

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Роздатковий матеріал

**Ситуаційної вправи (TABLETOP EXERCISE)**

**ТЕМА: "[ТЕМА ВПРАВИ]"**

**Київ - 2023**

# ЗМІСТ

|  |  |  |
| --- | --- | --- |
| 1 | Закон України «Про критичну інфраструктуру» | 3 |
| 2 | Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 «Деякі питання об’єктів критичної інфраструктури» | 35 |
| 3 | Порядок ведення Реєстру об’єктів критичної інфраструктури, включення таких об’єктів до Реєстру, доступу та надання інформації з нього | 65 |
| 4 | Порядок розроблення та погодження паспорта безпеки на об’єкт критичної інфраструктури | 71 |
| 5 | Регламент обміну інформацією між суб’єктами національної системи захисту критичної інфраструктури | 77 |

**ЗАКОН УКРАЇНИ**

***(без прикінцевих положень)***

**Про критичну інфраструктуру**

**{Із змінами, внесеними згідно із Законом № 2684-IX від 18.10.2022}**

Цей Закон визначає правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури і є складовою законодавства у сфері національної безпеки.

**Розділ I**

**ЗАГАЛЬНІ ПОЛОЖЕННЯ**

**Стаття 1.** Визначення основних термінів

1. У цьому Законі наведені нижче терміни вживаються в такому значенні:

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

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

3) захист критичної інфраструктури - всі види діяльності, що виконуються перед або під час створення, функціонування, відновлення і реорганізації об’єкта критичної інфраструктури, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об’єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації;

4) ідентифікація об’єкта критичної інфраструктури - процедура віднесення об’єкта інфраструктури до об’єктів критичної інфраструктури;

5) інцидент безпеки критичної інфраструктури (далі - інцидент) - подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки несанкціонованого втручання в функціонування об’єкта критичної інфраструктури, які становлять загрозу його безпеці, системі управління технологічними процесами об’єкта критичної інфраструктури, створюють ймовірність порушення штатного режиму функціонування такого об’єкта (у тому числі зриву та/або блокування роботи, та/або несанкціонованого управління його ресурсами), ставлять під загрозу його захищеність;

6) категоризація об’єктів інфраструктури - віднесення об’єктів інфраструктури до категорій критичності об’єктів інфраструктури;

7) категорія критичності (критерії) об’єкта критичної інфраструктури - ступінь (відносний рівень) важливості об’єкта критичної інфраструктури, класифікована (категоризована) залежно від його впливу на виконання життєво важливих функцій та/або надання життєво важливих послуг;

8) кризова ситуація - порушення або загроза порушення штатного режиму функціонування критичної інфраструктури чи окремого її об’єкта, реагування на яке потребує залучення додаткових сил і ресурсів;

9) критична інфраструктура - сукупність об’єктів критичної інфраструктури;

10) критична технологічна інформація - дані, що обробляються (приймаються, передаються, зберігаються) в системах управління технологічними процесами об’єктів критичної інфраструктури;

11) національна система захисту критичної інфраструктури - сукупність органів управління, сил та засобів центральних і місцевих органів виконавчої влади (військово-цивільних адміністрацій - у разі утворення), органів місцевого самоврядування, операторів критичної інфраструктури, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури;

12) несанкціоноване втручання - незаконні дії, що створили загрозу безпечному функціонуванню об’єкта критичної інфраструктури та призвели до одного або декількох з таких наслідків: порушили його безперервність і стійкість; створили реальні чи потенційні загрози для населення, суспільства, соціально-економічного стану, національної безпеки і оборони України;

13) об’єкти критичної інфраструктури - об’єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам;

14) оператор критичної інфраструктури - юридична особа будь-якої форми власності та/або фізична особа - підприємець, що на правах власності, оренди або на інших законних підставах здійснює управління об’єктом критичної інфраструктури та відповідає за його поточне функціонування;

15) охорона об’єктів критичної інфраструктури - комплекс режимних, інженерних, інженерно-технічних та інших заходів (крім заходів із захисту інформації та кіберзахисту об’єктів критичної інформаційної інфраструктури), які організовуються і проводяться суб’єктами національної системи захисту критичної інфраструктури з метою запобігання та/або недопущення чи припинення протиправних дій (актів несанкціонованого втручання) на об’єктах критичної інфраструктури;

16) паспорт безпеки - документ встановленої форми, який містить відомості про об’єкт критичної інфраструктури, а також комплекс заходів, що вживаються для захисту цього об’єкта від визначених для нього видів загроз (відомості, що містяться у паспорті безпеки, є інформацією з обмеженим доступом);

17) проектна загроза об’єкту критичної інфраструктури - документ встановленої форми, який визначає властивості, характеристики реальних і потенційних загроз об’єкту критичної інфраструктури, на зниження ймовірності реалізації яких має бути спрямовано функціонування системи захисту критичної інфраструктури;

18) реєстр об’єктів критичної інфраструктури - автоматизована система, що містить перелік найбільш важливої для життєдіяльності суспільства та держави критичної інфраструктури, щодо якої встановлюються особливі вимоги із забезпечення її безпеки та стійкості і здійснюється моніторинг їх дотримання;

19) режим функціонування критичної інфраструктури - визначені оператором умови та вимоги до функціонування критичної інфраструктури залежно від стану і динаміки розвитку ситуації (штатний режим функціонування; режим функціонування у кризовій ситуації; режим відновлення);

20) рівень критичності об’єкта критичної інфраструктури - відносна міра важливості об’єкта, якою враховується його вплив на можливість виконання життєво важливих функцій та надання життєво важливих послуг;

21) сектор критичної інфраструктури - сукупність об’єктів критичної інфраструктури, які належать до одного сектору (галузі) економіки та/або мають спільну функціональну спрямованість;

22) секторальний орган у сфері захисту критичної інфраструктури - державний орган, визначений законодавством відповідальним за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури;

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

24) функціональний орган у сфері захисту критичної інфраструктури - державний орган, визначений відповідальним за функціонування окремих державних систем захисту та реагування.

**Стаття 2.** Законодавство про критичну інфраструктуру та її захист

1. Законодавство про критичну інфраструктуру та її захист складають Конституція України, цей Закон, інші закони України, міжнародні договори України, згода на обов’язковість яких надана Верховною Радою України, інші нормативно-правові акти, прийняті на виконання цього Закону.

**Стаття 3.** Сфера застосування цього Закону

1. Цей Закон регулює відносини у сфері функціонування та захисту критичної інфраструктури в цілому та її об’єктів у мирний час.

2. Особливості захисту та правового режиму об’єктів критичної інфраструктури в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, особливого періоду регулюються законами України "Про правовий режим воєнного стану", "Про правовий режим надзвичайного стану", "Про функціонування єдиної транспортної системи України в особливий період" та "Про оборону України".

3. Окремим законом регулюються відносини щодо забезпечення кіберзахисту та кібербезпеки об’єктів критичної інфраструктури.

**Розділ II**

**ОСНОВНІ ЗАСАДИ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ**

**Стаття 4.** Засади державної політики у сфері захисту критичної інфраструктури

1. Захист критичної інфраструктури є складовою частиною забезпечення національної безпеки України.

2. Державна політика у сфері захисту критичної інфраструктури ґрунтується на засадах:

1) визнання необхідності забезпечення безпеки та стійкості критичної інфраструктури;

2) визначення законодавчих вимог до принципів, пріоритетів, стратегічних завдань, підходів щодо захисту критичної інфраструктури;

3) визначення суб’єктів національної системи захисту критичної інфраструктури, їх повноважень та засад відповідальності, порядку взаємодії;

4) створення умов та впровадження заходів, спрямованих на ефективне зниження і контроль за ризиками безпеки, на зниження ризику реалізації можливих загроз, ліквідацію та/або мінімізацію наслідків реалізованих загроз, кризових ситуацій та інших їх видів;

5) створення системи раннього виявлення загроз критичній інфраструктурі;

6) запровадження державно-приватного партнерства, взаємодії суб’єктів господарювання та населення з питань забезпечення захисту та стійкості критичної інфраструктури;

7) забезпечення міжнародного співробітництва у сфері захисту критичної інфраструктури;

8) створення умов швидкого відновлення надання життєво важливих функцій та послуг у разі реалізації загроз і порушення функціонування критичної інфраструктури.

3. Державна політика у сфері захисту критичної інфраструктури спрямовується на формування комплексу організаційних, нормативно-правових, інженерно-технічних, ресурсних, інформаційно-аналітичних та методологічних заходів, спрямованих на забезпечення безпеки критичної інфраструктури.

**Стаття 5.** Мета та завдання державної політики у сфері захисту критичної інфраструктури

1. Метою державної політики у сфері захисту критичної інфраструктури є забезпечення безпеки об’єктів критичної інфраструктури, запобігання проявам несанкціонованого втручання в їх функціонування, прогнозування та запобігання кризовим ситуаціям на об’єктах критичної інфраструктури.

2. До завдань формування і реалізації державної політики у сфері захисту критичної інфраструктури належать:

1) запобігання проявам несанкціонованого втручання в її функціонування, прогнозування та запобігання кризовим ситуаціям на об’єктах критичної інфраструктури;

2) попередження кризових ситуацій, що порушують безпеку критичної інфраструктури;

3) створення, впровадження, розвиток та забезпечення функціонування національної системи захисту критичної інфраструктури, у тому числі шляхом визначення уповноваженого органу у сфері захисту критичної інфраструктури України, а також визначення повноважень у сфері захисту критичної інфраструктури інших суб’єктів національної системи захисту критичної інфраструктури;

{Пункт 3 частини другої статті 5 із змінами, внесеними згідно із Законом № 2684-IX від 18.10.2022}

4) розроблення нормативно-правової та нормативно-технічної бази з питань забезпечення безпеки об’єктів критичної інфраструктури;

5) розроблення та реалізація державних цільових програм із захисту критичної інфраструктури;

6) розроблення комплексу заходів з контролю за ризиками безпеки, виявлення, запобігання та ліквідації наслідків інцидентів безпеки на об’єктах критичної інфраструктури;

7) встановлення обов’язкових вимог із забезпечення безпеки об’єктів критичної інфраструктури, їх захищеності на всіх етапах життєвого циклу, у тому числі під час створення, прийняття в експлуатацію, модернізації;

8) аналіз викликів та загроз, що впливають на стійкість критичної інфраструктури, оцінка стану її захищеності;

9) розроблення методології аналізу результативності державної політики у сфері захисту критичної інфраструктури;

10) підготовка, перепідготовка, підвищення кваліфікації, тренування працівників національної системи захисту критичної інфраструктури;

11) забезпечення взаємодії національної системи захисту критичної інфраструктури з відповідними міжнародними системами, насамперед європейськими та євроатлантичними.

**Стаття 6.** Основні принципи функціонування національної системи захисту критичної інфраструктури

1. До основних принципів функціонування національної системи захисту критичної інфраструктури належать:

1) єдність методологічних засад;

2) координованість;

3) державно-приватне партнерство;

4) безпека, захист та охорона інформації з обмеженим доступом;

5) міжнародне співробітництво.

**Стаття 7.** Рівні управління національною системою захисту критичної інфраструктури

1. Національна система захисту критичної інфраструктури має такі рівні управління:

1) загальнодержавний рівень, управління на якому здійснюється Кабінетом Міністрів України, уповноваженим органом у сфері захисту критичної інфраструктури України, органами державної влади відповідно до розподілу повноважень згідно з цим Законом, іншими центральними органами виконавчої влади та державними органами, Національним банком України;

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

3) місцевий рівень, управління на якому здійснюється місцевими органами виконавчої влади (військово-цивільними адміністраціями - у разі створення), органами місцевого самоврядування в межах повноважень, покладених на них цим Законом;

4) об’єктовий рівень, управління на якому здійснюється оператором критичної інфраструктури на підставі нормативно-правових та регуляторних актів у сфері захисту критичної інфраструктури.

**Розділ III**

**КРИТИЧНА ІНФРАСТРУКТУРА УКРАЇНИ**

**Стаття 8.** Віднесення об’єктів до критичної інфраструктури

1. Віднесення об’єктів до критичної інфраструктури здійснюється в порядку, встановленому Кабінетом Міністрів України.

Віднесення банків, інших об’єктів, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, платіжних організацій, учасників платіжних систем, операторів послуг платіжної інфраструктури здійснюється в порядку, встановленому Національним банком України.

Віднесення об’єктів до критичної інфраструктури, що здійснюють діяльність на ринках послуг, державне регулювання та нагляд за діяльністю яких здійснюють державні органи, здійснюється в порядку, встановленому такими державними органами.

2. Віднесення об’єктів до критичної інфраструктури здійснюється за сукупністю критеріїв, що визначають їх соціальну, політичну, економічну, екологічну значущість для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку, зокрема для реалізації життєво важливих функцій та надання життєво важливих послуг, свідчать про існування загроз для них, можливість виникнення кризових ситуацій через несанкціоноване втручання в їх функціонування, припинення функціонування, людський фактор чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму.

3. До таких критеріїв належать:

1) виконання функцій із забезпечення життєво важливих національних інтересів;

2) існування викликів і загроз, що можуть виникати щодо об’єктів критичної інфраструктури;

3) ймовірність завдання значної шкоди нормальним умовам життєдіяльності населення;

4) уразливість таких об’єктів, тяжкість 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); державному суверенітету (зниження обороноздатності, дискредитація іміджу країни, дестабілізація системи державного управління та унеможливлення виконання державою своїх функцій); економіці (вплив на внутрішній валовий продукт, розмір економічних втрат, як прямих, так і непрямих); природним ресурсам загальнодержавного та місцевого значення;

5) масштабність негативних наслідків для держави, які впливають на діяльність стратегічно важливих об’єктів для кількох секторів життєзабезпечення чи призводять до втрати унікальних національно значущих активів, систем і ресурсів, матимуть тривалі наслідки для держави і позначаться на діяльності ряду інших секторів;

6) тривалість ліквідації таких наслідків та дія подальшого негативного впливу на інші сектори держави;

7) вплив на функціонування суміжних секторів критичної інфраструктури.

4. Об’єкти критичної інфраструктури, що не можуть належати:

фізичним і юридичним особам - громадянам та/або резидентам держави, визнаної Верховною Радою України державою-агресором, або кінцевими бенефіціарними власниками яких є громадяни держави, визнаної Україною державою-агресором або державою-окупантом;

юридичним особам, зареєстрованим згідно із законодавством держав, включених FAТF до списку держав, що не співпрацюють у сфері протидії відмиванню доходів, одержаних злочинним шляхом, а також юридичним особам, 50 і більше відсотків статутного капіталу яких належать прямо або опосередковано таким особам, протягом року підлягають відчуженню.

**Стаття 9.** Сектори критичної інфраструктури

1. Для організації ефективного забезпечення безпеки і стійкості критичної інфраструктури з урахуванням специфіки забезпечення окремих життєво важливих функцій та/або послуг визначаються сектори критичної інфраструктури.

2. Для секторів критичної інфраструктури визначаються особливості реалізації державної політики у сфері захисту критичної інфраструктури. Формування та реалізацію державної політики у відповідних секторах здійснюють секторальні органи у сфері захисту критичної інфраструктури.

Секторальні органи у сфері захисту критичної інфраструктури складають та ведуть секторальні переліки об’єктів критичної інфраструктури.

3. Перелік секторів критичної інфраструктури та суб’єктів, відповідальних за формування та реалізацію державної політики у відповідних секторах національної системи захисту критичної інфраструктури (далі - Перелік), визначається Кабінетом Міністрів України. У разі необхідності внесення змін до Переліку Кабінет Міністрів України переглядає та змінює його виходячи з критеріїв критичності, визначених цим Законом.

4. До життєво важливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки України, належать, зокрема:

1) урядування та надання найважливіших публічних (адміністративних) послуг;

2) енергозабезпечення (у тому числі постачання теплової енергії);

3) водопостачання та водовідведення;

4) продовольче забезпечення;

5) охорона здоров’я;

6) фармацевтична промисловість;

7) виготовлення вакцин, стале функціонування біолабораторій;

8) інформаційні послуги;

9) електронні комунікації;

10) фінансові послуги;

11) транспортне забезпечення;

12) оборона, державна безпека;

13) правопорядок, здійснення правосуддя, тримання під вартою;

14) цивільний захист населення та територій, служби порятунку;

15) космічна діяльність, космічні технології та послуги;

16) хімічна промисловість;

17) дослідницька діяльність.

**Стаття 10.** Категоризація об’єктів критичної інфраструктури

1. Для визначення рівня вимог щодо забезпечення захисту об’єктів критичної інфраструктури відповідно до рівня їх важливості для забезпечення окремих життєво важливих функцій у межах секторів критичної інфраструктури здійснюється категоризація об’єктів критичної інфраструктури відповідно до категорій критичності, визначених цим Законом.

2. Установлюються такі категорії критичності об’єктів критичної інфраструктури:

1) I категорія критичності - особливо важливі об’єкти, які мають загальнодержавне значення, значний вплив на інші об’єкти критичної інфраструктури та порушення функціонування яких призведе до виникнення кризової ситуації державного значення;

2) II категорія критичності - життєво важливі об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення;

3) III категорія критичності - важливі об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації місцевого значення;

4) IV категорія критичності - необхідні об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації локального значення.

3. Категоризація об’єктів критичної інфраструктури здійснюється секторальними органами у сфері захисту критичної інфраструктури відповідно до секторальної специфіки та вимог секторального законодавства.

4. Секторальні органи разом з операторами критичної інфраструктури здійснюють категоризацію об’єктів критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури відповідно до Методики категоризації об’єктів критичної інфраструктури, що затверджується Кабінетом Міністрів України, а в банківській та фінансовій системах - Національним банком України, у сферах, державне регулювання та нагляд за діяльністю яких здійснюють державні органи, - такими державними органами.

**Стаття 11.** Реєстр об’єктів критичної інфраструктури

1. Для цілей узгодження дій суб’єктів національної системи захисту критичної інфраструктури формується Реєстр об’єктів критичної інфраструктури (далі - Реєстр).

2. Збирання, узагальнення, попередній аналіз даних щодо об’єктів критичної інфраструктури та пропозиції щодо включення таких об’єктів до Реєстру в межах визначених секторів здійснюються секторальними органами у сфері захисту критичної інфраструктури.

3. Реєстр формується та ведеться уповноваженим органом у сфері захисту критичної інфраструктури України на основі пропозицій суб’єктів національної системи захисту критичної інфраструктури.

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

5. Порядок ведення Реєстру, включення об’єктів до Реєстру, доступу та надання інформації з нього визначається Кабінетом Міністрів України.

6. Інформація про об’єкти критичної інфраструктури, що міститься в Реєстрі, є відкритою, загальнодоступною та безоплатною, крім інформації з обмеженим доступом. Розпорядник забезпечує цілодобовий доступ до відкритої інформації Реєстру на своєму офіційному веб-сайті.

7. Для посадових осіб суб’єктів національної системи захисту критичної інфраструктури, визначених статтею 14 цього Закону, інформація з Реєстру у зв’язку із здійсненням ними повноважень, передбачених законом, надається за суб’єктом права чи за об’єктом критичної інфраструктури в електронній формі шляхом безпосереднього доступу до Реєстру, за умови ідентифікації відповідної посадової особи у порядку, встановленому Законом України "Про електронні довірчі послуги".

**Стаття 12.** Паспортизація об’єктів критичної інфраструктури

1. З метою проведення аналізу можливих основних загроз та потенційних негативних наслідків для об’єктів критичної інфраструктури, запобігання та попередження виникнення таких загроз для критичної інфраструктури оператори об’єктів критичної інфраструктури готують і подають на погодження до відповідних секторальних органів у сфері захисту критичної інфраструктури, відповідного функціонального органу паспорт безпеки на кожний об’єкт критичної інфраструктури.

2. Паспорт безпеки на об’єкт критичної інфраструктури містить інформацію про ідентифікацію об’єкта та заходи щодо його захисту і безпеки, а також визначає перелік посад та відповідальних осіб, до завдань яких належать зв’язок та обмін інформацією з суб’єктами національної системи захисту критичної інфраструктури.

3. Паспорт безпеки розробляється (переглядається) з урахуванням визначених проектних загроз. Погодження паспорта безпеки на об’єкт критичної інфраструктури здійснюється безоплатно для усіх операторів об’єктів критичної інфраструктури незалежно від форми власності.

4. Вимоги до порядку розроблення та погодження паспорта безпеки на об’єкт критичної інфраструктури, його наповнення, зміст, порядок і строки подання встановлюються Кабінетом Міністрів України.

5. Національний банк України визначає з урахуванням вимог цього Закону порядок розроблення паспорта безпеки на об’єкти критичної інфраструктури, зміст і строки подання його банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, платіжними організаціями, учасниками платіжних систем, операторами послуг платіжної інфраструктури.

6. Оператор критичної інфраструктури несе відповідальність за достовірність даних, наведених у паспорті безпеки, своєчасність внесення до нього змін.

7. Відомості, що містяться у паспорті безпеки, є інформацією з обмеженим доступом, вимога щодо захисту якої встановлена законом.

**Розділ IV**

**НАЦІОНАЛЬНА СИСТЕМА ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ**

**Стаття 13.** Формування та реалізація державної політики у сфері захисту критичної інфраструктури

1. Кабінет Міністрів України забезпечує проведення державної політики у сфері захисту критичної інфраструктури України, організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи захисту критичної інфраструктури, визначає уповноважений орган з питань захисту критичної інфраструктури України.

2. Формування та реалізацію державної політики в окремих секторах критичної інфраструктури здійснюють секторальні та функціональні органи у сфері захисту критичної інфраструктури відповідно до визначених законом повноважень.

3. Формування та реалізацію державної політики у сфері захисту критичної інфраструктури, координацію діяльності суб’єктів національної системи захисту критичної інфраструктури забезпечує уповноважений орган у сфері захисту критичної інфраструктури України.

{Частина третя статті 13 в редакції Закону № 2684-IX від 18.10.2022}

4. Для забезпечення обміну інформацією та взаємодії суб’єктів національної системи захисту критичної інфраструктури Кабінет Міністрів України затверджує Регламент обміну інформацією.

5. Обмін інформацією в рамках функціонування національної системи захисту критичної інфраструктури здійснюється відповідно до вимог законодавства у сфері захисту інформації.

**Стаття 14.** Суб’єкти національної системи захисту критичної інфраструктури

1. Суб’єктами національної системи захисту критичної інфраструктури є:

1) Кабінет Міністрів України;

2) Апарат Ради національної безпеки і оборони України;

3) Центральна виборча комісія;

4) Національний банк України;

5) Національна комісія з цінних паперів та фондового ринку, Національна комісія, що здійснює державне регулювання у сфері зв’язку та інформатизації, Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг;

6) Адміністрація Державної служби спеціального зв’язку та захисту інформації України;

7) Фонд державного майна України, інші центральні органи виконавчої влади із спеціальним статусом;

8) уповноважений орган у сфері захисту критичної інфраструктури України;

9) центральний орган виконавчої влади, який забезпечує формування та реалізує державну політику у сфері цивільного захисту;

10) секторальні та функціональні органи, інші міністерства та центральні органи виконавчої влади;

11) Служба безпеки України;

12) правоохоронні та розвідувальні органи, суб’єкти оперативно-розшукової та контррозвідувальної діяльності;

13) Збройні Сили України, інші військові формування, утворені відповідно до законів України;

14) місцеві органи виконавчої влади (військово-цивільні адміністрації - у разі утворення);

15) органи місцевого самоврядування;

16) оператори критичної інфраструктури;

17) підприємства, установи та організації незалежно від форми власності, які провадять діяльність, пов’язану із забезпеченням безпеки та стійкості критичної інфраструктури.

**Стаття 15.** Режими функціонування національної системи захисту критичної інфраструктури

1. Забезпечення захисту та стійкості критичної інфраструктури здійснюється в таких режимах її функціонування:

1) штатний режим - суб’єктами національної системи захисту критичної інфраструктури стосовно оцінки можливих загроз та інформування щодо них. Функціонування інфраструктури здійснюється відповідно до проектного цільового призначення;

2) режим готовності та запобігання реалізації загроз - секторальними та функціональними органами у сфері захисту критичної інфраструктури: проводиться перевірка та переведення системи захисту до готовності забезпечити захист та реагування на випадок реалізації загрози. Функціонування інфраструктури здійснюється відповідно до проектного цільового призначення;

3) режим реагування на виникнення кризової ситуації - суб’єктами національної системи захисту критичної інфраструктури із застосуванням заходів реагування на кризову ситуацію. Функціонування інфраструктури відбувається в режимі кризової ситуації, вводяться обмеження на режими роботи об’єктів інфраструктури, економічні умови господарювання, доступ до об’єктів;

4) режим відновлення штатного функціонування - суб’єктами національної 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.

2. Суб’єктами національної системи захисту критичної інфраструктури розробляється план взаємодії з іншими суб’єктами національної системи захисту, який погоджується з уповноваженим органом у сфері захисту критичної інфраструктури України та затверджується Кабінетом Міністрів України і переглядається раз на три роки. У плані взаємодії можуть бути визначені особливості взаємодії для режимів функціонування національної системи захисту критичної інфраструктури.

3. Рішення про оголошення режимів функціонування критичної інфраструктури приймається секторальними органами у сфері захисту критичної інфраструктури, відповідальними за сектор критичної інфраструктури.

**Стаття 16.** Уповноважений орган у сфері захисту критичної інфраструктури України

1. Уповноважений орган у сфері захисту критичної інфраструктури України забезпечує формування та реалізує державну політику у сфері захисту критичної інфраструктури, здійснює функціональне управління національною системою захисту критичної інфраструктури, забезпечує координацію діяльності міністерств та операторів критичної інфраструктури з питань забезпечення стійкості та захисту об’єктів критичної інфраструктури.

Діяльність уповноваженого органу у сфері захисту критичної інфраструктури України спрямовує, координує та контролює Кабінет Міністрів України.

{Абзац другий частини першої статті 16 в редакції Закону № 2684-IX від 18.10.2022}

2. Уповноважений орган у сфері захисту критичної інфраструктури України:

1) координує діяльність міністерств, інших центральних та місцевих органів виконавчої влади (військово-цивільних адміністрацій - у разі утворення) у сфері захисту критичної інфраструктури;

2) узагальнює пропозиції суб’єктів національної системи захисту критичної інфраструктури, формує та веде Реєстр;

3) взаємодіє з секторальними, функціональними органами у сфері захисту критичної інфраструктури та операторами критичної інфраструктури з питань забезпечення захисту об’єктів, включених до Реєстру;

4) організовує здійснення оцінки захищеності об’єктів критичної інфраструктури, внесених до Реєстру, аналізує та оцінює загальний стан їх захищеності;

5) проводить оцінку загроз критичній інфраструктурі на національному рівні та оцінку загроз національній безпеці внаслідок реалізації загроз критичній інфраструктурі із залученням секторальних та функціональних органів у сфері захисту критичної інфраструктури;

6) готує щорічну оцінку ризиків і загроз критичній інфраструктурі національного рівня;

7) погоджує проектні ризики та загрози критичній інфраструктурі секторального рівня;

8) готує рекомендації щодо визначення вимог до забезпечення захисту та стійкості секторів критичної інфраструктури відповідно до категорій об’єктів критичної інфраструктури;

9) надає пропозиції Кабінету Міністрів України щодо:

Національного плану захисту та забезпечення стійкості критичної інфраструктури;

порядку розроблення, форми та змісту паспорта безпеки об’єкта критичної інфраструктури;

порядку розроблення, форми та змісту планів заходів щодо захисту критичної інфраструктури, які приймаються на національному рівні;

10) розробляє та затверджує Проектні загрози критичній інфраструктурі національного рівня, що становлять інформацію з обмеженим доступом;

11) готує висновки та рекомендації власнику/оператору критичної інфраструктури щодо зміни права власності, цільового призначення чи режиму функціонування об’єкта критичної інфраструктури;

12) забезпечує функціонування системи обміну інформацією між суб’єктами національної системи захисту критичної інфраструктури;

13) створює бази даних щодо загроз і вразливостей критичній інфраструктурі;

14) забезпечує координацію секторальних органів, підготовку пропозицій до проектів стратегічних документів щодо забезпечення безпеки та стійкості, здійснення захисту критичної інфраструктури - Стратегії національної безпеки України, Стратегії кібербезпеки України та Стратегії громадської безпеки та цивільного захисту України;

15) бере участь у розробленні нової галузі знань, програм навчання, підвищення кваліфікації, робочих і навчальних програм з питань забезпечення стійкості та захисту критичної інфраструктури;

16) здійснює міжнародне співробітництво, забезпечує дотримання і виконання зобов’язань, взятих відповідно до міжнародних договорів України з питань захисту критичної інфраструктури, налагоджує і підтримує зв’язки з міжнародними організаціями, іноземними державами, їх правоохоронними органами і спеціальними службами;

17) здійснює інші повноваження, передбачені цим Законом.

3. Положення про уповноважений орган у сфері захисту критичної інфраструктури затверджується Кабінетом Міністрів України.

{Частина третя статті 16 в редакції Закону № 2684-IX від 18.10.2022}

**Стаття 17.** Функціональні органи у сфері захисту критичної інфраструктури

1. Органи державної влади, визначені відповідальними за функціонування окремих державних систем захисту та реагування:

1) беруть участь у встановленому законодавством порядку в реагуванні на кризові ситуації, пов’язані із забезпеченням безпеки та стійкості критичної інфраструктури;

2) готують пропозиції щодо включення об’єктів інфраструктури до Реєстру;

3) формують перелік об’єктів критичної інфраструктури, що належать до сфери їх управління;

4) надають власникам та операторам інфраструктури консультації щодо ризиків і загроз критичній інфраструктурі та заходів щодо їх нейтралізації;

5) здійснюють іншу діяльність для забезпечення стійкості та захисту критичної інфраструктури в межах повноважень, що регулюють діяльність суб’єктів захисту критичної інфраструктури, зокрема:

організовують проведення оцінки загроз та ризиків критичній інфраструктурі у відповідних сферах;

беруть участь у проведенні оцінки загроз та ризиків критичній інфраструктурі на загальнодержавному рівні;

формують пропозиції щодо національних та секторальних проектних ризиків і загроз;

забезпечують організацію взаємодії та обміну інформацією з іншими суб’єктами національної системи захисту критичної інфраструктури;

здійснюють моніторинг рівня безпеки об’єктів критичної інфраструктури у відповідних сферах.

**Стаття 18.** Особливості діяльності окремих органів, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури

1. Діяльність Національного банку України, уповноваженого органу у сфері захисту критичної інфраструктури України, центрального органу виконавчої влади, який забезпечує формування та реалізує державну політику у сфері цивільного захисту, Служби безпеки України, Національної гвардії України, Національної поліції України, Збройних Сил України, Державної спеціальної служби транспорту та Державної служби спеціального зв’язку та захисту інформації України з питань формування та/або реалізації державної політики у сфері захисту критичної інфраструктури здійснюється в рамках, визначених цим Законом, та у порядку, встановленому законами України, що регламентують правові засади організації та діяльності зазначених у цій статті органів.

**Стаття 19.** Секторальні органи у сфері захисту критичної інфраструктури

1. Державні органи, визначені відповідальними за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури, здійснюють такі завдання:

1) створюють у межах штатної чисельності у своєму складі структурні підрозділи з питань захисту критичної інфраструктури;

2) збирають, узагальнюють та здійснюють попередній аналіз даних щодо критичної інфраструктури та її функціонування;

3) спільно з операторами критичної інфраструктури здійснюють категоризацію об’єктів критичної інфраструктури своїх секторів критичної інфраструктури, формують секторальні переліки об’єктів критичної інфраструктури, подають інформацію до Реєстру;

4) розробляють та затверджують:

а) вимоги до захисту об’єктів критичної інфраструктури відповідно до їх категорій;

б) проектні загрози критичній інфраструктурі секторального рівня;

в) плани взаємодії функціональних органів у сфері захисту критичної інфраструктури у відповідних секторах для всіх режимів функціонування критичної інфраструктури; плани взаємодії та підтримання життєво важливих функцій на випадок порушення функціонування об’єктів критичної інфраструктури;

5) розробляють та впроваджують норми і регламенти захисту критичної інфраструктури у відповідних секторах критичної інфраструктури;

6) затверджують проектні загрози критичній інфраструктурі об’єктового рівня у відповідних секторах;

7) погоджують паспорти безпеки об’єктів критичної інфраструктури, надані операторами у відповідних секторах;

8) здійснюють:

а) перевірку та оцінку захищеності об’єктів критичної інфраструктури;

б) підготовку пропозицій до проектних ризиків та загроз критичній інфраструктурі національного рівня та щорічної оцінки ризиків і загроз критичній інфраструктурі національного рівня;

в) організацію системи підготовки персоналу, навчання та тренувань щодо забезпечення стійкості та захисту секторів критичної інфраструктури;

г) підготовку щорічного звіту щодо забезпечення захисту критичної інфраструктури у відповідному секторі;

ґ) участь у встановленому законодавством порядку в реагуванні на кризові ситуації, пов’язані з безпекою, захистом та стійкістю об’єктів критичної інфраструктури, а також у створенні умов для належного виконання правоохоронними, розвідувальними та контррозвідувальними органами своїх завдань щодо захисту критичної інфраструктури;

д) попередження про загрози операторів критичної інфраструктури та надають інформаційну, консультативну, експертну, методичну допомогу операторам критичної інфраструктури, користувачам їх послуг (населенню) задля попередження, реагування, мінімізації можливого впливу загроз;

9) надають операторам об’єктів критичної інфраструктури рекомендації з питань захисту критичної інфраструктури та обов’язкові до виконання вимоги щодо усунення причин і умов, які порушують стійкість критичної інфраструктури;

10) виконують:

а) збір, аналіз та узагальнення даних щодо об’єктів критичної інфраструктури та загроз їх функціонуванню;

б) заходи із функціонування відповідних систем обміну інформацією, моніторингу рівня безпеки об’єктів критичної інфраструктури;

11) організовують функціонування системи обміну інформацією та взаємодії у відповідних секторах критичної інфраструктури між суб’єктами національної системи захисту критичної інфраструктури;

12) готують пропозиції до стратегічних документів щодо забезпечення стійкості та захисту критичної інфраструктури.

2. Секторальні органи у сфері захисту критичної інфраструктури щороку відповідно до строків та форми звіту, затверджених Кабінетом Міністрів України, подають інформацію уповноваженому органу у сфері захисту критичної інфраструктури України.

**Стаття 20.** Місцеві органи виконавчої влади та військово-цивільні адміністрації

1. Місцеві органи виконавчої влади (військово-цивільні адміністрації - у разі утворення) у сфері захисту критичної інфраструктури забезпечують:

1) розроблення та затвердження місцевих програм забезпечення безпеки та стійкості критичної інфраструктури, програм підвищення стійкості територіальних громад до кризових ситуацій, викликаних припиненням або погіршенням надання важливих для їх життєдіяльності послуг чи для здійснення життєво важливих функцій;

2) розроблення, затвердження та погодження із заінтересованими органами:

а) місцевих планів взаємодії залучених суб’єктів у кризовій ситуації з метою підтримання життєво важливих функцій та надання життєво важливих послуг, планів відновлення функціонування критичної інфраструктури;

б) програм навчання населення для забезпечення захисту в разі виникнення режиму реагування на виникнення кризової ситуації та режиму відновлення штатного функціонування.

**Стаття 21.** Завдання, права та обов’язки операторів критичної інфраструктури

1. Основними завданнями операторів критичної інфраструктури є:

1) забезпечення захисту об’єктів критичної інфраструктури, зокрема створення, налагодження та підтримання функціонування ефективної системи фізичної безпеки, безпеки операційних систем та кібербезпеки;

2) розроблення, оновлення та забезпечення виконання об’єктових планів заходів щодо забезпечення безпеки і стійкості критичної інфраструктури, правил управління ризиками безпеки, планів локалізації та ліквідації наслідків аварій, а також заходів кіберзахисту;

3) проведення оцінки ризиків на об’єктах критичної інфраструктури та обмін інформацією про ризики та загрози з іншими суб’єктами національної системи захисту критичної інфраструктури, а також створення умов для належного виконання правоохоронними, розвідувальними та контррозвідувальними органами своїх завдань щодо захисту критичної інфраструктури;

4) створення окремого структурного підрозділу або визначення відповідальної особи за організацію захисту критичної інфраструктури та забезпечення постійного зв’язку з відповідними суб’єктами національної системи захисту критичної інфраструктури;

5) оперативне реагування на протиправні дії, фізичні атаки, спрямовані на відключення або пошкодження роботи операційних систем чи систем забезпечення фізичної безпеки об’єкта критичної інфраструктури;

6) організація заходів з реагування на інциденти, кризові ситуації, а також ліквідації їх наслідків на об’єктах критичної інфраструктури у взаємодії з іншими суб’єктами національної системи захисту критичної інфраструктури;

7) забезпечення відновлення функціонування об’єктів критичної інфраструктури в разі виникнення аварій та інших небезпечних подій, вчинення протиправних дій;

8) участь у заходах із захисту повітряного простору над визначеними об’єктами критичної інфраструктури;

9) негайне інформування уповноваженого органу у сфері захисту критичної інфраструктури України, органів Національної поліції України, Служби безпеки України, підрозділів Національної гвардії України, інших державних органів про інциденти, пов’язані з порушеннями систем фізичної безпеки та кібербезпеки, а також інформування Служби безпеки України про загрози та ризики диверсій, терористичних актів, актів кібертероризму проти систем управління, операційних та інших систем об’єктів критичної інфраструктури, надзвичайних ситуацій або інших небезпечних подій на важливих державних об’єктах;

10) забезпечення постійного зв’язку з відповідальними за реагування на протиправні дії та з іншими компетентними організаціями та установами;

11) забезпечення постійної взаємодії з підприємствами, які забезпечують централізоване водопостачання, централізоване водовідведення, постачання теплової енергії, енергопостачання, функціонування електронних комунікаційних мереж, транспортне обслуговування, медичну допомогу, безпеку та інші послуги, від яких залежить процес реагування на кризові ситуації та відновлення функціонування об’єктів критичної інфраструктури;

12) створення і використання необхідних резервів фінансових та матеріальних ресурсів для реагування на кризові ситуації та ліквідації їх наслідків;

13) проведення навчань та тренінгів, підготовка та перевірка персоналу, який відповідає за охорону, безпеку та захист об’єктів критичної інфраструктури;

14) захист інформації про системи управління, зв’язку, фізичну безпеку та кібербезпеку, забезпечення відповідно до встановлених законодавством вимог конфіденційності інформації під час оброблення даних про об’єкти критичної інфраструктури;

15) забезпечення захисту персоналу об’єктів критичної інфраструктури, організація та здійснення евакуаційних заходів у разі виникнення надзвичайних ситуацій.

2. Оператори критичної інфраструктури забезпечують розроблення та затвердження у встановленому законодавством порядку:

1) вимог щодо організації захисту об’єктів критичної інфраструктури;

2) посадових інструкцій осіб, відповідальних за організацію та забезпечення захисту об’єктів критичної інфраструктури;

3) проведення навчань та тренінгів, підготовку та перевірку персоналу, який відповідає за охорону, безпеку та захист об’єктів критичної інфраструктури;

4) паспортів безпеки об’єктів критичної інфраструктури.

3. Оператори критичної інфраструктури мають право:

1) отримувати в установленому порядку від уповноважених органів державної влади інформацію про забезпечення безпеки об’єктів критичної інфраструктури;

2) самостійно розробляти заходи щодо забезпечення безпеки об’єктів критичної інфраструктури, що не суперечать вимогам цього Закону та прийнятих відповідно до нього нормативно-правових актів;

3) отримувати від уповноваженого органу у сфері захисту критичної інфраструктури України консультації щодо застосування законодавства у сфері захисту критичної інфраструктури та вжиття необхідних заходів для захисту критичної інфраструктури.

4. Оператори критичної інфраструктури зобов’язані:

1) забезпечити захист об’єктів критичної інфраструктури;

2) невідкладно поінформувати відповідальних суб’єктів національної системи захисту критичної інфраструктури (секторальні та функціональні органи) про інциденти, що сталися на об’єктах критичної інфраструктури, які належать їм на праві власності або на іншій законній підставі;

3) завчасно, але не менше ніж за 30 календарних днів до дати зміни стану об’єкта критичної інфраструктури або його частини, інформувати уповноважений орган у сфері захисту критичної інфраструктури України про наміри змінити цільове призначення, режим функціонування чи намір передати права на об’єкт критичної інфраструктури та виконувати надані їм висновки та рекомендації;

4) щороку надавати інформацію про виконання повноважень відповідно до цього Закону за формою, визначеною Кабінетом Міністрів України.

**Розділ V**

**ОРГАНІЗАЦІЙНІ ЗАСАДИ НАЦІОНАЛЬНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ**

**Стаття 22.** Планування заходів щодо забезпечення стійкості та захисту об’єктів критичної інфраструктури

1. Для організації функціонування національної системи захисту критичної інфраструктури Кабінетом Міністрів України, центральними органами виконавчої влади, місцевими органами виконавчої влади (військово-цивільними адміністраціями - у разі створення), органами місцевого самоврядування розробляються та затверджуються відповідні плани та програми реагування на кризові ситуації.

Кабінет Міністрів України встановлює вимоги щодо управління ризиками безпеки на об’єктах критичної інфраструктури I категорії критичності, крім банків, інших осіб, які здійснюють діяльність на ринках фінансових послуг, платіжних організацій, учасників платіжних систем, операторів послуг платіжної інфраструктури, державне регулювання, нагляд за діяльністю яких здійснює Національний банк України, та встановлює вимоги щодо управління ризиками безпеки.

2. На державному рівні розробляється Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури, який затверджується Кабінетом Міністрів України.

3. На секторальному (галузевому) та регіональному рівнях органи державної влади розробляють і затверджують галузеві, регіональні плани та програми з протидії загрозам критичній інфраструктурі, включаючи аварійні плани, плани реагування на кризові ситуації, плани взаємодії, плани відновлення об’єктів критичної інфраструктури, плани проведення навчань та тренувань.

4. Національна поліція України, Національна гвардія України, Служба безпеки України, Збройні Сили України, Державна служба України з питань надзвичайних ситуацій та інші складові сектору безпеки і оборони у межах компетенції здійснюють планування відповідних заходів із захисту критичної інфраструктури.

5. На місцевому рівні: місцеві органи виконавчої влади (військово-цивільні адміністрації - у разі утворення), органи місцевого самоврядування забезпечують розроблення, затвердження і виконання місцевих програм підвищення стійкості територіальних громад до кризових ситуацій, викликаних припиненням надання чи погіршенням якості важливих для їх життєдіяльності послуг або припиненням здійснення життєво важливих функцій. Такі програми включають заходи із забезпечення безпеки та стійкості критичної інфраструктури, взаємодії суб’єктів національної системи захисту критичної інфраструктури, а також відновлення функціонування об’єктів критичної інфраструктури.

6. На об’єктовому рівні: оператори критичної інфраструктури на кожному об’єкті критичної інфраструктури розробляють та забезпечують виконання об’єктового плану заходів щодо захисту і забезпечення стійкості критичної інфраструктури, який включає заходи з фізичного захисту, протидії загрозам, ефективного зниження та контролю за ризиками безпеки, забезпечення безпеки інформації та кібербезпеки на об’єктах критичної інфраструктури.

7. Плани та програми, затверджені відповідно до цієї статті, є обов’язковими до виконання всіма суб’єктами національної системи захисту критичної інфраструктури.

**Стаття 23.** Здійснення моніторингу рівня безпеки об’єктів критичної інфраструктури

1. Моніторинг рівня безпеки об’єктів критичної інфраструктури здійснюється шляхом проведення оцінки стану захищеності об’єктів критичної інфраструктури.

Оцінка стану захищеності об’єктів критичної інфраструктури проводиться секторальними та функціональними органами у сфері захисту критичної інфраструктури відповідно до їх повноважень, визначених законом.

2. Метою здійснення моніторингу є встановлення відповідності стану захищеності об’єкта критичної інфраструктури вимогам законодавства, достовірності наданої інформації визначеним суб’єктам національної системи захисту критичної інфраструктури, надання методичної допомоги операторам об’єктів критичної інфраструктури в удосконаленні системи захисту критичної інфраструктури.

3. За результатами проведення моніторингу рівня безпеки готуються пропозиції щодо удосконалення системи захисту об’єктів критичної інфраструктури, оцінки стану безпеки об’єктів критичної інфраструктури секторальними та функціональними органами у сфері захисту критичної інфраструктури. Пропозиції щодо удосконалення системи захисту об’єктів критичної інфраструктури, підготовлені за результатами моніторингу оцінки стану захищеності, є інформацією з обмеженим доступом.

4. Порядок здійснення моніторингу оцінки стану безпеки об’єктів критичної інфраструктури та його періодичність затверджуються Кабінетом Міністрів України.

**Стаття 24.** Взаємодія національної системи захисту критичної інфраструктури з іншими системами захисту у сфері національної безпеки

1. Для забезпечення безпеки і стійкості критичної інфраструктури до загроз усіх видів, реалізації національних інтересів, функціонування суспільства та забезпечення соціально-економічного розвитку національна система захисту критичної інфраструктури взаємодіє з іншими системами захисту у сфері національної безпеки:

1) з єдиною державною системою запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків, з територіальною та функціональною підсистемами, структурними підрозділами суб’єктів боротьби з тероризмом;

2) з національною системою захисту інформаційних ресурсів в інформаційно-телекомунікаційних системах;

3) з національною системою кібербезпеки;

4) з правоохоронними органами у сфері протидії злочинності, а також з контррозвідувальними та розвідувальними органами у сфері забезпечення державної безпеки;

5) з об’єднаною цивільно-військовою системою організації повітряного руху України;

6) з єдиною державною системою цивільного захисту;

7) з державною системою фізичного захисту з питань охорони і оборони важливих державних об’єктів, захищеності та охорони ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання державної власності, запобігання диверсіям, крадіжкам або будь-якому іншому неправомірному вилученню радіоактивних матеріалів, протидії незаконному використанню безпілотних літальних апаратів;

8) із системою захисту персональних даних.

2. Взаємодія між державними системами захисту здійснюється у разі загрози виникнення або виникнення:

1) протиправних дій (у тому числі із застосуванням безпілотних літальних апаратів), захоплення об’єктів критичної інфраструктури або важливих державних об’єктів, що загрожують безпеці громадян і порушують функціонування систем життєзабезпечення;

2) диверсій, терористичних актів, викрадення, навмисного знищення, пошкодження майна та інших дій на об’єктах критичної інфраструктури, важливих державних об’єктах, внаслідок яких загинули люди або заподіяно значну матеріальну шкоду;

3) масштабних кібератак, актів кібертероризму проти систем управління, операційних та інших систем об’єктів критичної інфраструктури;

4) надзвичайних ситуацій або інших небезпечних подій на об’єктах критичної інфраструктури та важливих державних об’єктах;

5) аварій та технічних збоїв, кризових ситуацій на об’єктах критичної інфраструктури, що створюють загрозу життю та здоров’ю персоналу таких об’єктів та місцевого населення.

3. Організація взаємодії між суб’єктами національної системи захисту критичної інфраструктури здійснюється шляхом:

1) оперативного обміну інформацією щодо виконання завдань із захисту критичної інфраструктури;

2) проведення спільних оперативних нарад керівного складу уповноваженого органу у сфері захисту критичної інфраструктури України, центральних та територіальних органів Національної поліції України, Служби безпеки України, Національної гвардії України, Збройних Сил України, Державної служби України з питань надзвичайних ситуацій та інших заінтересованих державних органів;

3) здійснення спільних заходів із захисту критичної інфраструктури за планами, що розробляються на загальнодержавному, галузевому, регіональному місцевому та об’єктовому рівнях;

4) проведення спільних командно-штабних, тактико-спеціальних навчань, спільних тренувань та занять із захисту, охорони, оборони, припинення злочинних дій, інцидентів та кібератак проти об’єктів критичної інформаційної інфраструктури;

5) регулярного уточнення розрахунків сил та засобів, що залучаються до спільного виконання завдань із захисту об’єктів критичної інфраструктури та важливих державних об’єктів;

6) спільних заходів з припинення протиправних дій проти об’єктів критичної інфраструктури або важливих державних об’єктів, що загрожують безпеці громадян і порушують функціонування таких об’єктів;

7) участі у реагуванні та ліквідації наслідків інцидентів, кризових ситуацій на об’єктах критичної інфраструктури;

8) координації дій з підтримання або відновлення правопорядку в місцях розташування об’єктів критичної інфраструктури у разі виникнення кризових ситуацій;

9) здійснення інших заходів, передбачених законодавством.

**Стаття 25.** Державно-приватне партнерство у сфері захисту критичної інфраструктури

1. Державно-приватне партнерство у сфері захисту критичної інфраструктури здійснюється шляхом:

1) обміну інформацією між державними органами, місцевими органами виконавчої влади (військово-цивільними адміністраціями - у разі утворення), органами місцевого самоврядування, операторами критичної інфраструктури, громадськими об’єднаннями, організаціями роботодавців, а також громадянами щодо загроз критичній інфраструктурі та реагування на кризові ситуації;

2) визначення повноважень та відповідальності державних органів і операторів критичної інфраструктури у сфері забезпечення безпеки та стійкості критичної інфраструктури;

3) визначення порядку взаємодії між державними органами та операторами критичної інфраструктури у різних режимах функціонування об’єктів критичної інфраструктури;

4) створення системи підготовки кадрів для сфери захисту критичної інфраструктури;

5) підвищення комплексних знань, навичок і умінь персоналу та керівного складу операторів критичної інфраструктури, персоналу суб’єктів господарювання, які провадять діяльність, пов’язану із забезпеченням безпеки об’єктів критичної інфраструктури, з питань реагування на кризові ситуації на таких об’єктах;

6) залучення експертного потенціалу наукових установ, професійних та громадських об’єднань до підготовки галузевих проектів та нормативно-правових актів у сфері захисту критичної інфраструктури;

7) залучення до виконання завдань із забезпечення сталого функціонування об’єктів критичної інфраструктури суб’єктів господарювання, які провадять діяльність, пов’язану із забезпеченням безпеки об’єктів критичної інфраструктури, громадських об’єднань та професійних організацій;

8) надання державними органами консультативної та практичної допомоги операторам критичної інфраструктури з питань реагування на кризові ситуації на об’єктах критичної інфраструктури;

9) організації забезпечення захисту персоналу об’єктів критичної інфраструктури від можливих загроз;

10) забезпечення резервування основних ресурсів для функціонування критичної інфраструктури у різних режимах;

11) організації системи оповіщення населення та суб’єктів господарювання про інциденти та кризові ситуації на об’єктах критичної інфраструктури;

12) створення системи самооцінки віднесення об’єктів критичної інфраструктури за критеріями, визначеними цим Законом, створення інформаційних ресурсів для підвищення рівня знань із захисту об’єктів критичної інфраструктури;

13) створення механізмів для саморегулювання, обміну інформацією між операторами об’єктів критичної інфраструктури у певному секторі;

14) створення та підтримки розвитку систем сертифікації та оцінки відповідності у секторах критичної інфраструктури.

2. Державно-приватне партнерство у сфері захисту критичної інфраструктури здійснюється з урахуванням установлених законодавством особливостей правового режиму щодо окремих об’єктів критичної інфраструктури та окремих видів діяльності.

3. З метою забезпечення ефективної взаємодії представників громадськості, органів виконавчої влади та реального сектору економіки у формуванні та реалізації єдиної державної політики у сферах забезпечення захисту національних інтересів України у кіберпросторі та захисту об’єктів критичної інфраструктури можуть створюватися консультативно-дорадчі органи, об’єднання та мережі у порядку, встановленому законодавством.

**Стаття 26.** Проведення незалежного аудиту діяльності національної системи захисту критичної інфраструктури

1. Незалежна зовнішня оцінка діяльності уповноваженого органу у сфері захисту критичної інфраструктури України здійснюється шляхом проведення щорічного зовнішнього аудиту його діяльності. Зовнішній аудит діяльності уповноваженого органу у сфері захисту критичної інфраструктури України проводиться Рахунковою палатою.

2. Незалежна зовнішня оцінка діяльності національної системи захисту критичної інфраструктури здійснюється один раз на три роки Рахунковою палатою у визначеному нею порядку на підставі міжнародних стандартів оцінки.

3. Форма та зміст звіту про зовнішній аудит діяльності уповноваженого органу у сфері захисту критичної інфраструктури України затверджуються Кабінетом Міністрів України з урахуванням вимог цього Закону.

4. Відшкодування витрат, пов’язаних із проведенням щорічного зовнішнього аудиту, здійснюється за рахунок Державного бюджету України.

**Стаття 27.** Парламентський контроль у сфері захисту критичної інфраструктури

1. Контроль за дотриманням законодавства при здійсненні заходів із забезпечення захисту критичної інфраструктури здійснюється Верховною Радою України в порядку, визначеному Конституцією України. Комітет Верховної Ради України, до предмета відання якого належать питання національної безпеки і оборони, та комітет Верховної Ради України, до предмета відання якого належать питання кібербезпеки об’єктів критичної інформаційної інфраструктури, на своїх засіданнях розглядають звіт уповноваженого органу у сфері захисту критичної інфраструктури України про результати незалежного аудиту діяльності щодо ефективності системи забезпечення захисту критичної інфраструктури.

2. За результатами розгляду звіту уповноваженого органу у сфері захисту критичної інфраструктури України комітет Верховної Ради України, до предмета відання якого належать питання національної безпеки і оборони, може порушити питання про розгляд цих питань Верховною Радою України.

**Стаття 28.** Громадський нагляд у сфері захисту критичної інфраструктури

1. Право громадського нагляду у сфері захисту критичної інфраструктури реалізується громадянами України через громадські об’єднання, членами яких вони є, через депутатів місцевих рад, особисто шляхом звернення до Уповноваженого Верховної Ради України з прав людини або до державних органів у порядку, встановленому Конституцією України, Законом України "Про громадські об’єднання" та іншими законами України, участі у діяльності громадських рад при органах, що формують та забезпечують реалізацію державної політики у сфері забезпечення захисту критичної інфраструктури, проведення незалежного аудиту їх діяльності, право доступу до публічної частини звіту щодо забезпечення захисту об’єктів критичної інфраструктури.

2. Доступ до інформації у сфері захисту критичної інфраструктури для реалізації громадського нагляду здійснюється у порядку, передбаченому Законом України "Про доступ до публічної інформації", та може бути обмежений виключно Законом України "Про державну таємницю".

**Стаття 29.** Відповідальність за порушення законодавства у сфері захисту критичної інфраструктури

1. Особи, винні у порушенні законодавства у сфері захисту критичної інфраструктури, несуть відповідальність згідно із законом.

**Стаття 30.** Фінансування заходів у сфері захисту критичної інфраструктури

1. Джерелами фінансування робіт і заходів із забезпечення захисту критичної інфраструктури є кошти державного і місцевих бюджетів, власні кошти операторів критичної інфраструктури, кредити банків, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством.

**Стаття 31.** 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 з міжнародними організаціями, які здійснюють боротьбу з міжнародною злочинністю та тероризмом.

2. Україна відповідно до міжнародних договорів, згода на обов’язковість яких надана Верховною Радою України, може брати участь у спільних заходах із забезпечення захисту критичної інфраструктури, зокрема у проведенні спільних навчань суб’єктів сектору безпеки і оборони в рамках заходів колективної оборони з дотриманням вимог законів України "Про порядок направлення підрозділів Збройних Сил України до інших держав" та "Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України".

3. Відповідно до законодавства у сфері зовнішніх зносин суб’єкти національної системи захисту критичної інфраструктури у межах своїх повноважень здійснюють міжнародну співпрацю безпосередньо на двосторонній або багатосторонній основі.

**Стаття 32.** Страхування ризиків

1. Оператор критичної інфраструктури зобов’язаний забезпечити страхування ризику настання кризової ситуації.

2. Перелік об’єктів критичної інфраструктури, включених до Реєстру, страхових ризиків настання кризової ситуації на таких об’єктах, які підлягають страхуванню, а також мінімальний ліміт відповідальності (у разі страхування відповідальності перед третіми особами) затверджуються Кабінетом Міністрів України, а щодо об’єктів критичної інфраструктури у сфері фінансових послуг - погоджуються з Національним банком України.

**ЗАТВЕРДЖЕНО**  
**постановою Кабінету Міністрів України**  
**від 9 жовтня 2020 р. № 1109**

**ПОРЯДОК**  
**віднесення об’єктів до критичної інфраструктури**

1. Цей Порядок визначає механізм віднесення об’єктів до критичної інфраструктури та їх категоризації.

Дія цього Порядку не поширюється на:

банки, інші об’єкти, що провадять діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, платіжні організації, учасників платіжних систем, операторів послуг платіжної інфраструктури, віднесення яких до критичної інфраструктури здійснюється в порядку, встановленому Національним банком;

об’єкти, що провадять діяльність на ринках послуг, державне регулювання та нагляд за діяльністю яких здійснюють державні органи, віднесення яких до критичної інфраструктури здійснюється в порядку, встановленому такими державними органами.

2. Терміни в цьому Порядку вживаються у значенні, наведеному в [Законі України](https://zakon.rada.gov.ua/laws/show/1882-20) “Про критичну інфраструктуру”.

3. Категорії критичності об’єктів критичної інфраструктури установлюються відповідно до [частини другої](https://zakon.rada.gov.ua/laws/show/1882-20#n120) статті 10 Закону України “Про критичну інфраструктуру”.

4. Секторальні органи у сфері захисту критичної інфраструктури, використовуючи перелік секторів критичної інфраструктури, ідентифікують об’єкти критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури.

5. Секторальні органи у сфері захисту критичної інфраструктури разом із оператором критичної інфраструктури здійснюють категоризацію об’єктів критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури відповідно до [Методики категоризації об’єктів критичної інфраструктури](https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF/print#n45), затвердженої постановою Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 “Деякі питання об’єктів критичної інфраструктури” (Офіційний вісник України, 2020 р., № 93, ст. 2994), подають інформацію до реєстру об’єктів критичної інфраструктури.

6. Відомості про об’єкти критичної інфраструктури, що віднесені до I, II, III і IV категорії критичності, вносяться секторальними органами у сфері захисту критичної інфраструктури до секторальних переліків об’єктів критичної інфраструктури, які ними складаються та ведуться.

7. Секторальні органи у сфері захисту критичної інфраструктури складають переліки всіх об’єктів критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури, що віднесені до I, II, III і IV категорії критичності.

Cекторальні органи подають уповноваженому органу з питань захисту критичної інфраструктури переліки об’єктів критичної інфраструктури для формування зведеного переліку об’єктів критичної інфраструктури, що затверджується Кабінетом Міністрів України.

Секторальні органи у сфері захисту критичної інфраструктури подають оновлені відомості про об’єкти критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури до зведеного переліку об’єктів критичної інфраструктури щомісяця та протягом одного місяця в разі:

зміни оператора або найменування об’єкта критичної інфраструктури;

зміни категорії критичності об’єкта критичної інфраструктури;

ліквідації (перетворення, знищення, припинення) об’єкта критичної інфраструктури.

Уповноважений орган з питань захисту критичної інфраструктури має право витребувати документи, на підставі яких було прийнято рішення щодо категоризації об’єктів критичної інфраструктури. У разі невідповідності наданих документів законодавству у сфері захисту критичної інфраструктури уповноважений орган з питань захисту критичної інфраструктури здійснює формування зведеного переліку об’єктів критичної інфраструктури без урахування таких об’єктів.

Уповноважений орган з питань захисту критичної інфраструктури має право ініціювати здійснення повторної категоризації секторальним органом об’єкта критичної інфраструктури.

8. Відомості про об’єкти критичної інфраструктури, що містяться у зведеному переліку об’єктів критичної інфраструктури та секторальних переліках об’єктів критичної інфраструктури, є інформацією з обмеженим доступом, захист якої забезпечується відповідно до вимог законодавства.

{Порядок в редакції Постанови КМ [№ 1384 від 16.12.2022](https://zakon.rada.gov.ua/laws/show/1384-2022-%D0%BF#n16)}

|  |  |
| --- | --- |
|  | **ЗАТВЕРДЖЕНО** **постановою Кабінету Міністрів України** **від 9 жовтня 2020 р. № 1109** **(в редакції постанови Кабінету Міністрів України** [**від 16 грудня 2022 р. № 1384**](https://zakon.rada.gov.ua/laws/show/1384-2022-%D0%BF#n37)**)** |

**ПЕРЕЛІК**  
**секторів критичної інфраструктури**

|  |  |  |  |
| --- | --- | --- | --- |
| Сектор | Підсектор | Тип основної послуги | Секторальний орган у сфері захисту критичної інфраструктури |
| Паливно-енергетичний сектор | електро-енергетика | виробництво електричної енергії  забезпечення функціонування ринку електричної енергії, організація купівлі-продажу електричної енергії на ринку | Міненерго |
|  |  |  |
|  |  | управління системами передачі та енергопостачання |  |
|  |  | розподіл електричної енергії |  |
|  | вугільно-промисловий комплекс | видобуток вугілля для генерації електроенергії на теплоелектростанціях та теплоелектро-централях |  |
|  |  | зберігання та постачання вугілля |  |
|  | торфодобування | розробка родовищ торфу |  |
|  |  | видобування корисних копалин |  |
|  | нафтова промисловість | видобуток нафти |  |
|  | передача (транзит) нафти та нафтопродуктів |  |
|  |  | очищення, переробка та обробка нафти |  |
|  |  | експлуатація нафтопроводів |  |
|  |  | зберігання та постачання нафти та нафтопродуктів |  |
|  | газова промисловість | видобуток газу |  |
|  | переробка та очищення газу |  |
|  |  | передача (транзит) газу |  |
|  |  | розподіл газу |  |
|  |  | забезпечення роботи систем зрідження природного газу |  |
|  |  | експлуатація газотранспортної системи |  |
|  |  | зберігання природного газу |  |
|  |  | забезпечення роботи систем зрідження природного газу |  |
|  | ядерна енергетика | виробництво ядерного палива |  |
|  |  | експлуатація ядерних підкритичних установок, ядерних реакторів, які включають критичні та підкритичні збірки дослідницьких реакторів |  |
|  |  | експлуатація атомних електростанцій, підприємств і установок по збагаченню та переробці палива, а також сховищ відпрацьованого палива |  |
| Цифрові технології | електронні довірчі послуги та електронна ідентифікація | надання електронних довірчих послуг, електронної ідентифікації та автентифікації | Мінцифри |
|  |  | забезпечення функцій центрального засвідчувального органу |  |
|  | електронні комунікації | адміністрування адресного простору українського сегмента Інтернету |  |
|  | електронне урядування | забезпечення функціонування системи електронної взаємодії органів виконавчої влади |  |
|  |  | забезпечення функціонування системи міжвідомчої взаємодії між органами державної влади, органами місцевого самоврядування та суб’єктами господарювання |  |
|  |  | надання електронних публічних послуг |  |
|  |  | автоматизація процесів надання адміністративних послуг |  |
|  |  | забезпечення функціонування правового режиму Дія Сіті |  |
| Захист інформації |  | надання послуг (сервісів) кіберзахисту | Держспецзв’язку |
| Системи життєзабезпечення | комунальні послуги | постачання теплової енергії | Мінрегіон |
|  |  | постачання гарячої води |  |
|  |  | централізоване питне водопостачання |  |
|  |  | централізоване водовідведення |  |
|  |  | поводження з побутовими відходами |  |
| Харчова промисловість та агропромисловий комплекс |  | виробництво та переробка сільськогосподарської та/або харчової продукції | Мінагрополітики |
|  | виробництво ветеринарних препаратів |  |
|  | експлуатація елеваторів |  |
|  | експлуатація зрошувальних систем, каналів |  |
| Державний матеріальний резерв |  | забезпечення зберігання запасів державного матеріального резерву | Мінекономіки |
| Охорона здоров’я | медична допомога | забезпечення надання екстреної медичної допомоги | МОЗ |
|  |  | забезпечення надання первинної медичної допомоги |  |
|  |  | забезпечення надання вторинної (спеціалізованої) медичної допомоги |  |
|  |  | забезпечення надання третинної (високоспеціалізованої) медичної допомоги |  |
|  |  | забезпечення надання паліативної медичної допомоги |  |
|  |  | забезпечення надання реабілітації у сфері охорони здоров’я |  |
|  | громадське здоров’я | заготівля і тестування донорської крові та компонентів крові |  |
|  |  | контроль за інфекційними захворюваннями та/або епідеміями |  |
|  | фінансове забезпечення у сфері охорони здоров’я | оплата згідно з тарифом за надані пацієнтам медичні послуги (включаючи медичні вироби) та лікарські засоби за договорами про медичне обслуговування населення за програмою медичних гарантій |  |
|  | інформаційні технології у сфері охорони здоров’я | функціонування електронної системи охорони здоров’я |  |
|  | фармацевтична промисловість | виробництво та постачання лікарських засобів і медичних виробів |  |
|  | медична наука | наукові дослідження в медичній галузі |  |
| Ринки капіталу та організовані товарні ринки |  | забезпечення функціонування ринків капіталів та організованих товарних ринків | НКЦПФР |
| Фінансовий сектор |  | планування, виконання та моніторинг виконання бюджетів | Мінфін |
|  |  | розрахунково-касове обслуговування розпорядників та одержувачів бюджетних коштів |  |
|  |  | здійснення контролю за надходженням до бюджетів та державних цільових фондів податків, зборів, платежів |  |
| Транспорт і пошта | авіаційний транспорт | управління повітряним рухом | Мінінфраструктури |
|  |  | авіаперевезення (робота авіаційного транспорту) |  |
|  |  | забезпечення роботи аеропортів та допоміжного обладнання, що розташоване в аеропортах |  |
|  | автомобільний та міський електротранспорт, у тому числі метрополітен | автобусні перевезення (міжміські, міжнародні) |  |
|  | міські перевезення (автобуси, трамваї, тролейбуси, метрополітен) |  |
|  |  | технічне обслуговування транспортної інфраструктури (доріг, мостів, тунелів, шляхопроводів) |  |
|  |  | служби контролю трафіку |  |
|  |  | функціонування інтелектуальних транспортних систем (управління рухом, мобільністю, взаємодія з іншими видами транспорту) |  |
|  | залізничний транспорт | пасажирські залізничні перевезення |  |
|  |  | вантажні залізничні перевезення |  |
|  |  | експлуатація та технічне обслуговування залізниці |  |
|  |  | забезпечення роботи вокзалів та вузлових станцій |  |
|  | морський та річковий транспорт | контроль і управління судноплавством |  |
|  | операції на внутрішньому, морському або прибережному пасажирському та вантажному транспорті |  |
|  |  | функціонування керуючих органів портів або суб’єктів експлуатації портового обладнання |  |
|  |  | експлуатація та обслуговування інфраструктури (каналів, дамб, фарватерів тощо) |  |
|  |  | регулювання руху суден |  |
|  |  | лоцманське проведення суден |  |
|  | поштовий зв’язок | надання послуг поштового зв’язку |  |
| Промисловість | хімічна промисловість | виробництво промислового газу | Мінстратегпром |
|  |  | виробництво добрив або азотистих сполук |  |
|  |  | виробництво пестицидів або інших агрохімічних продуктів |  |
|  |  | виробництво вибухових речовин |  |
|  |  | виробництво основних органічних хімічних речовин |  |
|  |  | виробництво основних неорганічних речовин |  |
|  | металургійна промисловість | гірничо-металургійний комплекс (металургійне виробництво та добування залізних руд) |  |
|  |  | виробництво коксу та коксопродуктів |  |
|  | оборонна промисловість | розробка, виробництво, модернізація та утилізація продукції військового призначення (оборонно-промисловий комплекс) |  |
|  | космічна промисловість | виробництво та постачання космічної техніки |  |
|  |  | космічна діяльність, космічні технології та послуги |  |
|  | авіаційна промисловість | виробництво та постачання продукції авіаційної промисловості |  |
|  | суднобудівна промисловість | суднобудування та постачання продукції суднобудування |  |
| Сектор громадської безпеки | громадська безпека | охорона публічного (громадського) порядку, фізичний захист критичної інфраструктури | МВС |
|  | екстрена допомога населенню за єдиним телефонним номером 112 | надання екстреної допомоги населенню за єдиним телефонним номером 112 |  |
| Цивільний захист населення і територій | служби порятунку (атестовані аварійно-рятувальні служби згідно із законодавством) | реагування на надзвичайні ситуації, проведення аварійно-рятувальних та інших невідкладних робіт з ліквідації наслідків надзвичайних ситуацій, надання допомоги постраждалим |  |
| Міграція (імміграція та еміграція) |  | оформлення документів, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус |  |
| Охорона навколишнього природного середовища | управління, використання та відтворення поверхневих водних ресурсів, розвиток водного господарства | забезпечення задоволення потреб населення і галузей економіки у водних ресурсах | Міндовкілля |
|  | проектування, будівництво і реконструкція систем захисту від шкідливої дії вод, групових і локальних водопроводів, систем водопостачання та каналізації у сільській місцевості, гідротехнічних споруд, водогосподарських об’єктів багатоцільового використання |  |
|  |  | захист від підтоплення захисних масивів, протипаводковий і протиповеневий захист |  |
|  | поводження з радіоактивними відходами | довгострокове зберігання і захоронення радіоактивних відходів |  |
|  | охорона, раціональне використання і відтворення об’єктів природно-заповідного фонду | охорона, раціональне використання земель та надр |  |
|  | охорона, раціональне використання і відтворення об’єктів природно-заповідного фонду |  |
|  | ведення лісового і мисливського господарства |  |
|  |  | поводження з відходами, небезпечними хімічними речовинами, пестицидами та агрохімікатами |  |
|  |  | створення, дослідження та практичне використання генетично модифікованих організмів у відкритій системі |  |
| Сектор оборони |  | оборона | Міноборони |
|  | зберігання боєприпасів | забезпечення зберігання боєприпасів, вибухових речовин |  |
|  | виробництво боєприпасів | виробництво ракет, боєприпасів, вибухових речовин |  |
| Національна безпека |  | захист національної державності | СБУ |
|  |  | охорона державної таємниці |  |
|  |  | боротьба з тероризмом |  |
| Правосуддя |  | здійснення правосуддя | ДСА |
| Тримання під вартою |  | тримання засуджених та осіб, взятих під варту, в установах виконання покарань та слідчих ізоляторах Державної кримінально-виконавчої служби | Мін’юст |
|  |  |  |
| Наукові дослідження та розробки | дослідницька інфраструктура наукових установ та закладів вищої освіти | наукова діяльність | МОН |
| надання послуг з використання наукового обладнання (у тому числі інструментів, приладів, інвентарю) |  |
|  |  |
|  |  | дослідницька діяльність |  |
| Фінансовий сектор | банківська система | надання банківських послуг | Національний банк |
|  |  | зберігання банками запасів готівки Національного банку та проведення операцій із ними |  |
|  | ринок небанківських фінансових послуг (крім ринків капіталу та організованих товарних ринків) | надання електронних довірчих послуг у банківській системі |  |
|  | надання небанківських фінансових послуг |  |
|  | ринок платіжних послуг | надання платіжних послуг |  |
| Вибори та референдуми |  | організація підготовки та проведення виборів та референдумів | Центральна виборча комісія |
| Соціальний захист | пенсійне забезпечення | забезпечення пенсійних виплат | Мінсоцполітики |
|  | соціальне страхування | надання матеріального забезпечення і страхових виплат |  |
|  | соціальна допомога і соціальні послуги | забезпечення соціальних виплат та надання соціальних послуг |  |
|  | інформаційна система соціальної сфери | надання адміністративних послуг соціального характеру в електронній формі |  |
| Інформаційні послуги | засоби масової інформації | надання послуг у сфері телебачення та радіомовлення | МКІП |
|  |  | надання послуг в інформаційній та видавничій сферах |  |
| Державна влада та місцеве самоврядування |  | виконання функцій держави | Держспецзв’язку |
|  |  | виконання функцій місцевого самоврядування |  |

*{*

|  |  |
| --- | --- |
|  | **ЗАТВЕРДЖЕНО** **постановою Кабінету Міністрів України** **від 9 жовтня 2020 р. № 1109** |

**МЕТОДИКА**  
**категоризації об’єктів критичної інфраструктури**

1. Ця Методика визначає механізм та критерії віднесення об’єкта критичної інфраструктури до однієї з категорій критичності.

Дія цієї Методики не поширюється на:

{Пункт 1 доповнено абзацом згідно з Постановою КМ [№ 1384 від 16.12.2022](https://zakon.rada.gov.ua/laws/show/1384-2022-%D0%BF#n40)}

банківську та фінансову системи, категоризація об’єктів критичної інфраструктури яких здійснюється відповідно до методики, затвердженої Національним банком;

сфери, державне регулювання та нагляд за діяльністю яких здійснюють державні органи, категоризація об’єктів критичної інфраструктури яких здійснюється відповідно до методики, затвердженої такими державними органами.

2. У цій Методиці під терміном “час відновлення” розуміється час, що необхідний для відновлення функціонування об’єкта критичної інфраструктури у частині надання основних послуг у штатному режимі після виникнення кризової ситуації, пошкодження або знищення об’єкта.

Інші терміни вживаються у значенні, наведеному в [Законі України](https://zakon.rada.gov.ua/laws/show/1882-20) “Про критичну інфраструктуру”.

3. Категорія критичності об’єкта критичної інфраструктури визначається на основі аналізу рівня негативного впливу, якого особа, суспільство, навколишнє природне середовище, економіка, національна безпека та обороноздатність країни можуть зазнати внаслідок порушення або припинення функціонування об’єкта інфраструктури відповідно до критеріїв, зазначених у [додатках 1](https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF/print#n91) і [2](https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF/print#n94).

4. Категорія об’єкта критичної інфраструктури визначається за такою процедурою:

1) секторальний орган у сфері захисту критичної інфраструктури ідентифікує всі об’єкти критичної інфраструктури свого сектору (підсектору) критичної інфраструктури згідно з [Порядком віднесення об’єктів до критичної інфраструктури](https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF/print#n11), затвердженим постановою Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 “Деякі питання об’єктів критичної інфраструктури” (Офіційний вісник України, 2020 р., № 93, ст. 2994), - в редакції постанови Кабінету Міністрів України від 16 грудня 2022 р. № 1384;

2) секторальний орган у сфері захисту критичної інфраструктури відповідно до [Порядку віднесення об’єктів до критичної інфраструктури](https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF/print#n11) для кожного об’єкта свого сектору (підсектору) критичної інфраструктури визначає, які основні послуги надає цей об’єкт;

3) секторальний орган у сфері захисту критичної інфраструктури разом із оператором критичної інфраструктури проводить оцінку критичності об’єкта критичної інфраструктури, використовуючи секторальні та міжсекторальні критерії визначення рівня негативного впливу, наведені у [додатках 1](https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF/print#n91) і [2](https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF/print#n94), які враховують:

рівень негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури;

соціальну значущість об’єкта критичної інфраструктури;

суспільну значущість об’єкта критичної інфраструктури;

економічну значущість об’єкта критичної інфраструктури;

наявність взаємозв’язків між об’єктами критичної інфраструктури;

значущість об’єкта критичної інфраструктури для забезпечення національної безпеки та обороноздатності країни;

4) під час заповнення форми [додатка 1](https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF/print#n91) обирається рівень негативного впливу в рамках сектору або підсектору об’єкта критичної інфраструктури та у графі “Оцінка РКi” виставляється бал, який відповідає рівню негативного впливу, опис якого характеризує наслідки, які можуть настати у разі порушення функціонування об’єкта критичної інфраструктури;

5) під час заповнення форми [додатка 2](https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF/print#n94) обирається рівень негативного впливу за кожним критерієм, наведеним у формі, та у графі “Оцінка РКi” виставляється бал, який відповідає рівню негативного впливу, опис якого характеризує наслідки, які можуть настати у разі порушення функціонування об’єкта критичної інфраструктури;

6) підсумовуються всі бали, що були отримані під час оцінки об’єкта критичної інфраструктури згідно з формами, наведеними в [додатках 1](https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF/print#n91) і [2](https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF/print#n94);

7) розраховується узагальнена нормована оцінка рівня критичності за такою формулою:



|  |
| --- |
| де РКОКІ - узагальнена нормована оцінка рівня критичності об’єкта критичної інфраструктури;   - сума балів, які отримав об’єкт критичної інфраструктури за всіма критеріями критичності ([додатки 1](https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF/print#n91) і [2](https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF/print#n94));   - максимальна можлива сума балів (розраховується виходячи з того, що об’єкт отримує максимальні бали за всіма критеріями оцінки рівня негативного впливу). |
| Примітка. У цій Методиці залежно від сектору використовується 17 або 18 критеріїв. Тому для об’єктів критичної інфраструктури, що належать до секторів критичної інфраструктури за пунктами 1, 3-7 [додатка 1](https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF/print#n91), максимальна можлива сума балів буде дорівнювати  = 18 × 4 = 72 балів, для об’єктів критичної інфраструктури, що належать до секторів за пунктами 2, 8-13 додатка 1, максимальна можлива сума балів буде дорівнювати  = 17 × 4 = 68 балів. |

8) рішення щодо категорії критичності об’єкта критичної інфраструктури приймається на основі узагальненої нормованої оцінки рівня критичності об’єкта критичної інфраструктури відповідно до такого правила:

I категорія критичності, якщо 0,8 < PKOKI ≤ 1;

II категорія критичності, якщо 0,63 < PKOKI ≤ 0,8;

III категорія критичності, якщо 0,37 < PKOKI ≤ 0,63;

IV категорія критичності, якщо 0,2 < PKOKI ≤ 0,37;

об’єкт не є критичним, якщо PKOKI ≤ 0,2;

9) відомості про об’єкти критичної інфраструктури, що віднесені до I, II, III і IV категорії критичності, секторальний орган у сфері захисту критичної інфраструктури подає уповноваженому органу у сфері захисту критичної інфраструктури для формування зведеного переліку об’єктів критичної інфраструктури;

{Підпункт 9 пункту 4 в редакції Постанови КМ [№ 1384 від 16.12.2022](https://zakon.rada.gov.ua/laws/show/1384-2022-%D0%BF#n51)}

10) відомості про об’єкти критичної інфраструктури, що віднесені до I, II, III і IV категорії критичності, вносяться до секторального переліку об’єктів критичної інфраструктури, який формується та ведеться секторальним органом у сфері захисту критичної інфраструктури у відповідному секторі (підсекторі).

{Підпункт 10 пункту 4 в редакції Постанови КМ [№ 1384 від 16.12.2022](https://zakon.rada.gov.ua/laws/show/1384-2022-%D0%BF#n51)}

5. [Методичні рекомендації щодо категоризації об’єкта критичної інфраструктури](https://zakon.rada.gov.ua/laws/show/v0023519-21#n10) затверджує Адміністрація Держспецзв’язку.

|  |  |
| --- | --- |
|  | Додаток 1 до Методики |

**ВИЗНАЧЕННЯ РІВНЯ**  
**негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури (секторальні критерії)**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Сектор/підсектор | | Фактор негативного впливу в секторі/підсекторі | Рівень негативного впливу: катастрофічні наслідки (4 бали) | Рівень негативного впливу: критичні наслідки (3 бали) | Рівень негативного впливу: значні наслідки (2 бал) | Рівень негативного впливу: незначні наслідки (1 бал) | Оцінка |
| 1. | Послуги, що надаються підсектором електроенергетики та підсектором ядерної енергетики | у разі знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури припиниться електропостачання | для більш як 145 000 жителів або для споживачів I категорії на території більш як однієї області або на території не менш як трьох міст обласного значення | для більш як 30 000 жителів або для споживачів II категорії на території однієї області або на території більш як одного району міста - обласного центру, або на всій території одного міста обласного значення | для більш як 2000 жителів | для менш як 2000 жителів |  |
| час відновлення функціонування у штатному режимі не може перевищувати 6 годин | час відновлення функціонування у штатному режимі може становити від 6 до 24 годин | час відновлення функціонування у штатному режимі може становити від однієї до трьох діб | час відновлення функціонування у штатному режимі може бути більше трьох діб |
| 2. | Послуги, що надаються підсектором нафти та нафтопродуктів | у разі знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури зменшиться постачання нафти та нафтопродуктів для споживання на внутрішньому ринку України | більш як на 25 відсотків відносно аналогічного періоду календарного року чи попереднього календарного місяця | від 12 до 25 відсотків відносно аналогічного періоду календарного року чи попереднього календарного місяця | від 7 до 12 відсотків відносно аналогічного періоду календарного року чи попереднього календарного місяця | менш як на 7 відсотків відносно аналогічного періоду календарного року чи попереднього календарного місяця |  |
| 3. | Послуги, що надаються підсектором постачання газу | у разі знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури припиниться постачання газу | для більш як 145 000 жителів або для споживачів з безперервною подачею газу на території більш як однієї області або на території не менш як трьох міст обласного значення | для більш як 20 000 жителів на території однієї області або на території більш як одного району міста - обласного центру, або на всій території одного міста обласного значення | для більш як 5000 жителів | для менш як 5000 жителів |  |
| час відновлення функціонування у штатному режимі не може перевищувати 6 годин | час відновлення функціонування у штатному режимі може становити від 6 до 24 годин | час відновлення функціонування у штатному режимі від однієї до трьох діб | час відновлення функціонування у штатному режимі може бути більше трьох діб |
| 4. | Послуги, що надаються інформаційним сектором | у разі знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури припиниться або порушиться надання основних послуг об’єктом | для більш як 145 000 жителів на території більш як однієї області або на території не менш як трьох міст обласного значення | для більш як 20 000 жителів на території однієї області або на території більш як одного району міста - обласного центру, або на всій території одного міста обласного значення | для більш як 2000 жителів | для менше як 2000 жителів |  |
|  |
| час відновлення функціонування у штатному режимі не може перевищувати 6 годин | час відновлення функціонування у штатному режимі може становити від 6 до 24 годин | час відновлення функціонування у штатному режимі може становити від однієї до трьох діб | час відновлення функціонування у штатному режимі може бути більше трьох діб |  |
| 5. | Послуги постачання теплової енергії та гарячої води | у разі знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури постачання теплової енергії та/або гарячої води буде перервано (під час опалювального сезону) | для більш як 145 000 жителів або на території більш як однієї області або не менш як трьох міст обласного значення | для більш як 30000 жителів або на території більш як одного району міста - обласного центру, або на всій території одного міста обласного значення | для більш як 2000 жителів | для менш як 2000 жителів |  |  |
| час відновлення функціонування у штатному режимі не може перевищувати 24 годин | час відновлення функціонування у штатному режимі може становити від доби до трьох діб | час відновлення функціонування у штатному режимі може становити від трьох діб | не застосовується |  |
| 6. | Послуги централізованого водопостачання | у разі знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури буде припинено централізоване водопостачання | для більш як 145 000 жителів або на території більш як однієї області, або не менш як трьох міст обласного значення | для більш як 30000 жителів або стаціонарним лікувальним закладам, будинкам соціальної допомоги, установам, що надають послуги освіти на території області або більш як одного району міста - обласного центру, або на всій території одного міста обласного значення | для більш як 2000 жителів | для менш як 2000 жителів |  |  |
| час відновлення функціонування у штатному режимі не може перевищувати 24 годин (час кризової ситуації не може перевищувати 24 годин) | час відновлення функціонування у штатному режимі може становити від доби до трьох діб (час кризової ситуації може становити від доби до трьох діб) | час відновлення функціонування у штатному режимі може становити від трьох діб (час кризової ситуації може становити більше трьох діб) | не застосовується |  |
| 7. | Послуги централізованого водовідведення | у разі знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури буде припинено централізоване водовідведення та очищення стічних вод | для більш як 145 000 жителів або на території обласного центру, або не менш як трьох міст обласного значення | для більш як 30 000 жителів або на території одного міського району обласного центру, або на всій території одного міста обласного значення | для більш як 2000 жителів | для менше як 2000 жителів |  |  |
| час відновлення функціонування у штатному режимі не може перевищувати 24 годин (час кризової ситуації не може перевищувати 24 годин) | час відновлення функціонування у штатному режимі може становити від доби до трьох діб (час кризової ситуації може становити від доби до трьох діб) | час відновлення функціонування у штатному режимі може становити від трьох діб (час кризової ситуації може становити від доби до трьох діб) | не застосовується |  |
| 8. | Послуги поводження побутовими відходами | у разі знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури буде припинено збір, зберігання, безпечна переробка (утилізація) побутових відходів | для більш як 145 000 жителів або на території обласного центру, або не менш як трьох міст обласного значення | для більш як 30 000 жителів або на території одного міського району обласного центру, або на всій території одного міста обласного значення | не застосовується | не застосовується |  |  |
| 9. | Послуги, що надаються підсектором авіаційного транспорту | знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури | наслідком є неможливість надання послуг з перевезення пасажирів та вантажів авіаційним транспортом хоча б одним із стратегічно важливих аеропортів України протягом більш як 24 години без можливості організації альтернативного способу надання послуг | наслідком є неможливість надання послуг з перевезення пасажирів та вантажів авіаційним транспортом хоча б одним із стратегічно важливих аеропортів України протягом більш як 24 години, при цьому зберігається можливість організації альтернативного способу надання послуги | наслідком є припинення повітряного руху на час відновлення штатного режиму функціонування | не застосовується |  |  |
| 10. | Послуги, що надаються підсектором автомобільного транспорту | знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури | наслідком є блокування (припинення) дорожнього руху на міжнародних та національних дорогах протягом більш як на 24 години та якщо немає обхідного шляху або немає можливості його відновлення протягом не більш як 24 години | наслідком є блокування (припинення) дорожнього руху на міжнародних та національних дорогах протягом не більш як на 24 години та якщо немає обхідного шляху | наслідком є блокування (припинення) дорожнього руху на регіональних дорогах протягом не більш як на 48 годин та якщо немає обхідного шляху або немає можливості його відновлення протягом не більш як 48 годин | наслідком є блокування (припинення) дорожнього руху на регіональних дорогах протягом не більш як на 48 годин та якщо немає обхідного шляху |  |  |
| 11. | Послуги, що надаються підсектором залізничного транспорту | знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури | наслідком є припинення залізничного руху більш як на 24 години на залізничних магістральних лініях I (I-П, І-ПС) та II категорії (категорію залізничної лінії визначено відповідно до ДБН В.2.3-19-2018) | наслідком є припинення залізничного руху більш як на 24 години на залізничних магістральних лініях III категорії | наслідком є припинення залізничного руху більш як на 24 години на залізничних магістральних лініях IV категорії | наслідком є припинення залізничного руху більш як на 24 години на залізничних магістральних лініях V категорії |  |  |
| 12. | Послуги, що надаються підсектором морського та річного транспорту | знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури | наслідком є припинення надання морських послуг у морських портах більш як на 72 години ([Правила надання послуг у морських портах України](https://zakon.rada.gov.ua/laws/show/z1401-13#n15), затверджені наказом Мінінфраструктури від 5 червня 2013 р. № 348) | наслідком є припинення надання морських послуг у морських портах від 24 до 72 годин | наслідком є припинення надання морських послуг у морських портах до 24 годин | не застосовується |  |  |
| 13. | Послуги, що надаються поштовим підсектором | у разі знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури буде припинено надання послуг поштового зв’язку | для більш як 145 000 жителів на території більш як однієї області або більш як трьох міст обласного значення | для більш як 20 000 жителів на території області або більше одного району міста - обласного центру, або на всій території одного міста обласного значення | для більш як 6000 жителів | для менш як 6000 жителів |  |  |
| 14. | Послуги, що надаються фінансовим сектором | знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури призведе до ненадання об’єктом основних послуг | для більш як 100 000 клієнтів | для більш як 50 000 клієнтів | для більш як 10 000 клієнтів | не застосовується |  |  |
| 15. | Послуги, що надаються сектором харчової промисловості та агропромислового комплексу, сектором охорони навколишнього природного середовища, сектором охорони здоров’я, сектором промисловості, сектором цивільного захисту населення та територій | знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури призведе до ненадання об’єктом основних послуг | для більш як 145 000 жителів на території більш як однієї області або не менш як трьох міст обласного значення | для більш як 30 000 жителів на території області або більш як одного району міста - обласного центру, або на всій території одного міста обласного значення | для більш як 6000 жителів | для менш як 6000 жителів |  |  |
| \_\_\_\_\_\_\_\_\_\_ Усього | |  |  |  |  |  |  |  |

|  |  |
| --- | --- |
|  | Додаток 2 до Методики |

**ВИЗНАЧЕННЯ РІВНЯ**  
**негативного впливу у разі знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури (міжсекторальні критерії)**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Негативний вплив | | | Рівень негативного впливу: катастрофічні наслідки (4 бали) | Рівень негативного впливу: критичні наслідки (3 бали) | Рівень негативного впливу: значні наслідки (2 бал) | Рівень негативного впливу: незначні наслідки (1 бал) | Рівень негативного впливу: надто малий (0 балів) | Оцінка РКі | |
| I. Соціальна значущість об’єкта критичної інфраструктури | | | | | | | | | |
| 1. | Заподіяння шкоди життю та здоров’ю людей | | Кількість населення, що може постраждати | | | | | | |
| небезпека для життя або здоров’я більш як 75 000 людей | небезпека для життя та здоров’я більш як 5000 людей | небезпека для життя або здоров’я більш як 50 людей | небезпека для життя або здоров’я менш як 50 людей | не критично | РК**1** = | |
| Географічний масштаб | | | | | | |
| небезпека для життя та здоров’я мешканців на території однієї або більш як однієї області, або на території трьох та більше міст обласного значення | небезпека для життя та здоров’я мешканців на території однієї області або міського району міста обласного центру, або на всій території одного міста обласного значення | небезпека для життя та здоров’я для людей на території об’єкта та для мешканців, що проживають у безпосередній близькості до розміщення об’єкта | небезпека для життя та здоров’я людей на території об’єкта | не критично | РК**2** = | |
| 2. | Заподіяння шкоди навколишньому природному середовищу | | Економічні втрати | | | | | | |
| нанесені збитки більш як 30 млн. гривень | нанесені збитки більш як 18 млн. гривень | нанесені збитки більш як 2 млн. гривень | нанесені збитки менш як на 2 млн. гривень | не критично | РК**3** = | |
| Географічний масштаб | | | | | | |
| шкідливий вплив розповсюджується на територію більш як однієї області або на території не менш як трьох міст обласного значення | шкідливий вплив розповсюджується на територію однієї області або на територію більш як одного міста обласного значення | шкідливий вплив розповсюджується на територію одного міста обласного значення | шкідливий вплив розповсюджується на територію об’єкта інфраструктури | не критично | РК**4** = | |
| Час | | | | | | |
| шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом більш як одного року | шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом від півроку до одного року | шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом від одного місяця до півроку | шкідливий вплив на навколишнє природне середовище та безпечні умови життя зберігається протягом одного місяця | не критично | РК**5** = | |
| II. Суспільна значущість об’єкта критичної інфраструктури | | | | | | | | | |
| 3. | Припинення або порушення функціонування державних органів | | припинення або порушення функціонування Верховної Ради України, Кабінету Міністрів України, Конституційного Суду України, Верховного Суду, а також Офісу Президента України, Ради національної безпеки та оборони України | припинення або порушення функціонування центральних органів виконавчої влади та облдержадміністрацій | припинення або порушення роботи районних держадміністрацій, територіальних органів центральних органів виконавчої влади | припинення або порушення роботи органів місцевого самоврядування | не критично | РК**6** = | |
| 4. | Негативний вплив на довіру людей до державних інституцій | | матиме значний вплив | матиме великий вплив | матиме середній вплив | матиме незначний вплив | не критично | РК**7** = | |
| 5. | Шкода інтересам інших держав - партнерів України | | так, принаймні двом країнам або порушення умов міжнародного договору, укладеного від імені України | так, принаймні одній країні або порушення умов міжнародного договору, укладеного від імені Уряду України | можливі негативні наслідки для інших держав, але їх вплив навряд чи буде значним | держави не постраждають або не має місце порушення умов міжнародного договору, укладеного від імені міністерства, іншого центрального органу виконавчої влади, державного органу | не критично | РК**8** = | |
| III. Економічна значущість об’єкта критичної інфраструктури | | | | | | | | | |
| 6. | Заподіяння збитків об’єкту інфраструктури (у відсотках прогнозованого обсягу річного доходу за всіма видами діяльності) | більш як 15 відсотків | | від 10 до 15 відсотків | від 5 до 10 відсотків | менш як 5 відсотків | не критично | РК**9** = | |
| 7. | Заподіяння збитків державному бюджету (зниження прибутків бюджету у відсотках прогнозованого річного прибутку бюджету) | більш як 0,1 відсотка | | від 0,1 до 0,05 відсотка | від 0,05 до 0,01 відсотка | менш як 0,01 відсотка | не критично | РК**10** = | |
| 8. | Заподіяння збитків місцевим бюджетам (зниження прибутків бюджету у відсотках прогнозованого річного прибутку бюджету) | більш як 0,1 відсотка | | від 0,1 до 0,05 відсотка | від 0,05 до 0,01 відсотка | менш як 0,01 відсотка | не критично | РК**11** = | |
| IV. Взаємозв’язок між об’єктами критичної інфраструктури | | | | | | | | | |
| 9. | Негативний вплив на безперервне та стійке функціонування іншого об’єкта інфраструктури, що забезпечує надання таких самих основних послуг | матиме негативний вплив (якщо так, вкажіть який) | |  |  | не матиме впливу | не критично | РК**12** = | |
| 10. | Негативний вплив на безперервне та стійке функціонування іншого об’єкта інфраструктури, що надає інші основні послуги | матиме негативний вплив (якщо так, вкажіть який) | |  |  | не матиме впливу | не критично | РК**13** = | |
| V. Значущість об’єкта критичної інфраструктури для забезпечення національної безпеки та обороноздатності країни | | | | | | | | | |
| 11. | Припинення або порушення (невиконання встановлених показників) функціонування пунктів управління (ситуаційного центру), що оцінюється в рівні (значущості) пункту управління або ситуаційного центру | припинення або порушення функціонування пунктів управління Верховного Головнокомандувача Збройних Сил, Головнокомандувача Збройних Сил, Начальника Генерального штабу Збройних Сил або ситуаційного центру Офісу Президента України, Кабінету Міністрів України, Ради національної безпеки та оборони України | | припинення або порушення функціонування пунктів управління або ситуаційного центру центральних органів виконавчої влади, пунктів управління Сухопутних військ, Повітряних Сил, Військово-Морських Сил, десантно-штурмових військ, сил спеціальних операцій, Національної гвардії, Держприкордонслужби | припинення або порушення функціонування обласної державної адміністрації, ситуаційних центрів | територіальних органів центральних органів виконавчої влади | не критично | РК**14** = | |
| 12. | Зниження показників державного оборонного замовлення | Зниження обсягів продукції (робіт, послуг) в заданий період часу (у відсотках) | | | | | | | |
| більш як 15 відсотків | | від 10 до 15 відсотків | від 5 до 10 відсотків | менше як 5 відсотків | не критично | РК**15** = | |
| Збільшення часу виготовлення продукції (робіт, послуг) із заданим обсягом (відсотків встановленого часу на виготовлення продукції) | | | | | | | |
| більш як 40 відсотків | | від 10 до 40 відсотків | від 5 до 10 відсотків | менш як 5 відсотків | не критично | РК**16** = | |
| \_\_\_\_\_\_\_\_\_\_ Усього | |  | |  |  |  |  |  |  |

# 

|  |  |
| --- | --- |
|  | **ЗАТВЕРДЖЕНО** **постановою Кабінету Міністрів України** **від 28 квітня 2023 р. № 415** |

**ПОРЯДОК**  
**ведення Реєстру об’єктів критичної інфраструктури, включення таких об’єктів до Реєстру, доступу та надання інформації з нього**

1. Цей Порядок визначає процедури формування і ведення Реєстру об’єктів критичної інфраструктури (далі - Реєстр), включення об’єктів критичної інфраструктури до Реєстру, внесення до нього інформації про об’єкти критичної інфраструктури та їх виключення, доступу та надання інформації з Реєстру.

2. У цьому Порядку під терміном “власник об’єкта критичної інфраструктури” розуміється юридична особа будь-якої форми власності або фізична особа - підприємець, якій на праві власності належить об’єкт критичної інфраструктури.

Інші терміни вживаються у значенні, наведеному у Законах України “Про інформацію”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про основні засади забезпечення кібербезпеки України”, “Про доступ до публічної інформації”, “Про критичну інфраструктуру”, “Про публічні електронні реєстри”, “Про електронні довірчі послуги”.

3. Реєстр ведеться з метою:

узгодження дій суб’єктів національної системи захисту критичної інфраструктури, які приймаються на національному рівні;

функціонування системи обміну інформацією між суб’єктами національної системи захисту критичної інфраструктури;

здійснення оцінки захищеності об’єктів критичної інфраструктури;

створення бази даних щодо загроз і вразливостей критичній інфраструктурі;

підготовки та надання уповноваженим органом у сфері захисту критичної інфраструктури України висновків/рекомендацій власнику/оператору критичної інфраструктури;

забезпечення паспортизації та захисту об’єктів критичної інфраструктури;

проведення аналізу інформації, яка обробляється в Реєстрі.

4. Реєстр забезпечує включення, оброблення, виключення, захист, відображення та надання інформації про найбільш важливу для життєдіяльності суспільства та держави критичну інфраструктуру, щодо якої встановлюються особливі вимоги із забезпечення її безпеки та стійкості, здійснюється моніторинг їх дотримання.

Власником Реєстру є держава в особі уповноваженого органу у сфері захисту критичної інфраструктури України.

5. Держателем та адміністратором Реєстру є уповноважений орган у сфері захисту критичної інфраструктури України, який здійснює облік, узагальнення, систематизацію, аналіз та надання інформації, яка подається секторальним органом, включення об’єкта критичної інфраструктури до Реєстру, внесення інформації про об’єкт до Реєстру та/або виключення інформації з Реєстру, внесення змін до відомостей, що містяться в Реєстрі, здійснює інші повноваження, пов’язані з веденням Реєстру для забезпечення його функціонування.

6. Користувачами Реєстру є суб’єкти національної системи захисту критичної інфраструктури.

Посадовим/службовим особам суб’єктів національної системи захисту критичної інфраструктури у зв’язку із здійсненням ними повноважень, передбачених Законом України “Про критичну інфраструктуру”, інформація з Реєстру надається за суб’єктом права чи за об’єктом критичної інфраструктури в електронній формі шляхом безпосереднього доступу до Реєстру за умови ідентифікації відповідної посадової/службової особи відповідно до вимог Закон України “Про електронні довірчі послуги”.

7. Реєстр формується і ведеться уповноваженим органом у сфері захисту критичної інфраструктури України.

8. Обробка інформації в Реєстрі здійснюється відповідно до вимог Законів України “Про захист інформації в інформаційно-комунікаційних системах”, “Про захист персональних даних”, “Про основні засади забезпечення кібербезпеки України”, “Про державну таємницю”.

9. Інформація, що міститься в Реєстрі, є державним інформаційним ресурсом. Інформація про об’єкти критичної інфраструктури, що міститься в Реєстрі, є відкритою, загальнодоступною та безоплатною, крім інформації з обмеженим доступом.

10. Реєстр ведеться в електронній формі. Мовою ведення Реєстру є державна мова.

11. До Реєстру вносяться відомості про:

секторальний орган, який подає інформацію;

оператора критичної інфраструктури;

документ, на підставі якого ідентифіковано та категоризовано об’єкт критичної інфраструктури;

об’єкт критичної інфраструктури;

погодження (перегляд) паспорта безпеки на об’єкт критичної інфраструктури.

12. До відкритої інформації у Реєстрі віднесена інформація про:

секторальний орган, який подав інформацію до Реєстру;

найменування (прізвище, власне ім’я, по батькові (за наявності), місцезнаходження (адреса) та код згідно з ЄДРПОУ (РНОКПП - за наявності) оператора критичної інфраструктури, форму власності, країну реєстрації, КВЕД основної діяльності;

кінцевого бенефіціарного власника/контролера;

реєстровий номер об’єкта критичної інфраструктури;

дату внесення інформації про об’єкт критичної інфраструктури до Реєстру вперше.

13. До інформації з обмеженим доступом у Реєстрі віднесена інформація про об’єкт критичної інфраструктури, а саме:

назва об’єкта критичної інфраструктури;

категорія критичності;

дата останнього оновлення інформації про об’єкт критичної інфраструктури в Реєстрі;

дата затвердження паспорта безпеки на об’єкт критичної інфраструктури;

адреса місцезнаходження об’єкта критичної інфраструктури, кадастровий (кадастрові) номер (номери);

найменування (прізвище, власне ім’я, по батькові (за наявності), місцезнаходження (адреса) та код згідно з ЄДРПОУ (РНОКПП - за наявності) власника об’єкта критичної інфраструктури/суб’єкта управління об’єкта критичної інфраструктури, форма власності, країна реєстрації/громадянство власника об’єкта критичної інфраструктури;

сектор, підсектор, тип основної послуги, життєво важлива функція та/або послуга, яку надає об’єкт критичної інфраструктури, КВЕД;

назва секторального органу, який погодив (переглянув) паспорт безпеки на об’єкт критичної інфраструктури;

дата погодження (перегляду) паспорта безпеки на об’єкт критичної інфраструктури;

дата погодження функціональними органами планів захисту від загроз критичній інфраструктурі;

відомості про особу, відповідальну за організацію та забезпечення захисту об’єкта критичної інфраструктури;

додаткові відомості щодо об’єкта критичної інфраструктури для внесення до Реєстру.

14. Уповноважений орган у сфері захисту критичної інфраструктури України забезпечує цілодобовий доступ до відкритої інформації на своєму офіційному веб-сайті.

15. Кожному об’єкту критичної інфраструктури присвоюється реєстровий номер, відкривається новий розділ та формується реєстраційна справа у Реєстрі.

Реєстровим номером об’єкта критичної інфраструктури є унікальний реєстровий номер, який присвоюється кожному індивідуально визначеному об’єкту критичної інфраструктури під час реєстрації вперше, не повторюється на всій території України, залишається незмінним протягом усього часу існування такого об’єкта критичної інфраструктури та не змінюється у разі зміни оператора критичної інфраструктури, форми власності, кінцевого бенефіціарного власника/контролера.

16. З моменту присвоєння об’єкту критичної інфраструктури унікального реєстрового номера в Реєстрі він вважається таким, що набув правового статусу об’єкта критичної інфраструктури.

17. Секторальні органи (створювачі) подають окремо про кожен об’єкт критичної інфраструктури повідомлення про внесення відомостей щодо об’єкта критичної інфраструктури до Реєстру за формою згідно з додатком 1 та додатки до нього в електронній формі з дотриманням вимог Законів України “Про електронні документи та електронний документообіг”, “Про електронні довірчі послуги”, “Про захист інформації в інформаційно-комунікаційних системах” або у паперовій формі.

В електронній формі повідомлення про внесення відомостей щодо об’єкта критичної інфраструктури до Реєстру подається із застосуванням електронних довірчих послуг відповідно до статті 17 Закону України “Про електронні довірчі послуги”.

Повідомлення про внесення відомостей щодо об’єкта критичної інфраструктури до Реєстру подається у паперовій формі з дотриманням законодавства у сфері захисту інформації.

До повідомлення про внесення відомостей щодо об’єкта критичної інфраструктури до Реєстру додаються документи, що обґрунтовують розрахунок віднесення об’єкта критичної інфраструктури до однієї з категорій критичності, здійснений відповідно до Методики категоризації об’єктів критичної інфраструктури, затвердженої постановою Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 “Деякі питання об’єктів критичної інфраструктури” (далі - Методика) (Офіційний вісник України, 2020 р., № 93, ст. 2994).Інформація про об’єкт критичної інфраструктури подається у місячний строк з моменту внесення об’єкта критичної інфраструктури до секторального переліку об’єктів критичної інфраструктури.

18. Підставою для внесення інформації до Реєстру є повідомлення про внесення відомостей щодо об’єкта критичної інфраструктури до Реєстру, яке подає секторальний орган.

Інформація до Реєстру вноситься відповідальною особою уповноваженого органу у сфері захисту критичної інфраструктури України за результатами перевірки повноти інформації, зазначеної в повідомленні про внесення відомостей щодо об’єкта критичної інфраструктури до Реєстру, обґрунтованості визначення категорії критичності об’єкта відповідно до Методики, про що повідомляється секторальному органу, який подав таке повідомлення.

Інформація вноситься до Реєстру відповідальною особою уповноваженого органу у сфері захисту критичної інфраструктури України протягом 30 днів з дня надходження повідомлення про внесення відомостей щодо об’єкта критичної інфраструктури до Реєстру.

У разі неповноти інформації, невідповідності визначення категорії критичності об’єкта критичної інфраструктури відповідно до Методики уповноважений орган у сфері захисту критичної інфраструктури України повертає подані документи до секторального органу.Після усунення невідповідностей, доповнення інформації або приведення у відповідність з категоріями критичності секторальний орган повторно подає уповноваженому органу у сфері захисту критичної інфраструктури України повідомлення про внесення відомостей щодо об’єкта критичної інфраструктури до Реєстру.

19. Зміни і додаткові відомості про об’єкт критичної інфраструктури до Реєстру вносяться уповноваженим органом у сфері захисту критичної інфраструктури України та фіксуються програмними засобами Реєстру на підставі повідомлення про погодження (перегляд) паспорта безпеки на об’єкт критичної інфраструктури за формою згідно з додатком 2 та/або повідомлення про внесення змін до відомостей щодо об’єкта критичної інфраструктури за формою згідно з додатком 3.

Інформація про моніторинг безпеки, перевірку та оцінку стану захищеності об’єкта критичної інфраструктури та їх результати вносяться до Реєстру уповноваженим органом у сфері захисту критичної інфраструктури України на підставі акта оцінки стану захищеності об’єкта критичної інфраструктури, складеного відповідно до Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 22 липня 2022 р. № 821 (Офіційний вісник України, 2022 р., № 60, ст. 3599).

20. Секторальний орган протягом 10 робочих днів з дня отримання інформації від оператора критичної інфраструктури про внесення змін до відомостей щодо об’єкта критичної інфраструктури подає уповноваженому органу у сфері захисту критичної інфраструктури України повідомлення про внесення змін до відомостей щодо об’єкта критичної інфраструктури в порядку, визначеному пунктом 17 цього Порядку.

21. Об’єкт критичної інфраструктури виключається з Реєстру у зв’язку з невідповідністю такого об’єкта критеріям віднесення його до критичної інфраструктури.

Об’єкт критичної інфраструктури виключається з Реєстру на підставі повідомлення про внесення змін до відомостей щодо об’єкта критичної інфраструктури за формою згідно з додатком 3, в якій зазначаються відомості про об’єкт критичної інфраструктури, який виключається з Реєстру.

22. У разі допущення технічної помилки під час внесення відомостей до Реєстру відповідальна особа уповноваженого органу у сфері захисту критичної інфраструктури України самостійно її виправляє та повідомляє секторальному органу протягом 10 робочих днів з дня виявлення такої технічної помилки.23. Фінансування створення, ведення та функціонування Реєстру здійснюється за рахунок коштів міжнародної технічної та/або поворотної або безповоротної фінансової допомоги міжнародних організацій та інших джерел, не заборонених законодавством.

24. Відповідальність за достовірність, своєчасність та повноту інформації, поданої уповноваженому органу у сфері захисту критичної інфраструктури України для внесення до Реєстру, несе секторальний орган.

**ЗАТВЕРДЖЕНО**  
**постановою Кабінету Міністрів України**  
**від 4 серпня 2023 р. № 818**

**ПОРЯДОК**  
**розроблення та погодження паспорта безпеки на об’єкт критичної інфраструктури**

1. Цей Порядок визначає вимоги до розроблення оператором критичної інфраструктури паспорта безпеки на об’єкт критичної інфраструктури (далі - паспорт безпеки) та його складових, а також механізм його погодження секторальними і функціональними органами у сфері захисту критичної інфраструктури.

Відомості, що містяться в паспорті безпеки та його складових, є інформацією з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Обробка інформації, що міститься в паспорті безпеки, його складових та інших документах, які містять інформацію з обмеженим доступом, що створюється під час розроблення і погодження такого паспорта та його складових, проводиться відповідно до Законів України “Про доступ до публічної інформації” і “Про державну таємницю”, Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затвердженого постановою Кабінету Міністрів України від 18 грудня 2013 р. № 939, Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затвердженої постановою Кабінету Міністрів України від 19 жовтня 2016 р. № 736 (Офіційний вісник України, 2016 р., № 85, ст. 2783), та цього Порядку.

Факсимільне відтворення підпису керівника оператора критичної інфраструктури, функціонального чи секторального органу або особи, що його заміщає, за допомогою засобів механічного або іншого копіювання на зазначених документах не допускається.

2. У цьому Порядку терміни вживаються в такому значенні:

власник об’єкта критичної інфраструктури - юридична особа будь-якої форми власності або фізична особа - підприємець, якій на правах власності або іншого речового права (господарського відання, оперативного управління) належить об’єкт критичної інфраструктури;

критичні елементи об’єкта критичної інфраструктури - технічні засоби та/або споруди, системи та/або їх сукупність, порушення у функціонуванні яких призведе до унеможливлення виконання життєво важливих функцій та/або надання послуг об’єктом критичної інфраструктури;

план захисту об’єкта критичної інфраструктури (далі - план захисту) - документ, що передбачає заходи із забезпечення безпеки об’єкта критичної інфраструктури та протидії проектним загрозам відповідно до режимів його функціонування.

Інші терміни вживаються у значенні, наведеному в Законах України “Про критичну інфраструктуру”, “Про основні засади забезпечення кібербезпеки України”, “Про інформацію”, “Про транспорт”.

3. Паспорт безпеки розробляється та затверджується оператором критичної інфраструктури (далі - оператор) на кожний об’єкт критичної інфраструктури.

Паспорт безпеки містить:

[титульний аркуш](https://zakon.rada.gov.ua/laws/show/818-2023-%D0%BF#n73), що оформлюється згідно з додатком 1;

загальну характеристику об’єкта критичної інфраструктури (далі - загальна характеристика);

плани захисту;

акти оцінки стану захищеності об’єкта критичної інфраструктури (далі - акти оцінки) (у разі наявності), складені за формою, визначеною в Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури, затвердженому постановою Кабінету Міністрів України від 22 липня 2022 р. № 821 (Офіційний вісник України, 2022 р., № 60, ст. 3599).

4. Загальна характеристика складається оператором за формою згідно з додатком 2 та підписується керівником оператора або особою, що його заміщає.

5. План захисту (як складову паспорта безпеки) розробляє оператор за кожною із проектних загроз національного, секторального та об’єктового (у разі наявності) рівня відповідно до форм планів захисту та рекомендацій з розроблення планів захисту, що затверджуються відповідними функціональними органами у сфері захисту критичної інфраструктури (далі - функціональний орган) щодо кожної проектної загрози.

Функціональні органи визначаються відповідно до проектних загроз.

6. Плани захисту підлягають обов’язковому погодженню відповідними функціональними органами, до яких, зокрема, належать МОЗ, Міноборони, Держспецзв’язку, ДСНС, Національна поліція.

У разі загрози диверсій, терористичних актів, актів кібертероризму проти систем управління, операційних та інших систем об’єктів критичної інфраструктури, надзвичайних ситуацій або інших небезпечних подій на об’єктах критичної інфраструктури, інцидентів, пов’язаних із порушеннями систем фізичної безпеки та кібербезпеки та інших проектних загроз національного, секторального та об’єктового (у разі наявності) рівня та потенційних негативних наслідків для об’єктів критичної інфраструктури плани захисту підлягають обов’язковому погодженню СБУ, Національною гвардією, іншими державними органами.

7. Для погодження плану захисту оператор подає функціональному органу такий план разом із супровідним листом і копією загальної характеристики.

Супровідний лист і план захисту підписує керівник оператора або особа, що його заміщає.

Плани захисту погоджуються у строк, що становить не більше як 10 робочих днів із дня їх реєстрації відповідними функціональними органами.

8. Функціональний орган перевіряє поданий оператором план захисту на відповідність вимогам до його розроблення, передбаченим пунктом 5 цього Порядку, а також щодо повноти відомостей і заходів із забезпечення безпеки та протидії відповідній проектній загрозі та їх ефективності.

У разі коли план захисту подано функціональному органу із порушенням вимог до його розроблення відповідно до форм планів захисту, передбачених пунктом 5 цього Порядку, що затверджуються відповідними функціональними органами, функціональний орган не пізніше ніж протягом двох робочих днів із дня реєстрації повертає його оператору разом із супровідним листом для приведення у відповідність із зазначеними вимогами.

У разі коли план захисту подано функціональному органу із порушенням вимог, передбачених пунктом 7 цього Порядку, функціональний орган відмовляє в реєстрації поданих документів і повертає їх (із зазначенням підстави повернення) для усунення оператором недоліків.

9. Свою позицію щодо плану захисту функціональний орган доводить до відома оператора шляхом надсилання листа, в якому зазначається інформація про погодження плану захисту без зауважень або про наявність зауважень (пропозицій) до плану захисту.

У разі відсутності зауважень (пропозицій) до плану захисту функціональний орган додає до такого листа погоджений ним план захисту та повертає інші документи, подані оператором разом із планом захисту.

Погодження плану захисту оформлюється шляхом проставлення на титульному аркуші відмітки про його погодження. Відмітка робиться функціональним органом шляхом проставлення грифа погодження, який містить у собі слово “ПОГОДЖЕНО”, найменування посади особи та функціонального органу, яким погоджується план захисту, особистий підпис, скріплений гербовою печаткою (за наявності), власне ім’я, прізвище і дату.

У разі наявності зауважень (пропозицій) до плану захисту функціональний орган повертає його оператору разом із супровідним листом, в якому доводить до відома оператора такі зауваження (пропозиції), а також повертає інші документи, подані оператором разом із планом захисту.

Функціональний орган зобов’язаний обґрунтувати свою позицію щодо наданих зауважень (пропозицій) до плану захисту. Зауваження (пропозиції) надаються виключно з тих питань, що належать до компетенції функціонального органу. Зауваження (пропозиції) до плану захисту не можуть стосуватися порушення вимог до його розроблення відповідно до форм планів захисту, передбачених пунктом 5 цього Порядку, що затверджуються відповідними функціональними органами та редакційних уточнень щодо тексту плану захисту.

Оператор забезпечує ознайомлення з інформацією про погодження відповідного плану захисту всіх функціональних органів, що беруть участь у його погодженні, за їх відповідним запитом, зокрема із дотриманням встановлених правил роботи з документами, які містять інформацію з обмеженим доступом.

10. У разі коли в результаті врахування оператором зауважень (пропозицій) функціональних органів план захисту або окремі його положення, погоджені іншими функціональними органами, зазнали змін, що суттєво змінюють зміст, такий план захисту підлягає повторному погодженню відповідними функціональними органами.

Повторне погодження здійснюється із дотриманням вимог до розроблення та погодження плану захисту, передбачених пунктами 5-9 цього Порядку.

11. Зміна керівника оператора, функціонального органу, секторального органу у сфері захисту критичної інфраструктури (далі - секторальний орган) не потребує повторного погодження плану захисту та/або паспорта безпеки.

12. План захисту переглядається в разі:

перегляду проектних загроз національного, секторального та/або об’єктового (у разі наявності) рівня;

зміни відомостей, що містяться в загальній характеристиці;

надання пропозиції щодо удосконалення системи захисту об’єктів критичної інфраструктури, усунення порушень та/або недоліків (у разі їх наявності) в акті оцінки.

План захисту переглядається із дотриманням вимог до розроблення та погодження плану захисту, передбачених пунктами 5-11 цього Порядку, та з урахуванням особливостей, передбачених цим пунктом.

Зміна керівника оператора, функціонального органу, секторального органу не потребує перегляду плану захисту.

13. Розроблений та затверджений оператором паспорт безпеки підлягає обов’язковому погодженню відповідним секторальним органом.

Оператор подає на погодження до секторального органу паспорт безпеки, що містить титульний аркуш, загальну характеристику, погоджені плани захисту за кожною із проектних загроз, а також акти оцінки (у разі наявності) разом із супровідним листом за підписом керівника оператора або особи, що його заміщає.

Паспорт безпеки погоджується у строк, що становить не більш як 10 робочих днів із дня їх реєстрації відповідними секторальними органами.

14. Секторальний орган перевіряє паспорт безпеки на відповідність планів захисту проектним загрозам національного, секторального та об’єктового (у разі наявності) рівня, зокрема про наявність у паспорті безпеки такого плану щодо кожної проектної загрози, а також дотримання оператором вимог пунктів 3-6, 13 цього Порядку.

У разі коли паспорт безпеки подано секторальному органу із порушенням вимог до наявності в паспорті безпеки планів захисту щодо кожної проектної загрози та вимог, передбачених пунктами 4-6 цього Порядку, секторальний орган не пізніше ніж протягом двох робочих днів із дня реєстрації повертає його оператору разом із супровідним листом за підписом керівника секторального органу для приведення у відповідність із зазначеними вимогами.

У разі коли паспорт безпеки подано секторальному органу із порушенням вимог, передбачених пунктами 3 і 13 цього Порядку, секторальний орган відмовляє в реєстрації поданих документів і повертає їх (із зазначенням підстави повернення) для усунення оператором недоліків.

15. Свою позицію щодо паспорта безпеки керівник секторального органу доводить до відома оператора шляхом надсилання листа, в якому зазначається інформація про погодження паспорта безпеки без зауважень або про наявність зауважень (пропозицій) до паспорта безпеки.

У разі відсутності зауважень (пропозицій) до паспорта безпеки секторальний орган додає до такого листа погоджений ним паспорт безпеки та повертає інші документи, подані оператором разом із паспортом безпеки.

У разі наявності зауважень (пропозицій) до паспорта безпеки керівник секторального органу повертає його оператору разом із супровідним листом, в якому доводить до відома оператора такі зауваження (пропозиції), а також повертає інші документи, подані оператором разом із паспортом безпеки.

Секторальний орган зобов’язаний обґрунтувати свою позицію щодо наданих зауважень (пропозицій) до паспорта безпеки. Зауваження (пропозиції) до паспорта безпеки надаються виключно з тих питань, що належать до компетенції секторального органу.

Під час опрацювання отриманого на погодження паспорта безпеки уповноважена особа секторального органу використовує відомості державних реєстрів (кадастрів) та інших баз даних.

Зауваження (пропозиції) до паспорта безпеки не можуть стосуватися погодженого плану захисту, дотримання вимог до оформлення титульного аркуша, а також редакційних уточнень щодо їх текстів.

16. Паспорт безпеки переглядається в разі:

перегляду проектних загроз національного, секторального та/або об’єктового (у разі наявності) рівня;

зміни відомостей, що містяться в загальній характеристиці та планах захисту;

надання пропозиції щодо удосконалення системи захисту об’єктів критичної інфраструктури, усунення порушень та/або недоліків (у разі їх наявності) в акті оцінки.

Паспорт безпеки переглядається із дотриманням вимог до розроблення та погодження паспорта безпеки, передбачених пунктами 3-6 цього Порядку, та з урахуванням особливостей, передбачених цим пунктом.

Зміна керівника оператора, функціонального органу, секторального органу не потребує перегляду паспорта безпеки.

17. Після погодження паспорта безпеки секторальним органом формується та подається уповноваженому органу у сфері захисту критичної інфраструктури повідомлення про погодження (перегляд) паспорта безпеки за формою, визначеною в Порядку ведення Реєстру об’єктів критичної інфраструктури, включення таких об’єктів до Реєстру, доступу та надання інформації з нього, затвердженому постановою Кабінету Міністрів України від 28 квітня 2023 р. № 415 (Офіційний вісник України, 2023 р., № 47, ст. 2567).

18. Для визначення вимог до забезпечення захисту та стійкості секторів критичної інфраструктури паспорт безпеки подається оператором уповноваженому органу у сфері захисту критичної інфраструктури за його запитом протягом 10 робочих днів із дня реєстрації оператором такого запиту.

За результатами проведеної роботи уповноважений орган у сфері захисту критичної інфраструктури повертає паспорт безпеки оператору протягом 10 робочих днів із дня його отримання.

**ЗАТВЕРДЖЕНО**  
**постановою Кабінету Міністрів України**  
**від 14 жовтня 2022 р. № 1174**

**РЕГЛАМЕНТ**  
**обміну інформацією між суб’єктами національної системи захисту критичної інфраструктури**

1. Цей Регламент визначає механізм інформаційної взаємодії між суб’єктами національної системи захисту критичної інфраструктури з метою забезпечення захисту та стійкості критичної інфраструктури.

2. Терміни в цьому Регламенті вживаються у значенні, наведеному в Законі України «Про критичну інфраструктуру».

3. Інформаційна взаємодія забезпечується шляхом послідовного обміну інформацією між суб’єктами національної системи захисту критичної інфраструктури, що здійснюється відповідальними особами, визначеними такими суб’єктами, з використанням засобів електронних комунікацій, національної системи конфіденційного зв’язку, спеціального зв’язку, шифрувального зв’язку та інформаційно-комунікаційних систем.

4. У штатному режимі, режимі готовності та запобігання реалізації загроз, а також у режимі відновлення штатного функціонування обмін інформацією щодо функціонування об’єктів критичної інфраструктури здійснюється щодня з 10 год. 00 хв. до 11 год. 00 хв. шляхом інформування засобами зв’язку з одночасним письмовим інформуванням.

Обмін інформацією здійснюється послідовно між операторами критичної інфраструктури (далі - оператори) та секторальними органами у сфері захисту критичної інфраструктури (далі - секторальні органи), між секторальними органами та уповноваженим органом у сфері захисту критичної інфраструктури (далі - уповноважений орган).

5. У разі виникнення кризової ситуації на об’єктах критичної інфраструктури обмін інформацією здійснюється протягом 30 хвилин з моменту отримання операторами інформації про її виникнення.

Обмін інформацією здійснюється послідовно між операторами та секторальними органами, між секторальними органами та уповноваженим органом, а також між секторальними органами та Кабінетом Міністрів України.

Усне інформування протягом години підтверджується секторальними органами письмово шляхом надсилання повідомлення за формою згідно з додатком за допомогою шифрувального зв’язку або спеціальної інформаційної системи уповноваженому органу та Кабінетові Міністрів України.

6. У режимі реагування на виникнення кризової ситуації на об’єктах критичної інфраструктури (у разі виявлення, запобігання і нейтралізації загроз) обмін інформацією про хід ліквідації її наслідків здійснюється двічі на добу: не пізніше 11 год. 00 хв. та 18 год. 00 хвилин.

Обмін інформацією здійснюється послідовно між операторами та секторальними органами, між секторальними органами та уповноваженим органом, а також між уповноваженим органом та Кабінетом Міністрів України.

Періодичне інформування про хід ліквідації кризової ситуації на об’єктах критичної інфраструктури до повного відновлення їх штатного режиму здійснюється секторальними органами шляхом надсилання повідомлення за формою згідно з додатком за допомогою шифрувального зв’язку або спеціальної інформаційної системи уповноваженому органу.

Секторальний орган також щодня інформує Кабінет Міністрів України про хід та результати вжиття суб’єктами національної системи захисту критичної інфраструктури заходів щодо повернення параметрів функціонування об’єктів критичної інфраструктури I категорії критичності до штатного режиму, строки відновлення штатного функціонування та проблемні питання, що виникли під час вжиття таких заходів, обмеження щодо режимів роботи суміжних об’єктів інфраструктури та доступу до них, економічні умови господарювання, а також надає аналітичну інформацію про вплив на стан та можливості подальшого забезпечення національної безпеки та оборони, стан навколишнього природного середовища, роботу інших галузей економіки та об’єктів критичної інфраструктури.