КАБІНЕТ МІНІСТРІВ УКРАЇНИ
ПОСТАНОВА

від 4 серпня 2023 р. № 818
Київ

Деякі питання паспортизації об’єктів критичної інфраструктури

{Із змінами, внесеними згідно з Постановами КМ
№ 1283 від 08.11.2024
№ 291 від 04.03.2026
№ 337 від 06.03.2026*}*

Відповідно до частини четвертої статті 12 Закону України “Про критичну інфраструктуру” Кабінет Міністрів України **п о с т а н о в л я є :**

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 або особи, яка його заміщає, керівника функціонального чи секторального органу або його заступника з використанням засобів механічного або іншого копіювання на зазначених документах не допускається.

{Абзац четвертий пункту 1 в редакції Постанови КМ № 337 від 06.03.2026}

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).

Контроль за своєчасним розробленням, затвердженням та поданням на погодження планів захисту та паспорта безпеки здійснюється секторальними органами.

{Пункт 3 доповнено абзацом згідно з Постановою КМ № 1283 від 08.11.2024}

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.

Під час воєнного стану оператор протягом місяця з дня внесення відомостей про об'єкт критичної інфраструктури до Реєстру об'єктів критичної інфраструктури розробляє план захисту (як складову паспорта безпеки), що передбачає заходи із захисту і протидії повітряному та артилерійському нападу.

{Пункт 5 доповнено новим абзацом згідно з Постановою КМ № 1283 від 08.11.2024}

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 пунктами 5, 7 цього Порядку, що затверджуються відповідними функціональними органами, функціональний орган не пізніше ніж протягом 10 робочих днів із дня реєстрації повертає його оператору разом із супровідним листом для приведення у відповідність із зазначеними вимогами цього Порядку.

{Абзац другий пункту 8 в редакції Постанови КМ № 337 від 06.03.2026}

{Абзац третій пункту 8 виключено на підставі Постанови КМ № 337 від 06.03.2026}

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.

{Абзац п'ятий пункту 9 із змінами, внесеними згідно з Постановою КМ № 337 від 06.03.2026}

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.

Під час воєнного стану оператор може затверджувати та подавати на погодження до секторального органу паспорт безпеки, що містить титульний аркуш, загальну характеристику та погоджений план захисту з урахуванням абзацу другого пункту 5 цього Порядку.

{Пункт 13 доповнено новим абзацом згідно з Постановою КМ № 1283 від 08.11.2024}

Під час воєнного стану у разі розроблення паспорта безпеки в порядку, передбаченому абзацом третім цього пункту, погоджені з функціональними органами плани захисту за іншими проектними загрозами національного, секторального та об'єктового (у разі наявності) рівня долучаються до паспорта безпеки, який подається до відповідного секторального органу для перегляду.

{Пункт 13 доповнено новим абзацом згідно з Постановою КМ № 1283 від 08.11.2024}

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 п'яти робочих днів із дня реєстрації повертає його оператору разом із супровідним листом за підписом керівника секторального органу або його заступника згідно з розподілом повноважень (обов'язків) для приведення у відповідність із зазначеними вимогами.

{Абзац другий пункту 14 із змінами, внесеними згідно з Постановою КМ № 337 від 06.03.2026}

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 секторальний орган 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.

{Абзац перший пункту 15 із змінами, внесеними згідно з Постановою КМ № 337 від 06.03.2026}

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 секторальний 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 паспортом безпеки.

{Абзац третій пункту 15 із змінами, внесеними згідно з Постановою КМ № 337 від 06.03.2026}

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;

настання підстав, передбачених абзацом четвертим пункту 13 цього Порядку.

{Пункт 16 доповнено новим абзацом згідно з Постановою КМ № 1283 від 08.11.2024}

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.

На вимогу Антитерористичного центру при СБУ оператор, об’єкт критичної інфраструктури якого віднесено до об’єкта можливих терористичних посягань відповідно до Правил антитерористичної безпеки, затверджених постановою Кабінету Міністрів України від 15 жовтня 2024 р. № 1172 (Офіційний вісник України, 2024 р., № 95, ст. 6145), з урахуванням вимог, передбачених пунктом 1 цього Порядку, подає копію плану захисту (як складової паспорта безпеки), що передбачає здійснення заходів із захисту та протидії загрозам диверсій та терористичних актів, протягом 10 робочих днів з дня отримання листа з такою вимогою.

{Пункт 18 доповнено абзацом згідно з Постановою КМ № 291 від 04.03.2026}

Додаток 1
до Порядку

ПАСПОРТ БЕЗПЕКИ
на об’єкт критичної інфраструктури

Додаток 2
до Порядку

ЗАГАЛЬНА ХАРАКТЕРИСТИКА
об’єкта критичної інфраструктури

Документи та файли

- Сигнальний документ — **f528085n78.docx** від 09.08.23 10:55, 13 кб
- Сигнальний документ — **f528085n79.docx** від 09.08.23 10:55, 17 кб

Публікації документа

- **Урядовий кур'єр** від 08.08.2023 — № 158
- **Офіційний вісник України** від 15.09.2023 — 2023 р., № 77, стор. 112, стаття 4366, код акта 119895/2023