ЩОДО РОЗРОБКИ ТА ЗАТВЕРДЖЕННЯ «НАЦІОНАЛЬНОГО ПЛАНУ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ»

Резюме

Розглянуто актуальність та визначено пріоритетні кроки щодо активізації процесу створення державної системи захисту критичної інфраструктури України. Зокрема відзначено стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури». Наголошено на необхідності створення державної системи захисту критичної інфраструктури на основі узгодження пріоритетів та координації діяльності існуючих в Україні державних систем захисту та реагування. Зроблено висновок про необхідність розробки інструменту формалізації функціонування державної системи захисту критичної інфраструктури на національному рівні. Запропоновано використання **Національного плану захисту критичної інфраструктури** у якості такого інструменту формалізації.

З метою розроблення пропозицій щодо змісту та структури Національного плану захисту критичної інфраструктури представлено модель функціонування державної системи захисту критичної інфраструктури, організації взаємодії та координації зусиль різних суб'єктів, долучених до питань захисту критичної інфраструктури. **Запропоновано проект Національного плану захисту критичної інфраструктури України**. У рамках зазначеного проекту Національного плану запропоновано механізми та інструменти формалізації завдань, визначено послідовність дій та механізм координації всіх залучених суб'єктів в різних режимах функціонування критичної інфраструктури.

Внесено пропозиції щодо подальшого розвитку державної системи захисту критичної інфраструктури.

ЩОДО РОЗРОБКИ ТА ЗАТВЕРДЖЕННЯ «НАЦІОНАЛЬНОГО ПЛАНУ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ»

У багатьох країнах світу захист ***критичної інфраструктури*** (далі - КІ) визнано пріоритетним напрямом у сфері національної безпеки. Відповідно, цими країнами активно розбудовуються національні системи для забезпечення захисту (безпеки) та стійкості критичної інфраструктури (КІ), приймається законодавство для регламентації діяльності учасників системи, проводиться підготовка кадрів, налагоджуються партнерські стосунки з приватним сектором, здійснюються освітні заходи серед населення тощо.

Розглянувши стан реалізації пріоритетних напрямів державної політики національної безпеки України щодо забезпечення безпеки критичної інфраструктури, Рада національної безпеки і оборони України у 2016 році вирішила вдосконалити правову основу ***захисту критичної інфраструктури*** (далі - ЗКІ) та створити систему державного управління її безпекою.[1]

На виконання зазначеного рішення Кабінет Міністрів України, за участю Національного інституту стратегічних досліджень, розробив та схвалив Концепцію створення державної системи захисту критичної інфраструктури.[2]

Прийнята Концепція зазначає, що створення державної системи ЗКІ (як комплексу заходів, спрямованих на забезпечення безпеки та стійкості КІ) потребує нормативно-правового врегулювання основоположних принципів її функціонування, запровадження єдиних підходів до організації управління об’єктами на різних рівнях різних галузей національної економіки та

---

[1] Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури». [Електронний ресурс].– Режим доступу: http://zakon.rada.gov.ua/laws/show/8/2017#n2

[2] Про схвалення Концепції створення державної системи захисту критичної інфраструктури. Розпорядження Кабінету Міністрів України від 6 грудня 2017 року №1009-р. – [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/1009-2017-%D1%80

визначення засад взаємодії залучених до ЗКІ державних органів та суб'єктів господарювання, суспільства та громадян.

Відповідно до Концепції, у якості інструменту формалізації функціонування державної системи ЗКІ на національному рівні має бути розроблено **Національний план захисту критичної інфраструктури.**

На наше переконання, подібний національний план має зафіксувати завдання, послідовність дій та механізм координації всіх залучених суб'єктів в різних режимах функціонування державної системи ЗКІ. Даного підходу дотримуються країни, які уже створили подібні національні системи. Зокрема структура та зміст Національних планів ЗКІ США,[3] Канади,[4] Австралії,[5] Великобританії,[6] Німеччини,[7] Польщі[8] підтверджують дану тезу та можуть бути використанні при розробці Національного плану захисту критичної інфраструктури України.

Та перш ніж говорити про підготовку Національного плану та створення правової бази функціонування державної системи ЗКІ необхідно, хоча б у загальних рисах, викласти бачення щодо моделі функціонування державної системи ЗКІ.

Пропонована нами модель функціонування державної системи ЗКІ та організації взаємодії різних її суб'єктів, ***яка наведена рисунку 1***, неодноразово обговорювалась на круглих столах та конференціях,

---

[3] National Infrastructure Protection Plan, 2013. Partnering for Critical Infrastructure Security and Resilience. – [Електронний ресурс]. – Режим доступу: https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

[4] 2018-2020 Action Plan for Critical Infrastructure of Canada. – [Електронний ресурс]. – Режим доступу: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2018-20/pln-crtcl-nfrstrctr-2018-20-en.pdf

[5] Critical Infrastructure Resilience Strategy of Australia: . – [Електронний ресурс]. – Режим доступу: https://www.tisn.gov.au/Documents/Australian+Government+s+Critical+Infrastructure+Resilience+Strategy.pdf

[6] Public Summary of Sector Security and Resilience Plans 2017. UK. – [Електронний ресурс]. – Режим доступу: 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

[7] National Strategy for Critical Infrastructure Protection (CIP Strategy) of Germany. – [Електронний ресурс]. – Режим доступу: https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v=1

[8] The National Critical Infrastructure Protection Programme 2015. Poland. – [Електронний ресурс]. – Режим доступу: http://rcb.gov.pl/wp-content/uploads/NPOIK-2015_eng-1.pdf

організованих Національним інститутом стратегічних досліджень, а окремі її аспекти детально висвітлені в ряді публікацій фахівців Інституту.[9]

При цьому, неодноразово наголошувалось, що створення державної системи ЗКІ не має на меті ліквідацію існуючих державних систем захисту чи реагування на надзвичайні (кризові) ситуації або їх підпорядкування пропонованій системі. Державна система ЗКІ має будуватись виходячи з позиції налагодження взаємодії та координації зусиль існуючих систем та залучених до їх функціонування суб'єктів для досягнення синергетичного ефекту.

Пропонована модель, з метою оптимізації суспільних витрат на функціонування системи державного управління, враховує спроможності, ресурси та сили існуючих державних систем захисту і реагування, зокрема наступних систем:

- Єдина державна система цивільного захисту[10];
- Єдина система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків[11];
- Державна система фізичного захисту [12] (мається на увазі державна система фізичного захисту ядерних установок, ядерних матеріалів);
- Національна система кібербезпеки, що створюється в рамках реалізації Стратегії кібербезпеки України;[13]
- Інші системи.

---

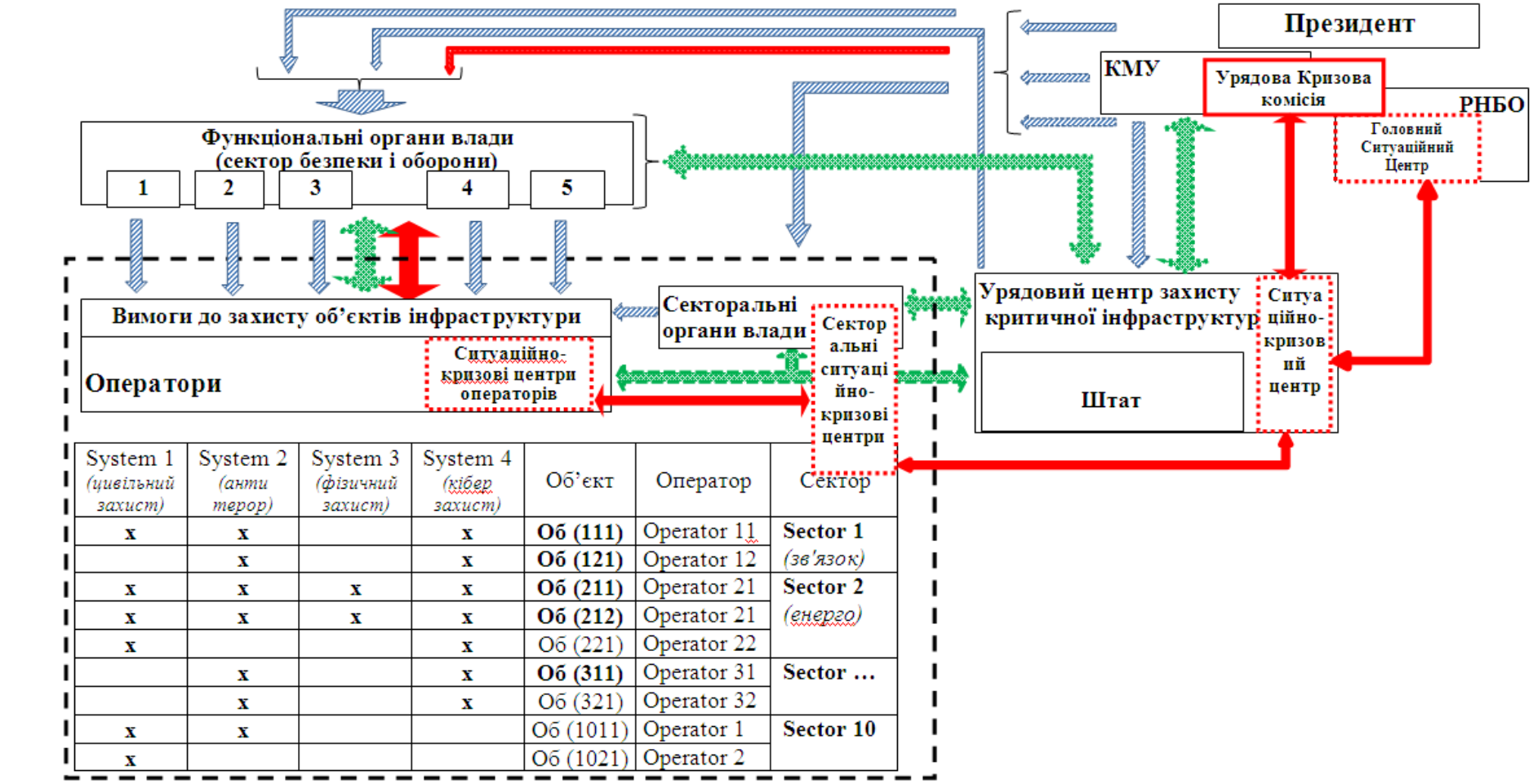
[9] Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С. І. Кондратов; за заг.ред. О.М.Суходолі. – К. : НІСД, 2016. – 176 с. – [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/2213/

[10] Постанова Кабінету Міністрів України від 09.01.2014 р. № 11 Про затвердження Положення про єдину державну систему цивільного захисту. [Електронний ресурс].– Режим доступу: http://zakon.rada.gov.ua/laws/show/11-2014-%D0%BF

[11] Постанова Кабінету Міністрів України від 18.02.2016 № 92 «Про затвердження Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків». [Електронний ресурс].– Режим доступу: http://zakon.rada.gov.ua/laws/show/92-2016-%D0%BF

[12] Постанова Кабінету Міністрів України від 21.12.2011 № 1337 «Про затвердження Порядку функціонування державної системи фізичного захисту». [Електронний ресурс].– Режим доступу: http://zakon.rada.gov.ua/laws/show/1337-2011-%D0%BF

[13] Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс].– Режим доступу: http://zakon.rada.gov.ua/laws/show/96/2016



System 1 *(цивільний 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	

Пояснення:
Об (і) - об'єкти інфраструктури, управління якими здійснюють оператори у відповідних секторах економіки, діяльність яких регулюється в рамках існуючих державних систем захисту і реагування (відображено значком **x);** виділенні жирним шрифтом – внесені до переліку об'єктів КІ.

Стрілка, заштрихована з нахилом вправо (синя) – основний напрям доведення законодавчих та організаційних вимоги до захисту КІ.

Стрілка, заштрихована хрестиком (зелена) – основні напрями обміну інформацією та взаємодії у нормальному режимі.

Стрілка суцільна (червона) – основні напрями інформаційних повідомлень в кризовому режимі.

Рисунок 1. Модель функціонування державної системи ЗКІ

Функціонування існуючих систем захисту і реагування координуються окремими органами державної влади, які у подальшому у моделі державної системи ЗКІ будуть визначатися як «**Функціональні органи**».[14]

Поряд із «функціональними органами» модель виділяє «**Секторальні органи**», які відображають органи влади (переважно центральні органи виконавчої влади), у компетенції яких знаходиться завдання формування та реалізації державної політики ЗКІ у відповідних галузях економіки та сферах життєдіяльності суспільства.[15]

Загалом слід зазначити, що перелік секторів КІ та відповідальних за сектори органи державної влади має бути окремо визначено та затверджено відповідним правовим актом. Пропонується, щоб зазначені переліки затверджувались Постановою Кабінету Міністрів України.

В рамках пропонованої моделі функціонування державної системи ЗКІ відповідні суб'єкти державної системи мають забезпечувати виконання наступних функціональних завдань:

1. **Кабінет Міністрів України** – формування та реалізації державної політики забезпечення ЗКІ, створення необхідної організаційної, інституційної та нормативно-правової основи діяльності суб'єктів державної системи.

2. **Рада національної безпеки і оборони України** – координація дій сектору безпеки і оборони та контроль за дотриманням вимог законодавства у сфері захисту КІ; затвердження Проектної загрози КІ на національному рівні, забезпечення проведення **Національної оцінки ризиків**.

3. **Урядовий центр безпеки і стійкості (УЦБС) - Національний уповноважений орган у сфері захисту критичної інфраструктури** – забезпечує функціонування державної системи ЗКІ: взаємодію відповідних

[14] До таких органів державної влади можна віднести: Служба безпеки України, Антитерористичний центр при Службі безпеці України, Національна поліція, Державна служба з надзвичайних ситуацій, Державна прикордонна служба, Державна служба спеціального зв'язку та захисту інформації, Державна інспекція ядерного регулювання України, Генеральний штаб Збройних сил України.

[15] До таких органів державної влади можна віднести: Міністерство інфраструктури України, Міністерство енергетики та вугільної промисловості України, Міністерство охорони здоров'я України, Міністерство аграрної політики та продовольства України, Міністерство регіонального розвитку, будівництва та житлово-комунального господарства України, Державна служба з надзвичайних ситуацій, Міністерство внутрішніх справ України, Міністерство оборони України, Національний банк України.

існуючих державних систем з питань забезпечення ЗКІ; розроблення єдиної методологічної основи функціонування державної системи ЗКІ; обмін інформацією між суб'єктами системи ЗКІ тощо.

4. **Секторальні органи державної влади** – формування політики у визначених секторах КІ. Розробляють секторальні вимоги законодавства щодо ЗКІ у відповідних секторах, затверджують секторальні проектні загрози та плани дій (відповідно до режимів функціонування критичної інфраструктури).

У рамках УЦБС та секторальних органів державної влади, створюються ситуаційно-кризові центри, які мають забезпечити взаємодію та обмін інформацією у всіх режимах функціонування державної системи ЗКІ.

5. **Функціональні органи державної влади** – формування вимог до забезпечення ЗКІ у відповідних сферах; надання секторальним органам, регуляторам, операторам інфраструктури консультації та допомоги у забезпеченні ЗКІ, здійснення контролю за дотриманням вимог законодавства.

6. **Оператори критичної інфраструктури** – забезпечення безпеки та стійкості критичної інфраструктури. Оператори проводять оцінку ризиків на рівні об'єктів (ресурсів, мереж, систем), якими вони управляють, та розробляють заходи щодо забезпечення їх безпеки та стійкості, залучення інвестицій у систему захисту, проводять навчання тощо. Оператори забезпечують розробку та затвердження відповідних документів, що регламентують забезпечення ЗКІ (паспортів безпеки ОКІ, планів запобігання, реагування, відновлення тощо).

При цьому слід зазначити, що відповідно до затвердженої Концепції державна система ЗКІ має функціонувати у чотирьох різних режимах, а саме:

- штатний режим функціонування (проведення оцінки можливих загроз та аналіз ризиків, інформування про імовірні загрози);

- захист та реагування на випадок реалізації загрози (залучення до ліквідації наслідків ресурсів суб'єктів державної системи захисту критичної інфраструктури та власників (розпорядників) об'єктів критичної інфраструктури);

- функціонування в кризовій ситуації (залучення ресурсів з метою забезпечення стійкості функціонування об’єктів критичної інфраструктури);

- відновлення штатного режиму роботи і ліквідація наслідків кризової ситуації.

Відповідно, залучення до функціонування державної системи захисту критичної інфраструктури різних суб’єктів потребує чіткої регламентації завдань та повноважень між ними, формалізації інструментів та механізмів управлінських впливів, [16, 17, 18] а також налагодження системи взаємодії, обміну інформації та координацію дій.[19]

Саме Національний план захисту критичної інфраструктури України, на наш погляд, і має стати таким інструментом формалізації діяльності суб’єктів системи для реалізації державної політики ЗКІ. Слід зазначити, що вимогу щодо розробки та затвердження Національного плану передбачено і проектом Закону України “Про критичну інфраструктуру та її захист”, розробленого робочою групою при Міністерстві економіки і торгівлі України.[20]

В рамках сприяння розробці нормативно-правової бази функціонування державної системи ЗКІ вносяться пропозиції щодо формалізації вимог та завдань суб’єктів системи на першому етапі її створення (на період до 5 років).

Проект Національного плану захисту критичної інфраструктури України, розроблений з урахуванням запропонованої моделі функціонування державної системи ЗКІ та положень Концепції, наводиться у Додатку.

---

[16] Суходоля О.М. Стійкість енергетичної системи чи стійкість енергозабезпечення споживачів: постановка проблеми // Стратегічні пріоритет. – 2018. - №2. – с.101-117. Зокрема у роботі наведено підходи до формалізації вимог до забезпечення безпеки і стійкості КІ на прикладі сектору електропостачання.

[17] Бобро Д.Г. Урахування проектних загроз у розбудові державної системи захисту критичної інфраструктури / Д. Г. Бобро // Стратегічні пріоритети. - 2017. - № 3. - С. 42-51.

[18] Іванюта С.П. Пріоритети формування реєстру об'єктів критичної інфраструктури та порядку їх обліку // Стратегічні пріоритети. – 2018. – №3.

[19] Кондратов С.І. Про забезпечення координації дій, взаємодії та обміну інформацією при створенні державної системи захисту критичної інфраструктури. Аналітична доповідь. НІСД, 2018

[20] Проект Закону України “Про критичну інфраструктуру та її захист”. – [Електронний ресурс]. – Режим доступу: http://me.gov.ua/Documents/Detail?lang=uk-UA&id=5bea651c-dcfe-4513-afe6-0453fda32e68&title=ProektZakonuUkrainiproKritichnuInfrastrukturuTaYiiZakhist

ПРОПОЗИЦІЇ ТА РЕКОМЕНДАЦІЇ:

1. Апарату Ради національної безпеки і оборони України:

- організувати робочу нараду за участі представників державних органів (включаючи правоохоронні органи та спецслужби), інших заінтересованих сторін, залучених до виконання рішення Ради національної безпеки і оборони України "Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури" від 29 грудня 2016 року, введеного в дію Указом Президента України від 16 січня 2017 року №8/2017, за результатами якого розробити план заходів щодо прискорення виконання зазначеного указу Президента України;

- з метою забезпечення необхідних умов для взаємоузгодженого реформування національного сектору безпеки і оборони розглянути можливість включення до плану роботи Ради національної безпеки і оборони України на 2019 рік питання "Про узгодження основних параметрів функціонування державних (національних) систем у сфері національної безпеки і оборони".

2. Кабінету Міністрів України:

- прискорити процес погодження законопроекту "Про критичну інфраструктуру та її захист" та винести його на розгляд Верховної Ради України;

- забезпечити підготовку та затвердження Національного плану захисту критичної інфраструктури України.

3. Міністерству економічного розвитку і торгівлі України:

- подати пропозиції Кабінету Міністрів України щодо структури та змісту Національного плану захисту критичної інфраструктури України.

4. Міністерствам та іншим органам державної влади, залученим до процесу створення державної системи захисту критичної інфраструктури:

- підготувати пропозиції Міністерству економічного розвитку і торгівлі України до Національного плану захисту критичної інфраструктури України, відповідно до їх компетенції.

Суходоля О.М.
Відділ енергетичної та техногенної безпеки
Національний інститут стратегічних досліджень
січень 2019 р.

Проект

Національний план захисту критичної інфраструктури України

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 ЗКІ, яка є основою реалізації життєво-важливих функцій (послуг).

Національний план безпосередньо визначає організаційно-інституційну модель та механізми взаємодії суб'єктів державної системи ЗКІ, 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 ЗКІ 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 ЗКІ 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 в безпеку;
- Формування системи взаємодії та обміну інформацією для управління ризиками КІ;
- Забезпечення постійного розвитку знань та адаптації суб'єктів до появи нових викликів та загроз стійкості національної критичної інфраструктури,

завдяки формуванню заходів щодо навчання та підготовки персоналу, проведення тренінгів та навчань.

2. Сучасні виклики та пріоритети створення державної системи БСКІ

Для стабільного і безпечного існування сучасне суспільство та держава мають надійно отримувати цілу низку самих різноманітних продуктів і послуг, мати доступ до ряду 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, в даний час 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 врегульовує дії суб’єктів системи щодо забезпечення ЗКІ, зокрема формування спроможності:

- *не допустити критичний негативний вплив загроз будь-якого виду та їх можливих комбінацій на функціонування критичної інфраструктури;*
- *критичної інфраструктури надійно функціонувати у штатному режимі, адаптуватись до умов, що постійно змінюються, протистояти загрозам та швидко відновлюватись після реалізації загроз усіх типів загроз.*

План формує систему управління ризиками та зменшення вразливості КІ до загроз будь-якого типу, завдяки чіткій організації та плануванню діяльності суб’єктів системи забезпечення ЗКІ, визначенню завдань та порядку взаємодії та обміну інформацією залучених суб’єктів системи на всьому циклу забезпечення функціонування КІ та імовірного 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 формуванням у них відчуття безпеки є базовими умовами забезпечення національної стійкості. Виділення найважливіших для життєдіяльності країни життєво-важливих функцій, і тим самим секторів КІ, виступає інструментом визначення меж відповідальності та завдань системи ЗКІ. Життєво-важливі функції/послуги, надання яких забезпечуються функціонуванням відповідних секторів КІ, також визначають розподіл та обсяг завдань для органів державної влади, залучених до функціонування системи ЗКІ.

План виходить з того, що основні життєво-важливі функції/послуги, підтримання яких має забезпечити відповідно КІ є 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[21] критичної інфраструктури, які забезпечують визначених життєво-важливих функції/послуг, 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.

3. Система взаємодії, координації та управління

Широке коло завдань та необхідність залучення широкого кола суб'єктів державної системи до узгодженої діяльності щодо забезпечення ЗКІ потребує створення ефективної системи координації на загальнодержавному та місцевому рівні.

План визначає основні завдання суб'єктів державної системи ЗКІ відповідно до режиму функціонування системи, у тому числі вимогу щодо формування з вимог законодавства у відповідних режимах (***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.

План встановлює вимогу щодо запровадження системи управління ризиками критичної інфраструктури. Завданням системи управління ризиками є забезпечення всіх суб'єктів державної системи чіткими та ефективними процедурами взаємодії та обміну інформацією з оцінки ризиків та періодичного проведення оцінки та аналізу наслідків реалізації загроз КІ на національному рівні; ініціювання необхідних змін системи забезпечення ЗКІ.

Складовою такої системи і вимогою Плану є завдання щодо підготовки **Національної оцінки ризиків для критичної інфраструктури**. План передбачає проведення моніторингу загроз, які можуть спричинити негативні наслідки для критичної інфраструктури ризики критичній протягом наступних 5 років.

[21] Перелік секторів критичної інфраструктури та відповідальних за сектори органів державної влади має бути затверджено рішенням Кабінету Міністрів України. Це може бути окрема постанова Кабінету Міністрів України або додатком до Національного плану.

Національна оцінка ризиків забезпечуватиме суб'єктів державної системи оцінкою 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. 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**. Даний документ слугуватиме для формування орієнтирів та порад населенню, громадам та бізнесу щодо планування своїх дій на випадок надзвичайних ситуацій цивільного характеру.

4. Планування розвитку державної системи ЗКІ

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 ЗКІ

План передбачає завдання суб'єктам державної системи щодо розробки нормативно-правової бази забезпечення ЗКІ.

Термін підготовки – шість місяців після прийняття Закону України «Про критичну інфраструктуру та її захист» [22]

4.2. Розробки плану розвитку системи забезпечення ЗКІ

План визначає завдання щодо розробки Плану заходів із розвитку системи забезпечення БСКІ.

Термін підготовки – щорічно

План заходів із розвитку системи забезпечення ЗКІ, затверджується Кабінетом Міністрів України та має забезпечити визначення відповідальних органів державної влади за виконання наступних 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, включаючи: розширення кола загроз та учасників, залучених до процесу аналізу; розробка профілів ризику та сценарного прогнозування розвитку ситуації; використанню сучасних стандартів кризового менеджменту; моніторингу прогресу; та подальшого тестування існуючих планів через тренування та навчання. Досягнення цієї стратегічної мети забезпечить більшу чіткість та ефективність діяльності усіх суб'єктів системи, визначить пріоритетність діяльності та розподілу ресурсів.

[22] Прийняття Закону України «Про критичну інфраструктуру та її захист» є вимогою рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури»

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*).**

  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 1 разу на 5 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 та тренінгів. Практичні навчання є ефективними інструментами оцінки, апробації та удосконалення планування дій суб'єктів ЗКІ;

  Термін підготовки – щорічно за встановленим графіком
- Сприяння прийняттю та практичному застосуванню сучасних стандартів забезпечення ЗКІ, 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 1 разу на 3 роки.
- Формування системи моніторингу рівня ЗКІ, 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 ЗКІ 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 ЗКІ. Формування програми дій та інструментів акцентування уваги підвищенні стійкості КІ забезпечить розуміння відповідної аудиторії (включаючи галузеві мережі, урядові структури та громадськість). Необхідне запровадження періодичних звітів щодо ЗКІ на різних управлінських рівнях.

  Термін підготовки – щорічно
- Формування платформи із співробітництва зацікавлених суб'єктів системи, шляхом запровадження різнорівневих дискусійних, експертних

площадок 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 1 року

- Залучення бізнес-ініціативи до вдосконалення ЗКІ, 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 ЗКІ. Своєчасний обмін інформацією між урядом та секторами КІ необхідний для ефективного управління ризиками та 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 1 року

- Розширення можливостей для обміну інформацією за допомогою різних засобів, включаючи формальні угоди, віртуальні та фізичні механізми, а також створення та поширення інформаційних продуктів. У той же час, розповсюдження та розголошення інформації, має здійснюватись за чіткими процедурами, що забезпечують захист чутливої інформації.

  Термін підготовки – протягом 1 року

- Ліквідація прогалин у забезпеченні захисту інформації в процесі обміну між суб'єктами системи завдяки врегулювання процедур взаємодії органів державної влади і операторів критичної інфраструктури, зацікавленими сторонами приватного сектору (бізнесу).

  Термін підготовки – протягом 2 років

Додаток до
Національного плану захисту критичної інфраструктури

1. Завдання суб'єктів державної системи забезпечення ЗКІ

1.1. <u>Завдання щодо запровадження системи забезпечення ЗКІ</u>

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 ЗКІ - *Протягом 2 років з 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 з дня прийняття Плану*;
- Організація 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*;
- Організація взаємодії з іншими суб'єктами системи забезпечення ЗКІ - *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*;
- Підготовка пропозицій до Реєстру об'єктів КІ - *Протягом 4 місяців з дня прийняття Плану*;
- Підготовка пропозицій до Національної оцінки ризиків критичній інфраструктури - *Протягом 9 місяців з 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:

- Розроблення та затвердження функціональних вимог законодавства щодо організації забезпечення ЗКІ - *Протягом 2 років з дня прийняття Плану*;
- Погодження Паспорта безпеки об'єктів КІ - *Протягом місяця з дати подання оператором*;
- Погодження Планів операторів КІ щодо запобігання та реагування на загрози КІ - *Протягом місяця з дати подання оператором*;
- Оцінка загроз та ризиків КІ; сценарне прогнозування розвитку ситуації - *Протягом 6 місяців з дня прийняття Плану*;
- Формування пропозицій до Національної та Секторальних Проектних загроз - *Протягом 3 місяців з дня прийняття Плану*;
- Організація взаємодії та обміну інформацією із іншими суб'єктами системи ЗКІ - *Протягом 1 року з дня прийняття Плану*;

- Контроль за дотриманням вимог законодавства - *Щорічно за встановленим графіком*;
- Підготовка пропозицій до Реєстру об’єктів КІ - *Протягом 4 місяців з 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 з дня прийняття Плану*;
- Підготовку пропозицій до Реєстру об’єктів КІ - *Протягом 4 місяців з дня прийняття Плану*;
- Підготовку пропозицій до Національної оцінки ризиків критичній інфраструктури - *Протягом 9 місяців з 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 з 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 ЗКІ - *Протягом 1 року з дня прийняття Плану*;
- Підготовку пропозицій до Реєстру об’єктів КІ - *Протягом 4 місяців з дня прийняття Плану*;

1.1.5. Урядовий центр безпеки і стійкості (УЦБС) здійснює такі заходи:

- Розроблення Методики оцінки загроз критичній інфраструктурі - *Протягом 4 місяців з дня прийняття Плану*;
- Затвердження Реєстру об’єктів КІ - *Протягом 6 місяців з дня прийняття Плану*;
- Розроблення Національної оцінки ризиків критичній інфраструктури - *Протягом 9 місяців з дня прийняття Плану*;
- Опублікування Оцінки ризиків критичній інфраструктури - *Протягом 1 року з дня прийняття Плану*;
- Розроблення проекту Національної проектної загрози КІ - *Протягом 1 року з дня прийняття Плану*;
- Підготовку проекту правового акту 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 графіку*.

1.1.6. КМУ та РНБО забезпечують:

- Затвердження процедури зміну режиму роботи критичної інфраструктури (відповідно до розподілу повноважень) - *Протягом 6 місяців з дня прийняття Плану*;
- Затвердження КМУ Національного плану захисту критичної інфраструктури - *Протягом 6 місяців з дня прийняття Плану*;
- Затвердження РНБО Національної Проектної загрози - *Не пізніше 2 років з 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, в частині формалізації вимог щодо діяльності	Протягом 1 року
	Прийняття та доведення рішення щодо зміни режиму функціонування критичної інфраструктури	Протягом 2 годин від прийняття інформації
Секторальні органи влади	Підготовка та прийняття нормативно-правових актів, в частині формалізації вимог щодо діяльності	Протягом 1 року
Функціональні органи влади	Підготовка та прийняття нормативно-правових актів, в частині формалізації вимог щодо діяльності	Протягом 1 року
Оператори	Підготовка та прийняття корпоративних рішень, в частині формалізації вимог щодо діяльності	Протягом 1 року
Місцеві органи влади	Підготовка та прийняття нормативно-правових актів, в частині формалізації вимог щодо діяльності	Протягом 1 року
КМУ та РНБО	Прийняття необхідних актів законодавства для формування нормативно-правової бази забезпечення захисту та стійкості критичної інфраструктури	Протягом 2 років
штатний режим функціонування		
УЦБС, КМУ та РНБО Секторальні органи	Забезпечення, за встановленими процедурами обробки та обміну інформацією щодо: оцінки загроз КІ, можливих сценаріїв розвитку ситуації внаслідок реалізації загроз; готовності системи захисту КІ відповідно до вимог;	За встановленим графіком

влади, Функціональні органи влади Оператори Місцеві органи влади	уточнення щодо Реєстру об'єктів КІ; доведення змін вимог законодавства щодо захисту КІ;	
Урядовий кризовий центр Секторальні органи влади	Доведення інформації щодо зміни режиму функціонування державної системи захисту критичної інфраструктури. Приведення сил оператора КІ та секторальних сил та ресурсів до режиму готовності.	Протягом 30 хвилин після прийняття рішення Протягом 1 години після прийняття рішення
режим запобігання виникненню кризової ситуації		
УЦБС	Забезпечення вчасного, ефективного і збалансованого інформування усіх суб'єктів реагування; Забезпечення виваженого інформування населення, ЗМІ та експертів; Доведення інформації щодо зміни режиму функціонування державної системи захисту критичної інфраструктури.	За встановленим графіком За встановленим графіком Протягом 15 хвилин 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; Оцінка можливих сценаріїв розвитку кризової ситуації; Забезпечення вчасного, ефективного і збалансованого інформування усіх суб'єктів реагування;	Протягом 15 хв після прийняття рішення Протягом 1 години після прийняття рішення 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 години 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 години після прийняття рішення)

Місцеві органи влади	Активація місцевих програм забезпечення захисту та стійкості критичної інфраструктури; планів взаємодії відповідно до секторів критичної інфраструктури	Протягом 1 години після прийняття рішення
КМУ та РНБО	Повідомлення для ЗМІ та міжнародного співтовариства	Протягом 2 годин після прийняття рішення
режим кризової ситуації		
УЦБС	Розгортання повномасштабної системи управління кризовою ситуацією (Міжвідомчого оперативного кризового штабу); Забезпечення управління в режимі кризової ситуації Збір та передача 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 години після прийняття рішення) Протягом 2 годин (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 години після прийняття рішення)
Оператори	Реалізація первинного реагування силами та засобами персоналу об’єкта критичної інфраструктури та зовнішніх сил, залучених відповідно до плану Здійснення попередньої оцінки ситуації (характеру інциденту та рівня кризової ситуації) та прийняття рішення щодо активізації Плану взаємодії із іншими силами сектору безпеки і оборони	Протягом 15 хв після прийняття рішення щодо запровадження режиму кризового реагування Відповідно до планів запобігання (не пізніше 1 години

	Активація планів (процедур) аварійного реагування, використання резервних можливостей для забезпечення надання життєво-важливих функцій/послуг	після прийняття рішення) Протягом 1 години (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 години після прийняття рішення)
КМУ та РНБО	Забезпечення управління в режимі кризової ситуації Недопущення ескалації кризи та її використання у цілях, що загрожують національній безпеці держави Мобілізація усіх ресурсів для нейтралізації можливих загроз національній безпеці Здійснення запиту (за необхідності) щодо допомоги від міжнародного співтовариства	Відповідно до планів запобігання (не пізніше 1 години після прийняття рішення)
режим відновлення		
УЦБС	Оцінка можливості скасування режиму кризового реагування. Припиняється робота секторального Міжвідомчого оперативного штабу реагування на кризову ситуацію.	Протягом 1 години після прийняття рішення
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 надзвичайних ситуацій. Аналіз уроків, винесених з кризової (надзвичайної) ситуації, планування заходів з підвищення рівня безпеки.	Протягом 1 години 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.	Відповідно до місцевих планів

	Активація місцевих програм відновлення надання життєво-важливих функцій/послуг.	
КМУ та РНБО	Прийняття рішення щодо скасування режиму кризового реагування (надзвичайного чи особливого стану). Здійснення запиту (за необхідності) щодо допомоги від міжнародного співтовариства.	