КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 4 серпня 2023 р. № 818

Київ

Деякі питання паспортизації об’єктів критичної інфраструктури

Відповідно до частини четвертої статті 12 Закону України “Про критичну інфраструктуру” Кабінет Міністрів України **постановляє**:

1. Затвердити Порядок розроблення та погодження паспорта безпеки на об’єкт критичної інфраструктури, що додається.

2. Установити, що оператори критичної інфраструктури протягом трьох місяців з дня внесення відомостей про об’єкт критичної інфраструктури до Реєстру об’єктів критичної інфраструктури забезпечують подання на погодження паспорта безпеки на об’єкт критичної інфраструктури до відповідного державного органу, визначеного законодавством відповідальним за забезпечення формування та реалізацію державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури.

Прем’єр-міністр України **Д. ШМИГАЛЬ**

Інд. 49

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, 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.

_____

Додаток 1
до Порядку

ЗАТВЕРДЖЕНО

_____
(найменування посади керівника або уповноваженої особи оператора критичної інфраструктури)

_____ _____
(підпис) (власне ім’я, прізвище)

___ __ 20___ р.

МП (у разі наявності)

ПАСПОРТ БЕЗПЕКИ
на об’єкт критичної інфраструктури

_____
(назва об’єкта критичної інфраструктури)

_____
(унікальний реєстровий номер об’єкта критичної інфраструктури)

ПОГОДЖЕНО

_____
(найменування посади керівника секторального органу у сфері захисту критичної інфраструктури)

_____ _____
(підпис) (власне ім’я, прізвище)

___ _____ 20___ р.

_____

Додаток 2
до Порядку

ЗАГАЛЬНА ХАРАКТЕРИСТИКА
об’єкта критичної інфраструктури

Оператор критичної інфраструктури

1. Найменування (прізвище, власне ім’я, по батькові (у разі наявності)
_____
_____

2. Ідентифікаційний код юридичної особи в ЄДРПОУ (реєстраційний номер облікової картки платника податків (крім випадків, коли фізична особа через свої релігійні переконання відмовилася від прийняття реєстраційного номера облікової картки платника податків та офіційно повідомила про це відповідному контролюючому органу і має відмітку в паспорті) _____
_____

3. Місцезнаходження _____
_____

4. Форма власності _____

5. Країна реєстрації _____

6. КВЕД основної діяльності _____
_____

7. Керівник оператора критичної інфраструктури (найменування посади, прізвище, власне ім’я, по батькові (у разі наявності), контактні дані) _____
_____

8. Кінцевий бенефіціарний власник/контролер _____
_____

Об’єкт критичної інфраструктури

9. Унікальний реєстровий номер, дата реєстрації об’єкта критичної інфраструктури у Реєстрі об’єктів критичної інфраструктури _____
_____

10. Назва об’єкта критичної інфраструктури _____
_____

11. Категорія критичності _____

12. Місцезнаходження об’єкта критичної інфраструктури _____

_____

Загальна площа території _____

Кадастровий номер _____

Координати _____

Інші відомості, що можуть характеризувати місцезнаходження об’єкта критичної інфраструктури _____

_____

13. Власник об’єкта критичної інфраструктури _____

_____

У разі належності оператора критичної інфраструктури до державної або комунальної форми власності зазначається інформація про суб’єкта, до сфери управління якого він належить (господарського відання, оперативного управління) _____.

14. Загальна кількість працівників на об’єкті критичної інфраструктури _____

Розрахункова кількість осіб, які можуть одночасно перебувати на об’єкті критичної інфраструктури _____.

Кількість працівників найбільшої працюючої зміни об’єкта критичної інфраструктури та забезпечення їх укриття у захисних спорудах цивільного захисту, що готові до використання за призначенням _____

_____.

15. Особа, відповідальна за організацію захисту критичної інфраструктури та забезпечення постійного зв’язку з відповідними суб’єктами національної системи захисту критичної інфраструктури _____

_____

16. У разі наявності на об’єкті критичної інфраструктури об’єкта критичної інформаційної інфраструктури зазначається інформація про особу та/або підрозділ, що відповідає за стан захисту інформації (забезпечення інформаційної безпеки) та кіберзахисту об’єкта критичної інформаційної інфраструктури, зокрема тих, на яких покладено функції служби захисту інформації (прізвище, власне ім’я, по батькові (у разі наявності), номер телефону, адреса електронної пошти) _____

_____.

17. Секторальний орган у сфері захисту критичної інфраструктури:

сектор _____;

підсектор _____.

18. Тип основної послуги _____

Життєво важлива функція, яку виконує, та/або послуга, яку надає, об’єкт критичної інфраструктури _____.

КВЕД _____

19. Критичні елементи об’єкта критичної інфраструктури _____

_____

20. Наявність критичної інформаційної інфраструктури _____

_____

Зв’язок об’єкта критичної інфраструктури
з іншою інфраструктурою

21. Розташування об’єкта критичної інфраструктури стосовно транспортної інфраструктури, що складає єдину транспортну систему (із зазначенням найменування, місцезнаходження, відстані тощо), зокрема:

автомобільна (дороги, мостові переходи, автовокзали, автостанції тощо) _____;

залізнична (залізничні колії, мостові переходи, вокзали, станції, платформи, переїзди) _____;

повітряна (аеропорти, аеровокзали, аеродроми, злітно-посадкові смуги) _____;

річкова та морська (річкові та морські порти, річкові та морські вокзали, причали) _____;

метрополітен _____.

22. Розташування об’єкта критичної інфраструктури (із зазначенням найменування, місцезнаходження, відстані тощо) відносно:

населених пунктів _____;

житлових будинків _____;

будівель _____;

споруд _____;

місць масового перебування людей _____.

23. Розташування об’єкта критичної інфраструктури відносно систем енергозабезпечення (із зазначенням найменування, місцезнаходження, відстані тощо):

електромережі _____;

газопроводи _____;

споруди _____.

24. Розташування об’єкта критичної інфраструктури відносно систем життєзабезпечення (із зазначенням найменування, місцезнаходження, відстані тощо):

водопровідні мережі _____;

тепломережі _____;

киснепроводи та їх технічні споруди _____;

25. Розташування об’єкта критичної інфраструктури відносно пожежно-рятувальних підрозділів (частин), що залучаються до ліквідації наслідків надзвичайних ситуацій і пожеж (із зазначенням найменування, місцезнаходження, відстані тощо) _____

_____

26. Розташування об’єкта критичної інфраструктури відносно об’єктів підвищеної небезпеки (із зазначенням найменування, місцезнаходження, відстані тощо) _____

_____

Природно-кліматичні умови місцезнаходження
об’єкта критичної інфраструктури
(за період з _____ 20__ р. по _____ 20__ р.)

27. Кліматичний район _____

28. Сніговий район _____

29. Вітровий район _____

30. Характеристика ґрунтової основи _____

31. Загрози природного походження (землетруси, сейсмічність, зсуви, обвали, просідання, повені, дощові паводки, підтоплення, селі, сильні хвилі, припай, пожежі (лісові, степові, торф’яні) _____

_____

32. Інші відомості _____

Небезпечні технологічні процеси на
об’єкті критичної інфраструктури

33. Найменування технологічного процесу _____

_____

34. Відповідність вимогам безпеки (відповідає/не відповідає) _____

_____

35. Стан технологічного обладнання (задовільний/незадовільний) ____

_____

36. Найменування та вид джерела небезпеки (найменування, код і рівень можливих надзвичайних ситуацій) _____

37. Небезпечні речовини та матеріали (хімічні, вибухопожежо- та пожежонебезпечні), їх кількість та відповідність умовам зберігання (відповідає/не відповідає) _____

38. Інші відомості _____

_____	_____	_____
(найменування посади керівника або уповноваженої особи оператора критичної інфраструктури)	(підпис)	(власне ім’я, прізвище)

___ _____ 20___ р.

МП (у разі наявності)

_____