та безпеки країни.

План визначає сектори [240] критичної інфраструктури, які забезпечують визначені життєво важливі функції/послуги та відповідальних за формування державної політики ЗКІ у відповідних секторах органів державної влади.

План визначає механізми координації, взаємодії та обміну інформацією на різних рівнях та уточнення завдань суб'єктів державної системи відповідно до рівня загроз та режимів функціонування.

[240] Перелік секторів критичної інфраструктури, їх підсекторів та відповідальних за сектори органів державної влади наводиться в *Додатку 1.4*.

3. Система взаємодії, координації та управління

Широке коло завдань та необхідність залучення великого кола суб'єктів державної системи до узгодженої діяльності щодо забезпечення БСКІ потребує створення ефективної системи координації на загальнодержавному та місцевому рівнях.

План визначає основні завдання суб'єктів державної системи БСКІ відповідно до режиму функціонування системи, у т. ч. вимогу щодо формування з вимог законодавства у відповідних режимах (штатний режим, режим запобігання виникненню кризової ситуації, режим кризової ситуації, режим відновлення). (*Додаток до Національного плану*).

Рішення щодо запровадження визначеного режиму функціонування критичної інфраструктури здійснюється Кабінетом Міністрів України за зверненням національного уповноваженого органу з питань захисту критичної інфраструктури за процедурою, визначеною законодавством.

Планом встановлюється вимога щодо запровадження системи управління ризиками критичної інфраструктури. Завданням системи управління ризиками є забезпечення всіх суб'єктів державної системи чіткими та ефективними процедурами ВОІ з оцінки ризиків та періодичного проведення оцінки та аналізу наслідків реалізації загроз КІ на національному рівні; ініціювання необхідних змін системи забезпечення БСКІ.

Складовою такої системи і вимогою Плану є завдання щодо підготовки Національної оцінки ризиків для критичної інфраструктури. Планом передбачається проведення моніторингу загроз, які можуть спричинити негативні наслідки для критичної інфраструктури протягом наступних п'яти років.

Національна оцінка ризиків забезпечуватиме суб'єктів державної системи інструментами з оцінювання шкоди, що може бути спричинена реалізацією загроз, та формуватиме пріоритетні напрями запобігання виникнення кризової ситуації.

Проведення оцінки ризиків передбачає врахування масштабу та тривалості негативного впливу від реалізації загрози, вплив на пов'язані сектори КІ, виникнення каскадних ефектів та оцінку впливу на забезпечення життєво важливих функцій/послуг [241]. Це конфіденційна оцінка, що проводиться щороку і використовує експертизу широкого кола суб'єктів державної системи.

Для широкого загалу План передбачає оприлюднення загальнодоступної версії у вигляді **Огляду ризиків для критичної інфраструктури**. Цей документ слугуватиме для формування орієнтирів і порад населенню, громадам та бізнесу щодо планування своїх дій на випадок надзвичайних ситуацій цивільного характеру.

[241] Детальніше питання щодо проведення ризик-аналізу висвітлені у *підрозділі 3.3*.

4. Планування розвитку державної системи БСКІ

План визначає на найближчий період основні заходи щодо розвитку системи БСКІ, зокрема щодо розробки нормативно-правової бази забезпечення діяльності захисту критичної інфраструктури та завдань суб'єктів.

4.1. Розробки загальних законодавчих вимог до функціонування системи забезпечення БСКІ

План передбачає завдання суб'єктам державної системи щодо розробки нормативно-правової бази забезпечення БСКІ.

Термін підготовки – шість місяців після прийняття Закону України «Про критичну інфраструктуру» [242].

4.2. Розробки плану розвитку системи забезпечення БСКІ

План визначає завдання щодо розробки Плану заходів із розвитку системи забезпечення БСКІ.

Термін підготовки – щорічно.

План заходів із розвитку системи забезпечення БСКІ затверджується Кабінетом Міністрів України та має забезпечити визначення відповідальних органів державної влади за виконання таких заходів:

1. Управління ризиками

План передбачає формування узгодженого підходу до управління ризиками, який враховує імовірність реалізації загроз різного типу. Досягнути цього передбачається за допомогою різних засобів, у т. ч.: розширення кола загроз та учасників, залучених до процесу аналізу; розроблення профілів ризику та сценарного прогнозування розвитку ситуації; використання сучасних стандартів кризового менеджменту; моніторингу прогресу; подальшого тестування чинних планів через тренування та навчання. Досягнення цієї стратегічної мети забезпечить більшу чіткість та ефективність діяльності всіх суб'єктів системи, визначить пріоритетність діяльності та розподілу ресурсів.

Для досягнення цієї стратегічної мети суб'єкти державної системи в рамках своєї компетенції забезпечують:

– Запровадження комплексу формальних інструментів системи управління ризиками, а саме: **Національної оцінки ризиків КІ**; **Проектної загрози КІ**; **Секторальних проектних загроз**; **Планів запобігання реалізації загроз**; **Планів забезпечення стійкості забезпечення життєво важливих функцій/послуг (*реагування на кризові ситуації та відновлення КІ*).**

[242] Ці завдання мають відповідати плану законопроектної діяльності Кабінету Міністрів України за результатами прийняття Верховною Радою України Закону України «Про критичну інфраструктуру», проект якого наведено в *Додатку 3*.

Завданням є визначення та аналіз стійкості, міжсекторальних залежностей та взаємозалежності секторів КІ, усвідомлення суттєвих тенденцій та визначення основних загроз та оцінки вразливості КІ до загроз усіх типів (all-hazard approach).

Термін підготовки – не рідше одного разу на п'ять років.

– Запровадження системи постійного підвищення рівня кваліфікації персоналу завдяки таким інструментам: оцінка ризиків на місцях розміщення об'єктів критичної інфраструктури; навчання та підготовка персоналу; проведення практичних навчань і тренінгів. Практичні навчання є ефективними інструментами оцінки, апробації та вдосконалення планування дій суб'єктів БСКІ.

Термін підготовки – щорічно за встановленим графіком.

– Сприяння прийняттю та практичному застосуванню сучасних стандартів забезпечення БСКІ відповідно до ідентифікованого рівня загроз, технологічного розвитку та управлінської практики. Стандарти формують зручний інструмент допомоги операторам КІ щодо організації системи захисту своїх об'єктів на основі кращого світового досвіду.

Термін підготовки – не рідше одного разу на три роки.

– Формування системи моніторингу рівня БСКІ, зокрема шляхом визначення індикаторів оцінки діяльності з досягнення цілей та доведення результатів оцінки до зацікавлених суб'єктів.

Термін підготовки – щорічно.

2. Забезпечення партнерства суб'єктів державної системи

Посилення БСКІ вимагає взаємодоповнюючих та послідовних дій усіх партнерів для сприяння ефективності дій.

Для досягнення цієї стратегічної мети суб'єкти державної системи в рамках своєї компетенції забезпечують:

– Привернення уваги суспільства та держави до важливості забезпечення БСКІ. Формування програми дій та інструментів акцентування уваги підвищенні стійкості КІ забезпечить розуміння відповідної аудиторії (включно й галузеві мережі, урядові структури та громадськість). Необхідне запровадження періодичних звітів щодо БСКІ на різних управлінських рівнях.

Термін підготовки – щорічно.

– Формування платформи із співробітництва заінтересованих суб'єктів системи шляхом запровадження різнорівневих дискусійних, експертних майданчиків для обговорення проблематики та поширення кращого досвіду. Секторальні мережі забезпечують постійні форуми для обговорення та обміну інформацією між галузевими експертами та Урядом (секторальні комісії). Місцеві мережі забезпечують ту ж функцію між галузевими експертами, місцевими органами влади та населенням (територіальні

комісії). Необхідно також започаткувати функціонування національної платформи (Державна комісія) для оцінки ролі критичної інфраструктури в забезпеченні національної стійкості.

Термін підготовки – протягом одного року.

– Залучення бізнес-ініціативи до вдосконалення БСКІ шляхом формування інструментів стимулювання інвестицій у цю сферу. Створення нових комерційних інструментів для цілей захисту та стійкості критичної інфраструктури розширить коло зацікавлених осіб та знизить витрати.

Термін підготовки – 2 роки.

3. Запровадження обміну інформацією між суб'єктами системи

Обмін інформацією та захист інформації є взаємодоповнюючими елементами надійної основи для спільних зусиль щодо посилення БСКІ. Своєчасний обмін інформацією між Урядом та секторами КІ необхідний для ефективного управління ризиками й розуміння взаємозалежності та взаємодії між суб'єктами системи.

Для досягнення цієї стратегічної мети суб'єкти державної системи в рамках своєї компетенції забезпечують:

– Створення національної мережі ситуаційно-кризових центрів, розроблення регламентів обміну інформацією між різними суб'єктами системи.

Термін підготовки – протягом одного року.

– Розширення можливостей для обміну інформацією за допомогою різних засобів, включно й формальні угоди, віртуальні та фізичні механізми, а також створення та поширення інформаційних продуктів. У той же час розповсюдження та розголошення інформації має здійснюватися за чіткими процедурами, що забезпечують захист чутливої інформації.

Термін підготовки – протягом одного року.

– Ліквідація прогалин у забезпеченні захисту інформації в процесі обміну між суб'єктами системи завдяки врегулюванню процедур взаємодії органів державної влади та операторів критичної інфраструктури, зацікавленими сторонами приватного сектору (бізнесу).

Термін підготовки – протягом двох років.

Додаток
до Національного плану захисту критичної інфраструктури

1. Завдання суб'єктів державної системи забезпечення БСКІ

1.1. Завдання щодо запровадження системи забезпечення БСКІ

1.1.1. Органи державної влади, відповідальні за сектори критичної інфраструктури (Міненерговугілля, МОЗ, Мінінфраструктури тощо), виконують такі заходи:

- розроблення та затвердження секторальних вимог законодавства щодо забезпечення БСКІ (*протягом 2 років від дня прийняття Плану*);
- погодження Паспорта безпеки об'єктів КІ (*протягом місяця з дати подання оператором*);
- затвердження Планів операторів КІ щодо запобігання, реагування, відновлення КІ (*протягом 2 років із дня прийняття Плану*);
- організацію обміну інформацією у секторі, здійснення її аналізу та оцінка загроз та ризиків в рамках секторального ситуаційно-кризового центру (*протягом 1 року з дня прийняття Плану*);
- організацію взаємодії з іншими суб'єктами системи забезпечення БСКІ (*протягом 1 року з дня прийняття Плану*);
- розроблення проекту Секторальної проектної загрози (*протягом 1 року з дня прийняття Плану*);
- затвердження Плану взаємодії на випадок кризової ситуації (*протягом 1 року з дня прийняття Плану*);
- затвердження Плану відновлення функціонування секторальної КІ (*протягом 1 року з дня прийняття Плану)*;
- підготовку пропозицій до Реєстру об'єктів КІ (*протягом 4 місяців із дня прийняття Плану*);
- підготовку пропозицій до Національної оцінки ризиків критичній інфраструктури (*протягом 9 місяців із дня прийняття Плану*);

1.1.2. Органи державної влади, відповідальні за окремі функціональні аспекти забезпечення захисту та стійкості критичної інфраструктури (СБУ, ДСНС, СЗР, НБУ) виконують такі заходи:

- розробку та затвердження функціональних вимог законодавства щодо організації забезпечення БСКІ (*протягом 2 років із дня прийняття Плану*);
- погодження Паспорта безпеки об'єктів КІ (*протягом місяця із дати подання оператором*);
- погодження Планів операторів КІ щодо запобігання та реагування на загрози КІ (*протягом місяця із дати подання оператором*);

– оцінку загроз та ризиків КІ; сценарне прогнозування розвитку ситуації (*протягом 6 місяців із дня прийняття Плану*);
– формування пропозицій до Національної та секторальних проектних загроз (*протягом 3 місяців із дня прийняття Плану*);
– організацію взаємодії та обміну інформацією із іншими суб'єктами системи БСКІ (*протягом 1 року з дня прийняття Плану*);
– контроль за дотриманням вимог законодавства (*щорічно за встановленим графіком*);
– підготовку пропозицій до Реєстру об'єктів КІ (*протягом 4 місяців із дня прийняття Плану*);

1.1.3. Місцеві органи влади забезпечують:
– розробку місцевих програм забезпечення безпеки та стійкості критичної інфраструктури (*протягом 1 року з дня прийняття Плану*);
– розробку та погодження місцевих планів взаємодії залучених суб'єктів, планів відновлення функціонування критичної інфраструктури (*протягом 1 року з дня прийняття Плану*);
– розробку та впровадження місцевих програм підвищення стійкості громад до кризових ситуацій, викликаних припиненням або погіршенням надання важливих для їх життєдіяльності послуг, або доступу до ресурсів тощо (*протягом 2 років із дня прийняття Плану*);
– підготовку пропозицій до Реєстру об'єктів КІ (*протягом 4 місяців із дня прийняття Плану*);
– підготовку пропозицій до Національної оцінки ризиків критичній інфраструктури (*протягом 9 місяців із дня прийняття Плану*);

1.1.4. Оператори критичної інфраструктури забезпечують:
– розробку Паспорта безпеки об'єктів КІ (*протягом 1 року з дня прийняття Плану*);
– розробку планів запобігання, реагування, відновлення КІ (*протягом 2 років із дня прийняття Плану*);
– затвердження корпоративних вимог щодо організації захисту КІ відповідно до вимог законодавства (*протягом 1 року з дня прийняття Плану*);
– організацію обміну інформацією та взаємодію з іншими суб'єктами системи забезпечення БСКІ (*протягом 1 року з дня прийняття Плану*);
– підготовку пропозицій до Реєстру об'єктів КІ (*протягом 4 місяців із дня прийняття Плану*);

1.1.5. Урядовий центр безпеки і стійкості (УЦБС) здійснює такі заходи:
– розробку Методики оцінки загроз критичній інфраструктурі (*протягом 4 місяців із дня прийняття Плану*);

– затвердження Реєстру об'єктів КІ (*протягом 6 місяців із дня прийняття Плану*);
– розробку Національної оцінки ризиків критичній інфраструктурі (*протягом 9 місяців із дня прийняття Плану*);
– опублікування Оцінки ризиків критичній інфраструктурі (*протягом 1 року з дня прийняття Плану*);
– розробку проекту Національної проектної загрози КІ (*протягом 1 року з дня прийняття Плану*);
– підготовку та прийняття правового акта щодо порядку зміни режимів роботи функціонування критичної інфраструктури (*протягом 1 року з дня прийняття Плану*);
– затвердження секторальних проектних загроз (*протягом місяця з дати подання*);
– погодження секторальних планів взаємодії на випадок кризової ситуації (*протягом місяця з дати подання*);
– погодження секторальних планів відновлення функціонування КІ (*протягом місяця з дати подання*);
– контроль за дотриманням вимог законодавства (*відповідно до графіка*).

1.1.6. КМУ та РНБОУ забезпечують:
– затвердження процедури зміни режиму роботи критичної інфраструктури (відповідно до розподілу повноважень) (*протягом 6 місяців із дня прийняття Плану*);
– затвердження КМУ Національного плану захисту критичної інфраструктури (*протягом 6 місяців із дня прийняття Плану*);
– затвердження РНБОУ Національної Проектної загрози (*не пізніше 2 років із дня прийняття Плану*);
– координацію дій сектору безпеки і оборони (*постійно*).

1.2. Завдання в щодо зміни режимів функціонування системи забезпечення БСКІ

Виконавці	Завдання	Терміни
Загальносистемні завдання		
УЦБС	Підготовка та прийняття нормативно-правових актів у частині формалізації вимог щодо діяльності	Протягом 1 року
	Прийняття та доведення рішення щодо зміни режиму функціонування критичної інфраструктури	Протягом 2 год після прийняття інформації
Секторальні органи влади	Підготовка та прийняття нормативно-правових актів у частині формалізації вимог щодо діяльності	Протягом 1 року
Функціональні органи влади	Підготовка та прийняття нормативно-правових актів у частині формалізації вимог щодо діяльності	Протягом 1 року
Оператори	Підготовка та прийняття корпоративних рішень у частині формалізації вимог щодо діяльності	Протягом 1 року
Місцеві органи влади	Підготовка та прийняття нормативно-правових актів у частині формалізації вимог щодо діяльності	Протягом 1 року
КМУ та РНБОУ	Прийняття необхідних актів законодавства для формування нормативно-правової бази забезпечення захисту та стійкості критичної інфраструктури	Протягом 2 років
Штатний режим функціонування		
УЦБС, КМУ та РНБОУ	Забезпечення за встановленими процедурами обробки та обміну інформацією щодо:	За встановленим графіком
Секторальні органи влади, Функціональні органи влади	оцінки загроз КІ, можливих сценаріїв розвитку ситуації внаслідок реалізації загроз; готовності системи захисту КІ відповідно до вимог;	
Оператори	уточнення щодо Реєстру об'єктів КІ;	
Місцеві органи влади	доведення змін вимог законодавства щодо захисту КІ	

Виконавці	Завдання	Терміни
Урядовий кризовий центр	Доведення інформації щодо зміни режиму функціонування державної системи захисту критичної інфраструктури.	Протягом 30 хв після прийняття рішення
Секторальні органи влади	Приведення сил оператора КІ та секторальних сил і ресурсів до режиму готовності	Протягом 1 год після прийняття рішення
Режим запобігання виникненню кризової ситуації		
УЦБС	Забезпечення вчасного, ефективного і збалансованого інформування усіх суб'єктів реагування.	За встановленим графіком
	Забезпечення виваженого інформування населення, ЗМІ та експертів.	За встановленим графіком
	Доведення інформації щодо зміни режиму функціонування державної системи захисту критичної інфраструктури	Протягом 15 хв після прийняття рішення
Секторальні органи влади	Активація планів запобігання реалізації загроз будь-якого виду – приведення до максимальної готовності системи захисту та реагування до реалізації загроз.	Протягом 15 хв після прийняття рішення
	Оцінка можливих сценаріїв розвитку кризової ситуації.	Протягом 1 год після прийняття рішення
	Забезпечення вчасного, ефективного і збалансованого інформування усіх суб'єктів реагування	За встановленим графіком
Функціональні органи влади	Приведення сил сектору безпеки і оборони, визначених у планах захисту та реагування відповідних секторів критичної інфраструктури у режим «підвищеної готовності»	Протягом 1 год після прийняття рішення
Оператори	Реалізація планів запобігання реалізації загроз будь-якого виду. Створення команди для прийняття оперативних рішень. Забезпечення первинного реагування. Забезпечення вчасного, ефективного і збалансованого інформування усіх суб'єктів реагування	Відповідно до планів запобігання (не пізніше 1 год після прийняття рішення)

Виконавці	Завдання	Терміни
Місцеві органи влади	Активація місцевих програм забезпечення захисту та стійкості критичної інфраструктури; планів взаємодії відповідно до секторів критичної інфраструктури	Протягом 1 год після прийняття рішення
КМУ та РНБОУ	Повідомлення для ЗМІ та міжнародного співтовариства	Протягом 2 год після прийняття рішення
Режим кризової ситуації		
УЦБС	Розгортання повномасштабної системи управління кризовою ситуацією (Міжвідомчого оперативного кризового штабу). Забезпечення управління в режимі кризової ситуації. Збирання та передавання інформації для аналізу характеру та природи кризи, оцінки можливих сценаріїв її розвитку в рамках національної мережі обміну інформацією	Протягом 15 хв після прийняття рішення щодо запровадження кризового реагування За встановленими процедурами
Секторальні органи влади	Обмеження масштабу інциденту та стабілізація ситуації на місці подій. Попередня оцінка масштабів реалізації загроз, потреб у додаткових ресурсах (залучення додаткових сил та засобів сектору безпеки і оборони). Активація планів забезпечення стійкості та взаємодії функціонування критичної інфраструктури для надання життєво важливих функцій/послуг	Відповідно до планів запобігання (не пізніше 1 год після прийняття рішення) Протягом 2 год (за необхідності) після прийняття рішення щодо запровадження кризового реагування
Функціональні органи влади	Обмеження масштабу інциденту та стабілізація ситуації на місці подій відповідно до планів взаємодії із силами оператора та секторальних сил. Недопущення ескалації кризи та її використання у цілях, що загрожують національній безпеці держави. Забезпечення безпеки громадян та членів команд реагування	Відповідно до планів запобігання (не пізніше 1 год після прийняття рішення)

Виконавці	Завдання	Терміни
Оператори	Реалізація первинного реагування силами та засобами персоналу об'єкта критичної інфраструктури та зовнішніх сил, залучених відповідно до плану.	Протягом 15 хв після прийняття рішення щодо запровадження режиму кризового реагування
	Здійснення попередньої оцінки ситуації (характеру інциденту та рівня кризової ситуації) та прийняття рішення щодо активізації Плану взаємодії із іншими силами сектору безпеки і оборони.	Відповідно до планів запобігання (не пізніше 1 год після прийняття рішення)
	Активація планів (процедур) аварійного реагування, використання резервних можливостей для забезпечення надання життєво важливих функцій/послуг	Протягом 1 год (за необхідності)
Місцеві органи влади	Недопущення ескалації кризи та її використання у цілях, що загрожують національній безпеці держави. Забезпечення безпеки громадян та членів команд реагування. Запобігання виникненню і поширенню панічних настроїв в суспільстві	Відповідно до планів запобігання (не пізніше 1 год після прийняття рішення)
КМУ та РНБОУ	Забезпечення управління в режимі кризової ситуації. Недопущення ескалації кризи та її використання у цілях, що загрожують національній безпеці держави. Мобілізація всіх ресурсів для нейтралізації можливих загроз національній безпеці. Здійснення запиту (за необхідності) щодо допомоги від міжнародного співтовариства	Відповідно до планів запобігання (не пізніше 1 год після прийняття рішення)
Режим відновлення		
УЦБС	Оцінка можливості скасування режиму кризового реагування. Припиняється робота секторального Міжвідомчого оперативного штабу реагування на кризову ситуацію	Протягом 1 год після прийняття рішення

Виконавці	Завдання	Терміни
Секторальні органи влади	Оцінка можливості скасування режиму кризового реагування. Прийняття рішення про перехід до відновлення нормального функціонування пошкодженої критичної інфраструктури. Аналіз уроків, винесених з кризової (надзвичайної) ситуації, планування заходів з підвищення рівня безпеки	Відповідно до планів забезпечення стійкості (відновлення) КІ
Функціональні органи влади	Виконання заходів з пом'якшення та/або ліквідації довгострокових наслідків кризової ситуації, у т. ч. надання комплексної допомоги населенню. Передача основної координуючої ролі до Державної служби з надзвичайних ситуацій. Аналіз уроків, винесених із кризової (надзвичайної) ситуації, планування заходів з підвищення рівня безпеки	Протягом 1 год після прийняття рішення
Оператори	Активація планів відновлення функціонування об'єктів критичної інфраструктури	Відповідно до планів забезпечення стійкості (відновлення) КІ
Місцеві органи влади	Виконання заходів з пом'якшення та/або ліквідації довгострокових наслідків кризової ситуації, у т. ч. надання комплексної допомоги населенню. Активація місцевих програм відновлення надання життєво важливих функцій/послуг	Відповідно до місцевих планів
КМУ та РНБОУ	Прийняття рішення щодо скасування режиму кризового реагування (надзвичайного чи особливого стану). Здійснення запиту (за необхідності) щодо допомоги від міжнародного співтовариства	Відповідно до законодавства

Додаток 3

ПРОПОЗИЦІЇ ДО ПРОЕКТУ ЗАКОНУ УКРАЇНИ «ПРО КРИТИЧНУ ІНФРАСТРУКТУРУ»

ЗАКОН УКРАЇНИ

Про критичну інфраструктуру

Цей Закон визначає правові та організаційні засади діяльності із забезпечення захисту критичної інфраструктури, встановлює принципи та напрями розбудови державної системи захисту критичної інфраструктури і є складовою частиною законодавства України у сфері національної безпеки.

Розділ I
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів і понять

1. У цьому Законі терміни вживаються у такому значенні [243]:

1) критична інфраструктура – системи, мережі, об'єкти, ресурси (як фізичні, так і віртуальні чи інформаційні), які забезпечують реалізацію життєво важливих функцій та послуг і мають настільки велике значення, що їх знищення, пошкодження або виведення з ладу призведе до найсерйозніших негативних наслідків для життєдіяльності населення, суспільства, соціально-економічного розвитку країни, обороноздатності держави та забезпечення національної безпеки;

2) об'єкти критичної інфраструктури – окремі елементи критичної інфраструктури, визначені у встановленому законом порядку, щодо яких передбачається здійснення заходів із забезпечення їх захисту;

3) Реєстр критичної інфраструктури – перелік найбільш важливої для життєдіяльності суспільства та держави критичної інфраструктури, щодо якої встановлюються особливі вимоги забезпечення її безпеки та стійкості та здійснюється державний контроль за їх дотриманням;

4) захист критичної інфраструктури – усі види діяльності, спрямовані на: своєчасне виявлення, запобігання і нейтралізацію загроз об'єктам критичної інфраструктури; мінімізацію та ліквідацію наслідків у випадку реалізації загроз; швидке відновлення функціонування критичної інфраструктури;

[243] Розширений перелік термінів та їх визначень наведено у *Додатку 4*.

5) безпека критичної інфраструктури – стан критичної інфраструктури, коли дія зовнішніх та внутрішніх факторів (чинників) не призводить до порушення її функціонування;

6) стійкість критичної інфраструктури – спроможність надійно функціонувати у штатному режимі, адаптуватись до умов, що постійно змінюються, протистояти загрозам та швидко відновлюватись після реалізації загроз усіх типів, як за характером походження (природного, техногенного характеру, викликані протиправними діяннями (фізичні та кібератаки)), так і за спрямованістю (споруди, обладнання, ресурси, технологічні процеси, системи управління, персонал тощо);

7) життєво важливі послуги – послуги, які забезпечуються державними установами, підприємствами та організаціями будь-якої форми власності, збої та переривання у наданні яких призводять до швидких негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки;

8) життєво важливі функції – функції, які виконують державні органи, державні установи, підприємства та організації будь-якої форми власності, порушення яких призводить до швидких негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки;

9) сектор критичної інфраструктури – сукупність об'єктів критичної інфраструктури, які належать до однієї галузі економіки та/або мають спільну функціональну спрямованість;

10) оператор критичної інфраструктури – державний орган, підприємство, установа, організація, юридична та/або фізична особа, який/яке/яка на правах власності, оренди, господарського відання, оперативного управління або на інших законних підставах користується об'єктом критичної інфраструктури та відповідає за його поточне функціонування;

11) режими функціонування державної системи захисту критичної інфраструктури – умови та вимоги щодо функціонування критичної інфраструктури залежно від розвитку ситуації (штатний режим, режим запобігання виникненню кризової ситуації, режим кризової ситуації, режим відновлення).

2. Інші терміни вживаються у значеннях, наведених у Кодексі цивільного захисту України, Кримінальному кодексі України, Законах України «Про основи національної безпеки України», «Про боротьбу з тероризмом», «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання», «Про об'єкти підвищеної небезпеки», «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про державну таємницю», «Про оперативно-розшукову діяльність», «Про контррозвідувальну діяльність», «Про правовий режим надзвичайного стану», «Про правовий режим воєнного стану».

Стаття 2. Правова основа діяльності із захисту критичної інфраструктури

Правову основу діяльності із захисту критичної інфраструктури становлять Конституція України, міжнародні договори, що стосуються захисту критичної інфраструктури, згода на обов'язковість яких надана Верховною Радою України, цей Закон, інші закони України, акти Президента України, Кабінету Міністрів України, а також інші нормативно-правові акти, що прийняті на виконання цього Закону.

Стаття 3. Сфера застосування Закону

Закон врегульовує діяльність із захисту критичної інфраструктури у мирний час, під час кризової та надзвичайної ситуацій. Діяльність із захисту критичної інфраструктури в умовах надзвичайного та особливого періоду регулюється законами України.

Розділ ІІ
ОСНОВНІ ЗАСАДИ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стаття 4. Засади державної політики у сфері захисту критичної інфраструктури

1. Забезпечення захисту критичної інфраструктури є складовою частиною забезпечення національної безпеки України.

2. Державна політика у сфері захисту критичної інфраструктури ґрунтується на засадах:

визнання необхідності забезпечення безпеки та стійкості функціонування критичної інфраструктури;

визначення законодавчих вимог до захисту критичної інфраструктури;

створення умов, спрямованих на мінімізацію можливості реалізації загроз, ліквідацію та/або мінімізацію наслідків реалізованих загроз, швидкого відновлення функціонування критичної інфраструктури у випадку реалізованих загроз, надзвичайних/кризових ситуацій;

встановлення повноважень та відповідальності суб'єктів державної системи захисту критичної інфраструктури;

створення системи управління ризиками критичній інфраструктурі;

запровадження взаємодії держави, суб'єктів господарювання, експертного середовища та населення з питань забезпечення захисту та стійкості критичної інфраструктури;

забезпечення міжнародного співробітництва у сфері захисту критичної інфраструктури.

3. Державна політика у сфері захисту критичної інфраструктури спрямовується на формування комплексу організаційних, нормативно-правових, інженерно-технічних, експлуатаційних, наукових та інших заходів, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури.

Стаття 5. Основні принципи формування захисту критичної інфраструктури в Україні

До основних принципів формування захисту критичної інфраструктури належать принципи:

координованості;

єдності методологічних засад захисту критичної інфраструктури;

державно-приватної взаємодії;

забезпечення конфіденційності;

міжнародного співробітництва.

Стаття 6. Мета та завдання державної політики у сфері захисту критичної інфраструктури

1. Метою державної політики у сфері захисту критичної інфраструктури є забезпечення безперебійного та сталого функціонування критичної інфраструктури України, запобігання проявам актів неправомірного втручання у роботу об'єктів критичної інфраструктури, прогнозування та запобігання кризовим ситуаціям, а також підвищення рівня захисту, безпеки та стійкості цих об'єктів від існуючих загроз.

2. До завдань державної політики у сфері захисту критичної інфраструктури України належать:

забезпечення безпеки та стійкості критичної інфраструктури України;

попередження кризових та надзвичайних ситуацій, що порушують сталe функціонування критичної інфраструктури;

створення та організація державної системи захисту критичної інфраструктури;

розроблення нормативно-правової бази з питань захисту критичної інфраструктури;

встановлення обов'язкових вимог із забезпечення безпеки об'єктів критичної інфраструктури, їхньої захищеності на всіх етапах життєвого циклу, в тому числі під час створення, введення до експлуатації, модернізації;

запровадження державно-приватного партнерства у сфері захисту критичної інфраструктури;

розроблення та реалізація державних цільових програм із захисту критичної інфраструктури;

аналіз ризиків та загроз, які впливають на безпеку і стійкість критичної інфраструктури, її захищеності.

Стаття 7. Організаційні засади захисту критичної інфраструктури

Захист критичної інфраструктури включає в себе:

визначення секторів критичної інфраструктури, встановлення відповідальних суб'єктів захисту критичної інфраструктури за визначені сектори;

визначення компетенції і повноважень уповноваженого органу у справах захисту критичної інфраструктури України та інших суб'єктів державної системи захисту критичної інфраструктури;

категоризацію об'єктів критичної інфраструктури для визначення рівня вимог до забезпечення захисту критичної інфраструктури, повноважень та відповідальності суб'єктів;

складання та ведення секторальних переліків об'єктів критичної інфраструктури та загальнодержавного Реєстру критичної інфраструктури;

паспортизацію об'єктів критичної інфраструктури;

визначення режимів функціонування державної системи захисту критичної інфраструктури та розроблення планів реагування на кризові та надзвичайні ситуації;

взаємодію та обмін інформацією між суб'єктами державної системи захисту критичної інфраструктури та визначення рівня доступу до такої інформації третіх осіб;

здійснення контролю за рівнем безпеки об'єктів критичної інфраструктури та їх стійкості;

встановлення шляхів взаємодії між державними органами та приватним сектором в сфері захисту критичної інфраструктури;

запровадження критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури;

запровадження методології проведення оцінки загроз об'єктам критичної інфраструктури та реагування на них, зокрема щодо аварій і технічних збоїв, небезпечних природних явищ, зловмисних дій, тощо;

запровадження страхування ризиків у сфері захисту критичної інфраструктури;

реалізацію заходів, спрямованих на забезпечення захисту критичної інфраструктури від кіберзагроз, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем, захист технологічної інформації, що циркулює на об'єктах критичної інфраструктури.

Розділ ІІІ
КРИТИЧНА ІНФРАСТРУКТУРА УКРАЇНИ

Стаття 8. Об'єкти критичної інфраструктури

Об'єкти критичної інфраструктури визначаються та включаються до відповідних переліків об'єктів критичної інфраструктури в порядку, встановленому Кабінетом Міністрів України.

Віднесення об'єктів до критичної інфраструктури визначається за сукупністю критеріїв, що визначають їх важливість для реалізації життєво важливих функцій та надання життєво важливих послуг, а саме:

існування викликів і загроз, що можуть виникати щодо об'єктів критичної інфраструктури;

завдання значної шкоди нормальним умовам життєдіяльності населення;

уразливості цих об'єктів, тяжкості настання можливих негативних наслідків, внаслідок чого буде заподіяна значна шкода: здоров'ю населення (визначається кількістю постраждалих, загиблих та осіб, які отримали значні травми, а також чисельністю евакуйованого населення); соціальній сфері (руйнація систем соціального захисту населення і надання соціальних послуг, втрата спроможності держави задовольнити критичні потреби суспільства); економіці (вплив на ВВП, розмір економічних втрат, як прямих, так і непрямих); природним ресурсам загальнодержавного значення; обороноздатності; іміджу країни;

масштабності негативних наслідків для держави, які: вплинуть на діяльність стратегічно важливих об'єктів для кількох секторів життєзабезпечення чи призведуть до втрати унікальних національно значущих активів, систем і ресурсів, матимуть тривалі наслідки для держави і позначаться на діяльності низки інших секторів;

тривалості ліквідації таких наслідків та дією подальшого негативного впливу на інші сектори держави;

впливу на функціонування інших секторів критичної інфраструктури та спричинення виникнення каскадних ефектів.

Стаття 9. Категоризація об'єктів критичної інфраструктури

1. Для визначення рівня вимог до забезпечення захисту критичної інфраструктури, повноважень та відповідальності суб'єктів, у межах секторів здійснюється категоризація об'єктів критичної інфраструктури, на які поширюється сфера дії державної системи захисту критичної інфраструктури:

І категорія критичності – критично-важливі об'єкти, які мають загальнодержавне значення, розгалужені зв'язки та значний вплив на іншу інфраструктуру. Зазначені об'єкти включаються до переліку об'єктів критичної інфраструктури, формуються вимоги щодо забезпечення їх захисту;

ІІ категорія критичності – життєво важливі об'єкти, порушення функціонування яких призведе до кризової ситуації регіонального значення. Зазначені об'єкти включаються до переліку об'єктів критичної інфраструктури, формуються вимоги щодо розмежування завдань і повноважень органів державної влади та операторів критичної інфраструктури, спрямованих на забезпечення їх захисту та відновлення функціонування;

ІІІ категорія критичності – важливі об'єкти. Пріоритетом захисту такої інфраструктури є забезпечення швидкого відновлення функцій за рахунок диверсифікації та резервів. Відповідальність за стійкість функціонування об'єктів несуть оператори при встановлених законодавством вимогах щодо взаємодії із органами державної влади;

ІV категорія критичності – необхідні об'єкти. Об'єкти інфраструктури, безпосередній захист яких є відповідальністю оператора, який повинен мати план реагування на кризову ситуацію.

2. Категоризація об'єктів критичної інфраструктури в межах визначених секторів критичної інфраструктури здійснюється відповідальними за сектори суб'єктами державної системи захисту критичної інфраструктури відповідно до затвердженої Методики віднесення об'єктів інфраструктури до об'єктів критичної інфраструктури.

3. Суб'єкти державної системи захисту критичної інфраструктури, визначені відповідальними за сектори критичної інфраструктури, складають та ведуть переліки об'єктів інфраструктури І–ІV категорій.

4. До об'єктів інфраструктури І та ІІ категорії критичності встановлюються обов'язкові вимоги щодо організації захисту, безпеки та стійкості інфраструктури.

5. До об'єктів інфраструктури ІІІ та ІV категорії критичності встановлюються рекомендаційні вимоги щодо рівня організації захисту, безпеки та стійкості інфраструктури.

Стаття 10. Складання та ведення загальнодержавного Реєстру критичної інфраструктури

1. Для цілей узгодження дій суб'єктів державної системи захисту критичної інфраструктури з організації захисту найбільш важливої інфраструктури формується загальнодержавний Реєстр критичної інфраструктури.

2. Збирання, узагальнення, попередній аналіз даних щодо об'єктів критичної інфраструктури та пропозиції щодо внесення таких об'єктів до Реєстру критичної інфраструктури в межах визначених секторів здійснюється відповідальними за сектори суб'єктами державної системи захисту критичної інфраструктури.

3. Реєстр критичної інфраструктури формується та ведеться національним уповноваженим органом у сфері захисту критичної інфраструктури на

основі пропозицій суб'єктів державної системи захисту критичної інфраструктури.

4. Після внесення суб'єкта до Реєстру критичної інфраструктури відповідальний за сектор суб'єкт захисту критичної інфраструктури повідомляє про це оператора об'єкта критичної інфраструктури для організації робіт щодо паспортизації об'єкта критичної інфраструктури, планування забезпечення його захисту, безпеки та стійкості.

5. Реєстр критичної інфраструктури є автоматизованою інформаційно-довідковою системою, що забезпечує облік та обробку інформації щодо об'єктів критичної інфраструктури.

6. Порядок ведення Реєстру критичної інфраструктури та надання з нього інформації встановлюються Кабінетом Міністрів України за поданням національного уповноваженого органу у сфері захисту критичної інфраструктури.

Стаття 11. Паспортизація об'єктів критичної інфраструктури

1. Паспортизація об'єктів критичної інфраструктури є процедурою підготовки паспорта на окремий об'єкт критичної інфраструктури, де відображено комплекс заходів, що вживаються оператором з метою захисту та забезпечення стійкості функціонування об'єкта критичної інфраструктури.

2. Паспорт безпеки готується на кожний об'єкт критичної інфраструктури, включений до Реєстру критичної інфраструктури. Паспорт безпеки забезпезпечує проведення аналізу ризиків, основних можливих загроз та потенційних негативних наслідків для об'єктів критичної інфраструктури, запобіганню та попередженню виникненню загроз.

3. Паспорти безпеки готуються і затверджуються операторами критичної інфраструктури та погоджуються суб'єктами державної системи захисту критичної інфраструктури відповідно до порядку, встановленого законодавством.

4. Паспорт безпеки об'єкта критичної інфраструктури містить: інформацію щодо об'єкта критичної інфраструктури та його оператора, зв'язків та взаємовпливу об'єкта із іншою критичною інфраструктурою, стану організації захисту об'єкта, визначає перелік відповідальних осіб з питань захисту критичної інфраструктури, а також заходів із забезпечення безпеки і стійкості критичної інфраструктури.

5. Форма Паспорта безпеки, порядок його розробки, наповнення, зміст та строки подання встановлюються Кабінетом Міністрів України.

6. Оператор критичної інфраструктури несе відповідальність за достовірність даних, наведених у Паспорті безпеки, своєчасність внесення до нього змін.

Розділ IV
ДЕРЖАВНА СИСТЕМА ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стаття 12. Суб'єкти державної системи захисту критичної інфраструктури

Суб'єктами державної системи захисту критичної інфраструктури є:
Верховна Рада України;
Президент України;
Кабінет Міністрів України;
Рада національної безпеки і оборони України;
Урядовий центр безпеки і стійкості – уповноважений орган у справах захисту критичної інфраструктури України;
міністерства та інші центральні органи виконавчої влади;
місцеві державні адміністрації;
органи сектору безпеки і оборони України;
оператори критичної інфраструктури;
громадські організації, населення.

Стаття 13. Повноваження Верховної Ради України, Президента України, Кабінету Міністрів України, Ради національної безпеки і оборони України

У сфері забезпечення захисту критичної інфраструктури суб'єкти державної системи захисту критичної інфраструктури:

1. Верховна Рада України здійснює:

затвердження засад державної політики у сфері захисту критичної інфраструктури;

уточнення законодавства з питань забезпечення функціонування державної системи захисту критичної інфраструктури.

2. Президент України здійснює:

прийняття рішень щодо функціонування державної системи захисту критичної інфраструктури в період запровадження надзвичайної ситуації загальнодержавного рівня, надзвичайного та особливого стану;

загальну координацію дій суб'єктів державної системи захисту критичної інфраструктури.

3. Рада національної безпеки і оборони України забезпечує:

координацію діяльності суб'єктів державної системи захисту критичної інфраструктури та сил сектору безпеки і оборони;

затвердження Проектної загрози критичній інфраструктури на національному рівні;

затвердження загроз критичній інфраструктурі та проведення щорічної Національної оцінки ризиків;

4. Кабінет Міністрів України забезпечує:

формування та реалізацію державної політики у сфері захисту критичної інфраструктури;

визначення організаційних засад створення та функціонування державної системи захисту критичної інфраструктури;

затвердження Національного плану захисту критичної інфраструктури;

затвердження зміни режиму функціонування державної системи захисту критичної інфраструктури;

затвердження загальнодержавних цільових програм та планів у сфері захисту критичної інфраструктури.

Стаття 14. Національний уповноважений орган у сфері захисту критичної інфраструктури України

1. З метою формування й реалізації державної політики у сфері захисту критичної інфраструктури створюється та функціонує національний уповноважений орган у сфері захисту критичної інфраструктури України – Урядовий центр безпеки та стійкості.

2. Урядовий центр безпеки та стійкості:

забезпечує розроблення єдиної методологічної основи функціонування державної системи захисту критичної інфраструктури;

координує діяльність міністерств та інших центральних органів виконавчої влади з питань розробки нормативно-правового забезпечення у сфері захисту критичної інфраструктури та виконання планів захисту критичної інфраструктури загальнодержавного рівня (секторальні);

забезпечує функціонування системи обміну інформацією між суб'єктами державної системи захисту критичної інфраструктури;

взаємодіє з операторами критичної інфраструктури України з питань забезпечення захисту критичної інфраструктури;

формує та веде Реєстр критичної інфраструктури України;

здійснює оцінку захищеності об'єктів інфраструктури, внесених до Реєстру критичної інфраструктури України;

проводить із залученням суб'єктів державної системи захисту критичної інфраструктури оцінку загроз і ризиків критичній інфраструктурі на загальнодержавному рівні;

затверджує Методику оцінки загроз критичній інфраструктурі та проектні загрози критичній інфраструктурі секторального рівня;

погоджує секторальні нормативно-правові акти захисту критичної інфраструктури (плани запобігання, реагування, відновлення);

розробляє та подає на затвердження: Національний план захисту критичної інфраструктури; Національну проектну загрозу критичній інфраструктурі; перелік секторів критичної інфраструктури та суб'єктів державної системи захисту критичної інфраструктури, які є відповідальними за ці

сектори; порядок розробки, форму та зміст Паспорта безпеки об'єкта критичної інфраструктури; порядок розробки, форму та зміст планів захисту критичної інфраструктури загальнодержавного рівня (секторальні); порядок зміни режимів функціонування державної системи захисту критичної інфраструктури; типові вимоги щодо забезпечення захисту та стійкості об'єктів критичної інфраструктури відповідно до категорій критичності;

здійснює контроль за дотриманням вимог законодавства у сфері захисту критичної інфраструктури;

здійснює інші повноваження, передбачені цим Законом та Положенням про Урядовий центр безпеки і стійкості.

3. Положення про Урядовий центр безпеки та стійкості затверджується Кабінетом Міністрів України.

Стаття 15. Органи державної влади, які визначені відповідальними за функціонування окремих державних систем

З метою розподілення завдань із реалізації державної політики у сфері захисту критичної інфраструктури та організації захисту критичної інфраструктури визначається завдання органам державної влади, які визначені відповідальними за функціонування окремих державних систем захисту та реагування [244].

До переліку окремих державних систем захисту та реагування, із якими встановлюється система взаємодії та обміну інформацією, входять:

Єдина державна система цивільного захисту;

Державна система фізичного захисту ядерних утсановок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання;

Єдина державна система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків;

Національна система кібербезпеки;

органи сектору безпеки (спеціальні та правоохоронні органи);

органи сектору оборони (Збройні Сили України та система територіальної оборони).

Органи державної влади, які визначені відповідальними за функціонування окремих державних систем (функціональні органи):

беруть участь у встановленому законодавством порядку в реагуванні на кризові ситуації, пов'язані з безпекою, захистом та стійкістю критичної інфраструктури;

[244] До таких органів державної влади відносять перш за все: Службу безпеки України, Антитерористичний центр при Службі безпеки України, Державну службу спеціального зв'язку та захисту інформації, Національну гвардію, Національну поліцію, Державну службу з надзвичайних ситуацій, Державну прикордонну службу, Державну інспекцію ядерного регулювання України, Генеральний штаб Збройних Сил України.

готують пропозиції щодо включення об'єктів інфраструктури до Реєстру критичної інфраструктури;

формують перелік об'єктів критичної інфраструктури, що належать до сфери їх управління;

формують вимоги забезпечення захисту критичної інфраструктури у відповідних сферах;

надають секторальним органам влади, регуляторам, власникам та операторам інфраструктури консультації щодо загроз критичній інфраструктурі та заходів щодо їх нейтралізації;

здійснюють іншу діяльність для захисту критичної інфраструктури в межах повноважень, визначених законами, що регулюють діяльність суб'єктів захисту критичної інфраструктури, зокрема:

- розробку та затвердження функціональних вимог законодавства щодо забезпечення захисту критичної інфраструктури;
- забезпечення оцінки загроз та ризиків критичній інфраструктурі у відповідних сферах;
- участь у проведенні оцінки загроз та ризиків критичній інфраструктурі на загальнодержавному рівні;
- формування пропозицій до національної та секторальних проектних загроз;
- організацію взаємодії та обміну інформацією із іншими суб'єктами державної системи захисту критичної інфраструктури;
- контроль за дотриманням вимог законодавства у відповідних сферах;

у відповідних сферах забезпечують:

- погодження паспортів безпеки об'єктів критичної інфраструктури;
- погодження планів операторів щодо захисту критичної інфраструктури (запобігання, реагування, відновлення);
- організацію взаємодії та обміну інформацією з іншими суб'єктами державної системи захисту критичної інфраструктури відповідно до режимів функціонування державної системи захисту критичної інфраструктури.
- контроль за дотриманням вимог законодавства у своїй сфері.

Функціональні органи здійснюють діяльність у сфері захисту критичної інфраструктури через свої територіальні органи та/або підприємства, установи та організації, що належать до сфери їх управління.

Стаття 16. Органи державної виконавчої влади, які визначені відповідальними за забезпечення захисту відповідних секторів критичної інфраструктури

З метою розподілення завдань із реалізації державної політики у сфері захисту критичної інфраструктури та організації захисту критичної інфра-

структури між суб'єктами державної системи захисту критичної інфраструктури затверджується перелік секторів критичної інфраструктури та встановлюються суб'єкти державної системи захисту критичної інфраструктури, які є відповідальними за сектори.

Перелік секторів критичної інфраструктури та відповідальні за забезпечення захисту відповідних секторів критичної інфраструктури органів державної виконавчої влади затверджується Кабінетом Міністрів України.

Органи державної виконавчої влади, які визначені відповідальними за забезпечення захисту відповідних секторів критичної інфраструктури (секторальні органи), забезпечують:

збирання, узагальнення інформації та здійснення попереднього аналізу даних щодо функціонування критичної інфраструктури відповідного сектору та її вплив на функціонування суміжних секторів;

здійснення оцінки загроз критичній інфраструктурі та сценарний аналіз ризиків їх реалізації;

формування секторальних переліків критичної інфраструктури та внесення пропозицій щодо включення інфраструктурних об'єктів до Реєстру критичної інфраструктури;

організацію системи підготовки персоналу, навчання та тренувань щодо забезпечення захисту критичної енергетичної інфраструктури;

перевірку та оцінку захищеності об'єктів критичної інфраструктури;

підготовку щорічного звіту щодо забезпечення захисту критичної інфраструктури у відповідному секторі;

підготовку пропозицій до Проектної загрози критичній інфраструктурі на національному рівні та Національної оцінки ризиків критичній інфраструктури;

збирання, аналіз та узагальнення даних щодо об'єктів критичної інфраструктури та загроз їх функціонуванню;

організацію функціонування системи обміну інформацією та взаємодії у відповідних секторах критичної інфраструктури;

функціонування відповідних систем обміну інформацією, моніторингу безпекових умов на об'єктах критичної інфраструктури;

погодження паспортів безпеки об'єктів критичної інфраструктури, наданих операторами;

розроблення та затвердження вимог до забезпечення безпеки та стійкості об'єктів критичної інфраструктури відповідного сектору;

розроблення проектної загрози критичній інфраструктурі секторального рівня;

затвердження об'єктових проектних загроз операторів критичної інфраструктури відповідних секторів;

затвердження планів операторів критичної інфраструктури щодо запобігання, реагування та відновлення КІ;

розроблення та затвердження секторальних планів: захисту критичної енергетичної інфраструктури, планів запобігання реалізації загроз, відновлення критичної інфраструктури, взаємодії суб'єктів державної системи захисту критичної інфраструктури у відповідному секторі, відновлення функціонування секторальної критичної інфраструктури;

здійснення раннього оповіщення (попередження про загрози) операторів критичної інфраструктури та надання інформаційної, консультативної, експертної, технологічної допомоги операторам критичної інфраструктури, користувачам їх послуг (населенню) задля попередження, реагування, мінімізації можливого впливу загроз;

участь у встановленому законодавством порядку в реагуванні на надзвичайні ситуації, забезпеченні виконання завдань в умовах надзвичайного стану та особливий період;

секторальні органи здійснюють діяльність в сфері захисту критичної інфраструктури через свої управління, відділи, підрозділи, яким делеговані відповідні повноваження.

Перелік секторів критичної інфраструктури та органів виконавчої влади, визначених відповідальними за сектори критичної інфраструктури, затверджується Кабінетом Міністрів України [245].

Стаття 17. Місцеві органи виконавчої влади

Місцеві органи виконавчої влади у сфері захисту критичної інфраструктури забезпечують:

розробку місцевих програм забезпечення захисту та стійкості критичної інфраструктури, програм підвищення стійкості громад до кризових ситуацій, викликаних припиненням або погіршенням надання важливих для їх життєдіяльності послуг або доступу до життєво важливих ресурсів;

розробку та погодження із заінтересованими органами місцевих планів взаємодії залучених суб'єктів, планів відновлення функціонування критичної інфраструктури;

підготовку пропозицій до Реєстру критичної інфраструктури;

підготовку пропозицій до Національної оцінки ризиків критичній інфраструктури.

Стаття 18. Оператори критичної інфраструктури

1. Основними завданнями операторів критичної інфраструктури є:

забезпечення захисту об'єктів критичної інфраструктури;

розробка та оновлення об'єктових планів захисту критичної інфраструктури;

[245] Орієнтовний перелік секторів критичної інфраструктури та органів державної виконавчої влади, які визначені відповідальними за забезпечення захисту відповідних секторів, наведено у *Додатку 1.4*.

проведення оцінки ризиків на об'єктах критичної інфраструктури та обмін інформацією про ризики та загрози з іншими суб'єктам державної системи захисту критичної інфраструктури;

організація заходів з реагування на інциденти, кризові або надзвичайні ситуації, а також ліквідації їх наслідків на об'єктах критичної інфраструктури у взаємодії з іншими суб'єктами державної системи захисту критичної інфраструктури;

забезпечення постійного зв'язку з відповідальними за реагування суб'єктами державної системи захисту критичної інфраструктури;

забезпечення постійної взаємодії з підприємствами, які забезпечують підтримання життєво важливих функцій та надання життєво важливих послуг, від яких залежить процес реагування на кризові ситуації та відновлення функціонування об'єктів критичної інфраструктури;

створення необхідних резервів фінансових та матеріальних ресурсів для реагування на кризові ситуації та ліквідації їх наслідків;

захист інформації про системи управління, зв'язку, фізичну та кібернетичну безпеку, забезпечення відповідно до встановлених законодавством вимог конфіденційності інформації під час оброблення даних про об'єкти критичної інфраструктури.

2. Оператори забезпечують розробку та затвердження у встановленому законодавством порядку:

корпоративних вимог щодо організації захисту КІ;

посадових інструкцій осіб, відповідальних за організацію та забезпечення захисту об'єктів критичної інфраструктури;

порядку проведення навчань та тренінгів, підготовку та перевірку персоналу, який відповідає за охорону, безпеку та захист об'єктів критичної інфраструктури;

паспортів безпеки об'єктів критичної інфраструктури;

планів запобігання реалізації загроз, реагування на загрози, відновлення критичної інфраструктури тощо.

3. Оператори критичної інфраструктури мають право отримувати в установленому порядку від визначених суб'єктів державної системи захисту критичної інфраструктури інформацію, яка стосується забезпечення безпеки об'єктів критичної інфраструктури, що належать їм на праві власності або іншій законній підставі.

4. Оператори критичної інфраструктури зобов'язані:

забезпечити захист об'єктів критичної інфраструктури, що належать їм на праві власності або на іншій законній підставі;

виконувати у встановлені терміни запити (вимоги) щодо надання інформації про об'єкти критичної інфраструктури;

невідкладно інформувати відповідальних суб'єктів державної системи захисту критичної інфраструктури (секторальні та функціональні органи,

урядовий центр безпеки і стійкості) про інциденти, що сталися на об'єктах критичної інфраструктури, які належать їм на праві власності або іншій законній підставі;

забезпечити страхування об'єктів критичної інфраструктури відповідно до вимог цього Закону;

виконувати вимоги цього Закону та інших нормативно-правових актів, які регулюють діяльність об'єктів критичної інфраструктури.

Стаття 19. Здійснення контролю за рівнем безпеки об'єктів критичної інфраструктури та їх стійкості

Контроль за рівнем безпеки об'єктів критичної інфраструктури здійснюється шляхом оцінки захищеності об'єктів критичної інфраструктури.

Метою здійснення контролю є встановлення відповідності стану безпеки об'єкта критичної інфраструктури параметрам, задекларованим оператором об'єкта критичної інфраструктури у Паспорті безпеки на відповідний об'єкт, надання методичної допомоги операторам об'єктів критичної інфраструктури в удосконаленні системи захисту критичної інфраструктури.

Оцінка захищеності об'єктів критичної інфраструктури проводиться визначеними цим законом суб'єктами державної системи захисту об'єктів критичної інфраструктури.

Порядок проведення контролю визначається Кабінетом Міністрів України.

Стаття 20. Режими функціонування державної системи захисту критичної інфраструктури

Забезпечення захисту та стійкості критичної інфраструктури здійснюється в таких режимах її функціонування:

штатний режим – суб'єктами державної системи захисту критичної інфраструктури здійснюється оцінка можливих загроз та інформування щодо них;

режим готовності та запобігання реалізації загроз – суб'єктами державної системи захисту критичної інфраструктури здійснюється перевірка та переведення системи захисту до готовності забезпечити захист та реагування на випадок реалізації загрози;

режим реагування на виникнення кризової ситуації – суб'єктами державної системи захисту критичної інфраструктури застосовуються заходи реагування на кризову ситуацію. Функціонування інфраструктури здійснюється в режимі кризової або надзвичайної ситуації, вводяться обмеження на режими роботи об'єктів інфраструктури, економічні умови господарювання, доступу до об'єктів;

режим відновлення штатного функціонування – суб'єктами державної системи захисту критичної інфраструктури застосовуються заходи щодо повернення параметрів функціонування критичної інфраструктури до штатного режиму. Функціонування інфраструктури здійснюється з обмеженнями відповідно до визначених термінів ліквідації наслідків кризи.

Для кожного режиму функціонування державної системи захисту критичної інфраструктури відповідальними за сектори критичної інфраструктури розробляється план взаємодії з іншими суб'єктами державної системи захисту, який погоджується у встановленому законодавством порядку.

Рішення щодо зміни режимів функціонування державної системи захисту критичної інфраструктури приймається Кабінетом Міністрів України за поданням національного уповноваженого органу у сфері захисту критичної інфраструктури України.

Стаття 21. Державно-приватне партнерство у сфері захисту критичної інфраструктури

Державно-приватне партнерство у сфері захисту критичної інфраструктури здійснюється шляхом:

обміну інформацією між державними органами, приватним та громадським сектором і громадянами щодо загроз об'єктам критичної інфраструктури та кризових ситуацій на цих об'єктах;

підвищення комплексних знань, навичок і вмінь громадян з питань захисту критичної інфраструктури;

залучення експертного потенціалу, наукових установ, професійних об'єднань та громадських організацій до підготовки галузевих проектів та нормативних документів у сфері захисту критичної інфраструктури;

надання консультативної та практичної допомоги з питань реагування на кризові ситуації на об'єктах критичної інфраструктури;

запровадження механізму громадського контролю ефективності заходів із захисту критичної інфраструктури;

створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань захисту критичної інфраструктури;

організації забезпечення захисту персоналу від можливих загроз;

забезпечення резервування основних ресурсів для функціонування об'єкта критичної інфраструктури у різних режимах;

оповіщення місцевого населення про інциденти та кризові ситуації на об'єктах критичної інфраструктури.

Державно-приватна взаємодія у сфері захисту критичної інфраструктури застосовується з урахуванням встановлених законодавством особливостей правового режиму щодо окремих об'єктів та окремих видів діяльності.

Стаття 22. Національна мережа ситуаційно-кризових центрів у сфері захисту критичної інфраструктури

Для створення системи інформаційно-аналітичної підтримки процесу прийняття рішень щодо забезпечення захисту та стійкості критичної інфраструктури створюється та функціонує національна мережа ситуаційно-кризових центрів.

До мережі входять ситуаційно-кризові (інформаційно-аналітичні, диспетчерські) центри операторів об'єктів критичної інфраструктури, ситуаційно-кризові центри органів державної влади, відповідальних за реалізацію державної політики у сфері захисту критичної інфраструктури у відповідних секторах, ситуаційно-кризові центри сектору безпеки і оборони, ситуаційно-кризовий центр Кабінету Міністрів України та Головний ситуаційний центр Ради національної безпеки і оборони України.

Для забезпечення обміну інформацією та взаємодії суб'єктів державної системи захисту критичної інфраструктури Кабінет Міністрів України затверджує Регламент обміну інформацією.

Стаття 23. Страхування ризиків у сфері критичної інфраструктури

Страхування ризиків у сфері критичної інфраструктури здійснюється відповідно до вимог Закону України «Про страхування».

Страхування ризиків у сфері критичної інфраструктури здійснюється шляхом:

запровадження страхування об'єктів критичної інфраструктури від пошкодження внаслідок впливу стихійних лих або техногенних катастроф та від протиправних дій третіх осіб;

запровадження цивільної відповідальності операторів критичної інфраструктури за шкоду, яку може бути заподіяно припиненням функціонування та/або аваріями на об'єктах критичної інфраструктури, зумовленими невиконанням операторами критичної інфраструктури вимог законодавства у сфері захисту критичної інфраструктури.

страхування об'єктів критичної інфраструктури здійснюється у встановленому Кабінетом Міністрів України порядку. Страхування є обов'язковим стосовно об'єктів критичної інфраструктури, включених до Реєстру критичної інфраструктури.

Для створення умов та координації діяльності, пов'язаної із забезпеченням страхування у сфері критичної інфраструктури, забезпечення фінансової надійності страхування створюється страховий фонд безпеки критичної інфраструктури (Страховий пул безпеки інфраструктури).

Порядок проведення розслідувань припинення функціонування та/або аварій на об'єктах критичної інфраструктури встановлюється Кабінетом Міністрів України відповідно до вимог цього та інших законів.

Оцінка ризиків безпеки критичної інфраструктури здійснюється на основі задекларованої оператором критичної інфраструктури інформації щодо стану організації захисту критичної інфраструктури. Декларування інформації здійснюється шляхом підготовки та затвердження Паспорта безпеки об'єкта критичної інфраструктури. Порядок отримання інформації, відображеної у Паспорті безпеки об'єкта критичної інфраструктури, для забезпечення страхування у сфері критичної інфраструктури встановлюється Кабінетом Міністрів України відповідно до вимог цього та інших законів.

Стаття 24. Фінансування заходів у сфері захисту критичної інфраструктури

Джерелами здійснення заходів із захисту критичної інфраструктури та завдань, визначених цим Законом, є кошти державного і місцевих бюджетів, власні кошти суб'єктів господарювання, кредитні та інвестиційні ресурси, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством.

Для фінансування заходів за окремими напрями створюються цільові механізми, а саме:

– для формування власних цільових видатків ресурсів операторів критичної інфраструктури – включення до тарифів (цін) на послуги (продукцію) 50 відсотків видатків суб'єктів господарювання, здійснених на виконання вимог, визначених Законом;

– для заходів, включених до секторальних планів захисту критичної інфраструктури, – включення до валових витрат 50 відсотків видатків суб'єктів господарювання на реалізацію заходів;

– для створення мінімальних запасів ресурсів (обладнання) – залучення приватних ресурсів у рамках державно-приватного партнерства;

– для створення ринкового механізму інвестування у заходи безпеки – створення механізму страхування ризиків у сфері захисту критичної інфраструктури.

Виключний перелік заходів секторальних планів забезпечення захисту критичної інфраструктури та вимог Закону, щодо яких застосовуються вищезазначені механізми фінансування, затверджуються Кабінетом Міністрів України.

Стаття 25. Міжнародне співробітництво у сфері захисту критичної інфраструктури

1. Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері захисту критичної інфраструктури з іноземними державами, їх правоохоронними органами і спеціальними службами, а також із міжнародними організаціями, які здійснюють боротьбу з міжнародною злочинністю та тероризмом.

2. Відповідно до законодавства України у сфері зовнішніх відносин суб'єкти державної системи захисту критичної інфраструктури у межах своїх повноважень можуть здійснювати міжнародну співпрацю безпосередньо на двосторонній або багатосторонній основі.

Розділ V
ПРИКІНЦЕВІ ПОЛОЖЕННЯ

1. Цей Закон набирає чинності з дня його опублікування.

2. Кабінету Міністрів України протягом шести місяців у строк від дня набрання чинності цим Законом:

подати на розгляд Верховної Ради України пропозиції щодо приведення законів України у відповідність із цим Законом;

привести свої нормативно-правові акти у відповідність із цим Законом;

забезпечити перегляд і скасування міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів, що суперечать цьому Закону.

3. Внести зміни до таких законодавчих актів України:

пункт п'ятий частини першої статті 20 Закону України «Про Кабінет Міністрів України» після абзацу сьомого доповнити абзацом такого змісту: «забезпечує формування та реалізацію державної політики у сфері захисту критичної інфраструктури України»;

статтю 7 Закону України «Про страхування» доповнити пунктами 48 та 49 такого змісту:

«48) страхування цивільної відповідальності операторів критичної інфраструктури за шкоду, яку може бути заподіяно припиненням функціонування та/або аваріями на об'єктах критичної інфраструктури, зумовленими невиконанням операторами критичної інфраструктури вимог законодавства у сфері захисту критичної інфраструктури;

49) страхування об'єктів критичної інфраструктури від пошкодження внаслідок впливу стихійних лих або техногенних катастроф та від протиправних дій третіх осіб.»

Додаток 4

ГЛОСАРІЙ

Критична інфраструктура – системи, мережі, об'єкти, ресурси (як фізичні, так і віртуальні чи інформаційні), які забезпечують реалізацію життєво важливих функцій та послуг і мають настільки велике значення, що їх знищення, пошкодження або виведення з ладу призведе до найсерйозніших негативних наслідків для життєдіяльності населення, суспільства, соціально-економічного розвитку країни, обороноздатності держави та забезпечення національної безпеки;

об'єкти критичної інфраструктури – окремі елементи критичної інфраструктури, щодо яких у встановленому законом порядку здійснюються заходи із забезпечення їхнього захисту;

Реєстр критичної інфраструктури – перелік найбільш важливої для життєдіяльності суспільства та держави критичної інфраструктури, щодо якої встановлюються особливі вимоги із забезпечення її безпеки та стійкості та здійснюється державний контроль за їх дотриманням;

захист критичної інфраструктури – усі види діяльності, спрямовані на: своєчасне виявлення, запобігання і нейтралізацію загроз об'єктам критичної інфраструктури; мінімізацію та ліквідацію наслідків у випадку реалізації загроз; швидке відновлення функціонування критичної інфраструктури;

безпека критичної інфраструктури – стан критичної інфраструктури, коли дія зовнішніх та внутрішніх факторів (чинників) не призводить до порушення її функціонування;

стійкість критичної інфраструктури – спроможність надійно функціонувати у штатному режимі, адаптуватись до умов, що постійно змінюються, протистояти загрозам та швидко відновлюватись після реалізації загроз усіх типів, як за характером походження (природного, техногенного характеру, викликані протиправними діяннями (фізичні та кібератаки)), так і за спрямованістю (споруди, обладнання, ресурси, технологічні процеси, системи управління, персонал та ін.);

акт несанкціонованого втручання – протиправні діяння щодо критичної інфраструктури, що створили загрозу безпеці критичної інфраструктури (як у фізичному, так і кіберпросторі);

державна система захисту критичної інфраструктури – сукупність державних органів управління, сил та засобів центральних і місцевих органів виконавчої влади, органів місцевого самоврядування, операторів та/або власників об'єктів критичної інфраструктури (усіх форм власності), неурядових організацій (суб'єктів), які діють на основі відповідних норма-

тивно-правових документів, координуючи свою діяльність, а також співпрацюючи та обмінюючись інформацією з метою забезпечення безпеки та стійкості критичної інфраструктури щодо всіх фізичних загроз і кіберзагроз;

режими функціонування державної системи захисту критичної інфраструктури – умови та вимоги щодо функціонування критичної інфраструктури залежно від ситуації (штатний режим, режим запобігання виникненню кризової ситуації, режим кризової ситуації, режим відновлення);

життєво важливі послуги – послуги, які забезпечуються державними установами, підприємствами та організаціями будь-якої форми власності, збої та переривання у наданні яких призводять до швидких негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки;

життєво важливі функції – функції, які виконують державні органи, державні установи, підприємства та організації будь-якої форми власності, порушення яких призводить до швидких негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки;

загроза – наявні та потенційно можливі явища та чинники (події, інциденти тощо), що можуть призвести до негативних наслідків для населення, суспільства, соціально-економічного стану та національної безпеки;

загроза критичній інфраструктурі – наявні та потенційно можливі явища та чинники (події, інциденти тощо), що можуть призвести до порушення функціонування критичної інфраструктури;

категорія критичності об'єкта інфраструктури – відносна міра важливості об'єкта критичної інфраструктури, класифікована залежно від ступеня його впливу на реалізацію життєво важливих функцій та надання життєво важливих послуг;

категоризація об'єктів інфраструктури – віднесення об'єктів інфраструктури до категорій критичності;

кризова ситуація – ситуація, що склалася на елементі інфраструктури або у взаємопов'язаних сферах внаслідок настання події, яка призвела до порушення функціонування критичної інфраструктури, для реагування на яку та/або відновлення до штатного режиму необхідне залучення зовнішніх сил і ресурсів;

оператор критичної інфраструктури – державний орган, підприємство, установа, організація, юридична та/або фізична особа, який/яке/яка на правах власності, оренди, господарського відання, оперативного управління або на інших законних підставах користується об'єктом критичної інфраструктури та відповідає за його поточне функціонування;

паспорт безпеки – документ визначеної форми, який містить структуровані дані про об'єкт критичної інфраструктури та визначає комплекс за-

ходів, що вживаються оператором з метою захисту цього об'єкта від усіх видів загроз (відомості, що містяться в паспорті безпеки, можуть бути віднесені до відомостей, що становлять службову інформацію, державну або комерційну таємницю);

паспортизація об'єктів критичної інфраструктури – процедура підготовки, узгодження, затвердження та надання паспорта безпеки об'єкту критичної інфраструктури;

сектор критичної інфраструктури – сукупність об'єктів критичної інфраструктури, які належать до однієї галузі економіки та/або мають спільну функціональну спрямованість;

суб'єкти державної системи захисту критичної інфраструктури – державні органи, органи місцевого самоврядування, Збройні Сили України та інші військові формування, утворені відповідно до законів України; правоохоронні органи, а також підприємства, установи та організації незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням захисту критичної інфраструктури;

взаємодія – узгоджені за метою, завданням, місцем, часом та способом виконання завдань дії суб'єктів для досягнення мети;

відновлення – усунення наслідків загрози, повернення системи в робочий стан, включно із заходами зі зменшення факторів ризику;

вплив – імовірні (прогнозовані) наслідки реалізації загрози;

вразливість – нездатність критичної інфраструктури протистояти реалізації визначеної загрози чи сукупності загроз;

неперервність функціонування критичної інфраструктури – здатність критичної інфраструктури планувати свою роботу у разі інциденту та порушення її діяльності, забезпечуючи неперервність надання життєво важливих функцій та послуг на прийнятному рівні;

проектна загроза критичній інфраструктурі – перелік реальних та потенційних загроз критичній інфраструктурі (небезпечних чинників, подій, інцидентів, інших джерел ризику), що впливають на її безпечне функціонування та на захист від яких має бути розрахована державна система захисту критичної інфраструктури;

фізична безпека (захищеність) критичної інфраструктури – стан критичної інфраструктури, за якого забезпечується її спроможність протистояти загрозам, що зумовлені актами несанкціонованого втручання щодо критичної інфраструктури (включаючи кібератаки);

чутлива інформація – інформація, яку потрібно захищати від публічного розкриття, оскільки це може викликати негативний вплив на організацію, національну та громадську безпеку;

шкода – фізичне ушкодження і (або) збитки, заподіяні здоров'ю людей і (або) майну чи навколишньому середовищу.

ВІДОМОСТІ ПРО АВТОРІВ

Бобро Дмитро Геннадійович

Закінчив Київський політехнічний інститут за спеціальністю «Радіотехніка» (1982), Київський національний університет імені Тараса Шевченка за спеціальністю «Ядро, елементарні частинки й фізика високих енергій» (2001), кандидат фізико-математичних наук (2004). У Національному інституті стратегічних досліджень працює з 2014 р. на посаді провідного наукового співробітника відділу енергетичної та техногенної безпеки (донині).

Автор понад 50 публікацій у спеціалізованих та наукових виданнях, співавтор однієї монографії.

Іванюта Сергій Петрович

Випускник Національного технічного університету України «КПІ» за спеціальністю «Екологія та охорона навколишнього середовища» (1999), кандидат технічних наук (2007), старший науковий співробітник (2010), доктор технічних наук (2017). У Національному інституті стратегічних досліджень працює з 2011 р. на посадах старшого консультанта відділу екологічної та техногенної безпеки, головного консультанта відділу енергетичної та техногенної безпеки, заступника завідувача відділу енергетичної та техногенної безпеки (донині).

Автор понад 60 наукових публікацій та співавтор двох монографій.

Кондратов Сергій Іванович

Випускник Київського державного університету ім. Т. Г. Шевченка за спеціальністю «Радіофізика та електроніка» (1973). У Національному інституті стратегічних досліджень працює з 2010 р. на посадах наукового співробітника, старшого наукового співробітника відділу екологічної та техногенної безпеки, старшого наукового співробітника відділу енергетичної та техногенної безпеки (донині).

Автор понад 50 публікацій у спеціалізованих та наукових журналах, співавтор навчального посібника.

Суходоля Олександр Михайлович

Закінчив Національний технічний університет України «КПІ» за спеціальністю «Електропривод та автоматизація промислових установок» (1994), кандидат технічних наук (1998), доктор наук з державного управління (2007), професор (2015). У Національному інституті стратегічних досліджень працює з 2012 р. на посадах заступника завідувача відділу енергетичної і ядерної безпеки, завідувача відділу енергетичної і ядерної безпеки, завідувача відділу енергетичної та техногенної безпеки (донині).

Автор понад 150 наукових публікацій, автор і співавтор 8 монографій.

Наукове видання

Дмитро Геннадійович БОБРО
Сергій Петрович ІВАНЮТА
Сергій Іванович КОНДРАТОВ
Олександр Михайлович СУХОДОЛЯ

ОРГАНІЗАЦІЙНІ ТА ПРАВОВІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ І СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Аналітична доповідь

За загальною редакцією *О. М. Суходолі*

Редактор *Т. В. Карбовнича*

Відповідальний за випуск *А. Іщенко*

Формат 60х84/16. Ум. друк. арк. 13,72.
Наклад 200 пр. Зам. № ДФ __

Оригінал-макет підготовлено
в Національному інституті стратегічних досліджень,
вул. Пирогова, 7А, Київ, 01030.
Тел./факс: (044) 234-50-07.
e-mail: info-niss@niss.gov.ua
http://www.niss.gov.ua

ПП «Видавництво Фенікс»
Свідоцтво суб'єкта видавничої справи
ДК № 271 від 07.12.2000 р.
вул. Шутова, 13Б, Київ, 03067.
www.fenixprint.com.ua