



АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

НАКАЗ

м. Київ

14 січня 2025 року

№ 17

**Про затвердження Методики
та Критеріїв і показників
оцінки стану захищеності
об'єктів критичної інфраструктури**

ЗАРЕЄСТРОВАНО

в Міністерстві юстиції України

за № 845/48 КР/1

від 07.03.2025

Відповідно до статті 23 Закону України «Про критичну інфраструктуру», абзацу четвертого пункту 1, абзацу третього підпункту 1 пункту 3, підпункту 15¹ пункту 4 та пункту 10 Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411, пункту 7 Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 22 липня 2022 року № 821,

НАКАЗУЮ:

1. Затвердити такі, що додаються:
Методику оцінки стану захищеності об'єктів критичної інфраструктури;
Критерії і показники оцінки стану захищеності об'єктів критичної інфраструктури.
2. Департаменту захисту критичної інфраструктури Адміністрації Державної служби спеціального зв'язку та захисту інформації України забезпечити подання цього наказу на державну реєстрацію до Міністерства юстиції України в установленому порядку.
3. Контроль за виконанням цього наказу покласти на заступника Голови Державної служби спеціального зв'язку та захисту інформації України згідно з розподілом обов'язків.
4. Цей наказ набирає чинності з дня його офіційного опублікування.

Голова Служби

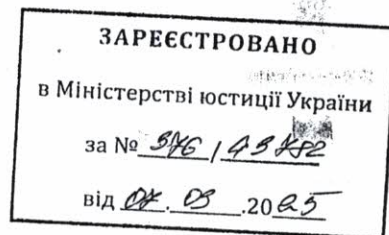


Згідно з оригіналом

Олександр ПОТІЙ

Заступник начальника
4 відділу 3 управління
ДПЗ Адміністрації Держспецзв'язку
Підпозначник СВ
"07" "04" 2025 року

О.В.Тертична



ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної
служби спеціального зв'язку та
захисту інформації України
14 січня 2025 року № 17

Методика

оцінки стану захищеності об'єктів критичної інфраструктури

1. Ця Методика спрямована на реалізацію заходів з визначення стану захищеності об'єктів критичної інфраструктури, а також вжитих і запланованих заходів для забезпечення захисту, безпеки та стійкості критичної інфраструктури.

2. У цій Методиці терміни вживаються у значенні, наведеному в Законі України «Про критичну інфраструктуру» та інших нормативно-правових актах у сфері захисту критичної інфраструктури.

3. Секторальні та функціональні органи у сфері захисту критичної інфраструктури проводять оцінку стану захищеності об'єктів критичної інфраструктури відповідно до Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 22 липня 2022 року № 821 (далі – Порядок моніторингу), та цієї Методики.

4. Секторальний орган у сфері захисту критичної інфраструктури проводить оцінку стану захищеності об'єктів критичної інфраструктури своїх секторів з урахуванням відомостей, зазначених у щорічному звіті оператора критичної інфраструктури, паспорті безпеки на об'єкт критичної інфраструктури, а також вимогах (планах, програмах, нормах, регламентах тощо) секторального органу у сфері захисту критичної інфраструктури щодо захисту та стійкості об'єктів критичної інфраструктури, передбачених законодавством у сфері захисту критичної інфраструктури.

Функціональний орган у сфері захисту критичної інфраструктури проводить оцінку захищеності об'єкта критичної інфраструктури з урахуванням відомостей, зазначених у плані захисту об'єкта критичної інфраструктури, який є складовою паспорта безпеки на об'єкт критичної інфраструктури, в частині проектних загроз національного, секторального та об'єктового (у разі наявності) рівнів, щодо яких він є відповідальним.

5. Оцінка стану захищеності об'єктів критичної інфраструктури банків, інших осіб, що провадять діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України,

операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг проводиться Національним банком України виключно за критеріями, визначеними в рядках 1.1 – 4.15 Критеріїв і показників оцінки стану захищеності об'єктів критичної інфраструктури, затверджених наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 14 січня 2025 року № 17, якщо додаткові критерії не встановлені Національним банком України.

6. Процедура оцінки стану захищеності об'єкта критичної інфраструктури містить такі етапи:

- підготовчий;
- проведення оцінки стану захищеності об'єкта критичної інфраструктури;
- складання акта оцінки стану захищеності об'єкта критичної інфраструктури згідно з формою, встановленою додатком до Порядку моніторингу.

7. Під час підготовчого етапу секторальний орган у сфері захисту критичної інфраструктури при формуванні річного плану проведення оцінки стану захищеності об'єктів критичної інфраструктури погоджує з відповідними функціональними органами у сфері захисту критичної інфраструктури, які залучаються до оцінки стану захищеності об'єктів критичної інфраструктури, дату/період проведення оцінки стану захищеності об'єктів критичної інфраструктури.

Розроблений секторальним органом у сфері захисту критичної інфраструктури річний план проведення оцінки стану захищеності об'єктів критичної інфраструктури надсилається на погодження до залучених для проведення оцінки стану захищеності об'єктів критичної інфраструктури функціональних органів у сфері захисту критичної інфраструктури.

Затверджений секторальним органом у сфері захисту критичної інфраструктури річний план проведення оцінки стану захищеності об'єктів критичної інфраструктури надсилається уповноваженому органу у сфері захисту критичної інфраструктури України в порядку, визначеному пунктом 5 Порядку моніторингу. За результатами розгляду річного плану проведення оцінки стану захищеності об'єктів критичної інфраструктури уповноважений орган у сфері захисту критичної інфраструктури України може ініціювати включення свого представника до складу Комісії з оцінки стану захищеності об'єктів критичної інфраструктури (далі – Комісія з оцінки стану захищеності) з переліку об'єктів критичної інфраструктури, визначених у річному плані проведення оцінки захищеності об'єктів критичної інфраструктури, про що має повідомити у десятиденний строк секторальний орган у сфері захисту критичної інфраструктури.

Персональний склад Комісії з оцінки стану захищеності затверджується секторальним органом у сфері захисту критичної інфраструктури не пізніше ніж

за 30 днів до дати проведення оцінки стану захищеності об'єкта критичної інфраструктури.

Секторальний орган у сфері захисту критичної інфраструктури доводить до відома оператора критичної інфраструктури витяг з річного плану проведення оцінки стану захищеності об'єктів критичної інфраструктури в частині, що його стосується, відповідно до Порядку моніторингу.

8. З метою актуалізації інформації щодо об'єкта критичної інфраструктури секторальний та/або функціональні органи у сфері захисту критичної інфраструктури, залучені для проведення оцінки стану захищеності об'єкта критичної інфраструктури, мають право надіслати письмовий запит до оператора критичної інфраструктури про надання ним:

підтверджувальної інформації або документів щодо проведення заходів фізичного захисту, кіберзахисту та охорони об'єкта критичної інфраструктури (фото, деталізація заходів тощо);

додаткових пояснень щодо інформації, отриманої від оператора критичної інфраструктури, та складених на об'єкт критичної інфраструктури документів, визначених пунктом 4 цієї Методики.

9. Під час етапу проведення оцінки стану захищеності об'єктів критичної інфраструктури використовується:

оціночний метод – шляхом аналізу інформації, отриманої від оператора критичної інфраструктури, та складених на об'єкт критичної інфраструктури документів, визначених пунктом 4 цієї Методики, з метою встановлення заходів, яких необхідно вжити для захисту об'єкта критичної інфраструктури;

прямий метод – шляхом обстеження об'єкта критичної інфраструктури щодо виконання заходів із захисту об'єкта критичної інфраструктури з метою визначення фактичного стану захищеності об'єкта критичної інфраструктури.

10. Під час проведення оцінки стану захищеності об'єкта критичної інфраструктури секторальний та функціональні органи у сфері захисту критичної інфраструктури у разі потреби мають право залучати представників інших органів державної влади, органів місцевого самоврядування, на яких поширюються вимоги законодавства про інформацію, за погодженням з їх керівниками.

11. Під час проведення оцінки стану захищеності об'єкта критичної інфраструктури секторальний і функціональні органи у сфері захисту критичної інфраструктури у складі Комісії з оцінки стану захищеності заповнюють Форму для визначення оцінки стану захищеності об'єкта критичної інфраструктури згідно з додатком до цієї Методики (далі – Форма про результати оцінювання) у межах своїх повноважень.

Форма про результати оцінювання заповнюється з проставленням відповідної кількості балів за показниками та ознаки рівня дотримання кожного критерія оцінки стану захищеності об'єкта критичної інфраструктури і об'єкта в цілому.

Секторальний орган у сфері захисту критичної інфраструктури заповнює рядки 1–3, 4.1–4.4, 4.13–4.15 Форми про результати оцінювання.

Функціональний орган (функціональні органи) у сфері захисту критичної інфраструктури заповнює (заповнюють) рядки 4.5–4.12, 5–10 Форми про результати оцінювання.

Кількість балів визначається, виходячи зі співвідношення набраної кількості балів за критерієм (об'єктом в цілому) до її максимально можливої суми.

12. Показники стану захищеності об'єкта критичної інфраструктури оцінюються секторальними і функціональними органами у сфері захисту критичної інфраструктури за бальною системою, виходячи з ознаки дотримання встановленого показника: «так», «частково», «ні» (крім випадків, передбачених в абзаці другому пункту 13, пункті 14 цієї Методики), при цьому:

якщо показник має ознаку «так», йому присвоюється 2 бали;

якщо показник має ознаку «частково», йому присвоюється 1 бал;

якщо показник має ознаку «ні», йому бали не присвоюються (0 балів).

13. Значення балів, що присвоєні відповідним показникам оцінки стану захищеності об'єкта критичної інфраструктури, підсумовуються за кожним критерієм оцінки стану захищеності об'єкта критичної інфраструктури та в цілому по об'єкту і виставляються у Формі про результати оцінювання.

Якщо певний показник/критерій оцінки стану захищеності об'єкта критичної інфраструктури не передбачений для об'єкта критичної інфраструктури, такий показник/критерій не бере участі у підрахунку балів, а у відповідному полі у Формі про результати оцінювання проставляється прочерк.

Оцінка стану захищеності об'єкта критичної інфраструктури за критерієм «Забезпечення кіберзахисту об'єкта критичної інфраструктури» проводиться шляхом здійснення внутрішнього та зовнішнього сканування мереж і ресурсів на вразливості.

14. Значення балів за критеріями «Документальне оформлення оператором критичної інфраструктури заходів із забезпечення захисту та стійкості об'єкта критичної інфраструктури», «Рівень фінансування об'єкта критичної інфраструктури» та «Рівень взаємодії оператора критичної інфраструктури з іншими суб'єктами національної системи захисту критичної інфраструктури» не виставляється та не підсумовується.

15. Якщо за результатами проведення оцінки стану захищеності об'єкта критичної інфраструктури буде виявлена невідповідність інформації, отриманої

від оператора критичної інфраструктури, та складених на об'єкт критичної інфраструктури документів, визначених пунктом 4 цієї Методики, показники балів у Формі про результати оцінювання коригуються відповідно до актуальної інформації, а за кожний такий випадок (якщо він погіршує стан захищеності об'єкта критичної інфраструктури) додатково знімається 1 бал за критерієм, щодо якого встановлена невідповідність.

16. Для показників стану захищеності об'єкта критичної інфраструктури за критерієм «Рівень захисту від епідемії» ознака рівня їх дотримання («так», «частково», «ні») проставляється відповідно до розрахунку стану захищеності об'єкта критичної інфраструктури за критерієм «Рівень захисту від епідемії» згідно з додатком 2 до цієї Методики.

17. Для показників стану захищеності об'єкта критичної інфраструктури за критерієм «Забезпечення кіберзахисту об'єкта критичної інфраструктури» ознака рівня їх дотримання («так», «частково», «ні») проставляється відповідно до розрахунку стану захищеності об'єкта критичної інфраструктури за критерієм «Забезпечення кіберзахисту об'єкта критичної інфраструктури» згідно з додатком 3 до цієї Методики.

18. Для показників стану захищеності об'єкта критичної інфраструктури за критерієм «Рівень захисту від економічного тероризму» ознака рівня їх дотримання («так», «частково», «ні») проставляється відповідно до розрахунку стану захищеності об'єкта критичної інфраструктури за критерієм «Рівень захисту від економічного тероризму» згідно з додатком 4 до цієї Методики.

19. Стан захищеності об'єкта критичної інфраструктури за їх критеріями та по об'єкту в цілому оцінюється секторальним і функціональними органами у сфері захисту критичної інфраструктури за ознаками: «забезпечує», «обмежено забезпечує», «не забезпечує».

20. Ознака стану захищеності об'єкта критичної інфраструктури за відповідним критерієм визначається відповідно до співвідношення набраної кількості балів до її максимально можливої суми і розраховується за формулою:

$$CЗ_{\text{крит}} = \frac{\sum БП_i}{\sum БП_{\text{max}}} \quad (1)$$

де $CЗ_{\text{крит}}$ – узагальнена нормована оцінка стану захищеності об'єкта критичної інфраструктури за певним критерієм;

$БП_i$ – фактична сума балів за певним показником оцінки стану захищеності об'єкта критичної інфраструктури;

$БП_{\text{max}}$ – максимально можлива сума балів за певним показником оцінки стану захищеності об'єкта критичної інфраструктури.

Відповідна ознака за критерієм визначається на основі узагальненої нормованої оцінки стану захищеності за цим критерієм відповідно до такого правила:

- якщо $0,85 < CЗ_{\text{крит}} \leq 1$, виставляється ознака «забезпечує»;
- якщо $0,65 < CЗ_{\text{крит}} \leq 0,85$, виставляється ознака «обмежено забезпечує»;
- якщо $CЗ_{\text{крит}} \leq 0,65$, виставляється ознака «не забезпечує».

21. Стан захищеності об'єкта критичної інфраструктури за критерієм «Стан інженерного захисту об'єкта критичної інфраструктури» оцінюється згідно з Методикою оцінювання стану інженерного захисту об'єктів критичної інфраструктури, затвердженою постановою Кабінету Міністрів України від 26 квітня 2024 року № 471 (далі – Методика № 471). Присвоєна за результатами оцінювання згідно з Методикою № 471 категорія стану споруди інженерного захисту об'єкта критичної інфраструктури в цілому відповідає такій ознаці та сумі балів цієї Методики:

- «нормальний» – є ознакою «забезпечує» і дорівнює 30 балам;
- «задовільний» – є ознакою «обмежено забезпечує» і дорівнює 15 балам;
- «незадовільний» та «недопустимий» – є ознакою «не забезпечує» і дорівнює 0 балам.

22. Ознака стану захищеності об'єкта критичної інфраструктури в цілому визначається відповідно до співвідношення набраної кількості балів до її максимально можливої суми і розраховується за формулою:

$$CЗ_{\text{окі}} = \frac{\sum BK_i}{\sum BK_{\text{max}}} \quad (2)$$

де $CЗ_{\text{окі}}$ – узагальнена нормована оцінка стану захищеності об'єкта критичної інфраструктури в цілому;

BK_i – фактична сума балів за всіма критеріями оцінки стану захищеності об'єкта критичної інфраструктури;

BK_{max} – максимально можлива сума балів за всіма критеріями оцінки стану захищеності об'єкта критичної інфраструктури.

Відповідна ознака стану захищеності об'єкта критичної інфраструктури в цілому визначається, виходячи з узагальненої нормованої оцінки стану захищеності об'єкта критичної інфраструктури в цілому, відповідно до такого правила:

- якщо $0,85 < CЗ_{\text{окі}} \leq 1$, виставляється ознака «забезпечує»;
- якщо $0,65 < CЗ_{\text{окі}} \leq 0,85$, виставляється ознака «обмежено забезпечує»;
- якщо $CЗ_{\text{окі}} \leq 0,65$, виставляється ознака «не забезпечує».

23. На етапі складання акта оцінки стану захищеності об'єкта критичної інфраструктури секторальний і функціональні органи у сфері захисту критичної інфраструктури проводять аналіз інформації та фактичного стану захищеності

об'єкта критичної інфраструктури з урахуванням даних, викладених у Формі про результати оцінювання.

За результатами проведеного аналізу інформації та фактичного стану захищеності об'єкта критичної інфраструктури представник секторального органу у сфері захисту критичної інфраструктури складає акт оцінки стану захищеності об'єкта критичної інфраструктури згідно з формою, визначеною додатком до Порядку моніторингу, з урахуванням заповнених членами Комісії з оцінки стану захищеності в межах повноважень Форм про результати оцінювання.

Директор Департаменту
захисту критичної інфраструктури
Адміністрації Держспецзв'язку



Валерій НОВАК

Додаток 1
до Методики оцінки стану
захищеності об'єктів критичної
інфраструктури
(пункт 11)

**Форма для визначення оцінки стану захищеності об'єкта критичної
інфраструктури**

_____ (найменування об'єкта критичної інфраструктури)

Суб'єкт моніторингу _____
(найменування секторального і функціональних органів у сфері захисту
критичної інфраструктури у складі Комісії з оцінки стану захищеності об'єктів критичної інфраструктури)

в особі головуєчого Комісії з оцінки стану захищеності об'єктів критичної
інфраструктури _____
(найменування посади, прізвище, власне ім'я, по батькові (за наявності))

_____ (представника секторального органу у сфері захисту критичної інфраструктури)

та уповноважених посадових осіб _____
(найменування посади, прізвища, власні імена, по батькові (за наявності))

_____ (посадових осіб, які провели оцінку стану захищеності об'єкта критичної інфраструктури)

на підставі _____
(реквізити документа, згідно з яким проводилася оцінка стану захищеності
об'єкта критичної інфраструктури)

у присутності _____
(найменування посади, прізвище, власне ім'я, по батькові (за наявності))

_____ (керівника об'єкта критичної інфраструктури)

та за участю структурного підрозділу/відповідальних осіб з питань захисту
об'єкта критичної інфраструктури, а саме _____
(найменування підрозділу/
прізвища, власні імена, по батькові (за наявності) відповідальних осіб)

у кількості _____ осіб провели оцінку стану захищеності об'єкта критичної
інфраструктури у період з _____ 20__ року по _____ 20__ року

№ з/п	Найменування критерію/показника оцінювання	Так/ні/частково	Кількість балів
1	Документальне оформлення оператором критичної інфраструктури заходів із забезпечення захисту та стійкості об'єкта критичної інфраструктури	x	x
1.1	Наявність структурного підрозділу режимно-секретного органу (PCO)		x
1.2	Наявність паспорта безпеки на об'єкт критичної інфраструктури		x
1.3	Наявність загальної характеристики об'єкта критичної інфраструктури		x
1.4	Наявність ідентифікованих проектних загроз національного, секторального (у разі затвердження) та об'єктового (за наявності) рівнів		x
1.5	Наявність розробленого плану захисту об'єкта критичної інфраструктури за кожною із проектних загроз національного, секторального (у разі затвердження) та об'єктового (за наявності) рівнів		x
1.6	Наявність розроблених вимог щодо організації захисту об'єкта критичної інфраструктури		x
1.7	Виконано заходи, рекомендовані оператору критичної інфраструктури за результатами проведення попереднього моніторингу рівня безпеки об'єкта критичної інфраструктури		x
1.8	Наявність розробленого об'єктового плану заходів щодо захисту і забезпечення стійкості об'єкта критичної інфраструктури		x
1.9	Наявність розроблених правил управління ризиками безпеки		x
1.10	Наявність розробленого плану локалізації та ліквідації наслідків аварій		x
1.11	Оператором критичної інфраструктури розроблено політику інформаційної безпеки, політику управління ризиками інформаційної безпеки, методику оцінювання та оброблення ризиків інформаційної безпеки		x
1.12	Наявність посадових інструкцій осіб, відповідальних за організацію та забезпечення захисту об'єкта критичної інфраструктури		x
1.13	Забезпечено постійну взаємодію 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 (наявність договорів з підприємствами/надавачами послуг)		x
1.14	Погоджено план захисту об'єкта критичної інфраструктури за кожною з проектних загроз відповідним функціональним органом (органами)		x
1.15	Погоджено паспорт безпеки на об'єкт критичної інфраструктури відповідним секторальним органом		x

№ з/п	Найменування критерію/показника оцінювання	Так/ні/частково	Кількість балів
1.16	Забезпечено належний рівень фінансування заходів безпеки об'єкта критичної інфраструктури та матеріально-технічної спроможності		x
2	Рівень фінансування об'єкта критичної інфраструктури	x	x
2.1	Забезпечено належний рівень фінансування та засобами і ресурсами функціонування системи захисту критичної інфраструктури		x
2.2	Наявність резервів фінансових і матеріальних ресурсів, необхідних для реагування на кризові ситуації та ліквідації їх наслідків		x
3	Рівень взаємодії оператора критичної інфраструктури з іншими суб'єктами національної системи захисту критичної інфраструктури	x	x
3.1	Забезпечено зв'язок (взаємодію) із суб'єктами національної системи захисту критичної інфраструктури		x
3.2	Організовано обмін інформацією про ризики та загрози з іншими суб'єктами національної системи захисту критичної інфраструктури		x
3.3	Створено умови для належного виконання правоохоронними органами, розвідувальними органами та органами, що здійснюють контррозвідувальну діяльність, і їх підрозділами завдань із захисту об'єкта критичної інфраструктури		x
3.4	Організовано заходи з реагування на інциденти, кризові ситуації, а також ліквідації їх наслідків на об'єкті критичної інфраструктури у взаємодії з іншими суб'єктами національної системи захисту критичної інфраструктури		x
4	Загальний рівень забезпечення захисту та стійкості об'єкта критичної інфраструктури	x	x
4.1	Проведено оцінку ризиків		
4.2	Забезпечується виконання вимог щодо організації захисту об'єкта критичної інфраструктури		
4.3	Розроблені вимоги щодо організації захисту об'єкта критичної інфраструктури відповідають вимогам секторального органу (за наявності таких вимог)		
4.4	Забезпечується виконання вимог секторального органу щодо захисту об'єкта критичної інфраструктури (за наявності таких вимог)		
4.5	Забезпечується виконання плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «Удари засобами повітряного нападу та ракетно-артилерійські удари (обстріли)»		
4.6	Забезпечується виконання плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «Терористичний акт або диверсія»		
4.7	Забезпечується виконання плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «Кібератака/кіберінцидент»		
4.8	Забезпечується виконання плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «Пожежі та вибухи»		

№ з/п	Найменування критерію/показника оцінювання	Так/ні/частково	Кількість балів
4.9	Забезпечується виконання плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «Епідемія»		
4.10	Забезпечується виконання плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «Економічний тероризм»		
4.11	Забезпечується виконання плану захисту об'єкта критичної інфраструктури за проектними загрозами секторального рівня (у разі затвердження)		
4.12	Забезпечується виконання плану захисту об'єкта критичної інфраструктури за проектними загрозами об'єктового рівня (за наявності)		
4.13	Забезпечується виконання правил управління ризиками безпеки		
4.14	Забезпечується виконання об'єктового плану заходів щодо захисту і забезпечення стійкості об'єкта критичної інфраструктури		
4.15	Забезпечується виконання плану локалізації та ліквідації наслідків аварій		
	Кількість балів, знятих за невідповідність інформації:	x	
	Всього балів за критерієм:	x	
	Максимально можлива кількість балів за критерієм:	x	
	Критерій відповідає ознаці:		
5	Стан інженерного захисту об'єкта критичної інфраструктури	x	x
5.1	Оцінка за Методикою оцінювання стану інженерного захисту об'єктів критичної інфраструктури, затвердженою постановою Кабінету Міністрів України від 26 квітня 2024 року № 471		
5.2	Забезпечено зв'язок (взаємодію) та обмін інформацією з функціональним органом (функціональними органами)		x
5.3	Забезпечено належний рівень фінансування та засобами і ресурсами функціонування системи захисту критичної інфраструктури за критерієм «Стан інженерного захисту об'єкта критичної інфраструктури»		x
5.4	Наявність резервів фінансових та матеріальних ресурсів, необхідних для реагування на кризові ситуації та ліквідації їх наслідків за критерієм «Стан інженерного захисту об'єкта критичної інфраструктури»		x
	Всього балів за критерієм:	x	
	Максимально можлива кількість балів за критерієм:	x	
	Критерій відповідає ознаці:		
6	Рівень захисту від терористичних актів та диверсій	x	x
6.1	Наявність витягу з превентивного плану проведення антитерористичної операції на об'єкті критичної інфраструктури в частині дій персоналу та охорони		
6.2	Забезпечено зв'язок (взаємодію) та обмін інформацією з функціональним органом (функціональними органами)		
6.3	Забезпечено належний рівень фінансування та засобами і ресурсами функціонування системи захисту критичної інфраструктури за критерієм «Рівень захисту від терористичних атак та диверсій»		x

№ з/п	Найменування критерію/показника оцінювання	Так/ні/частково	Кількість балів
6.4	Наявність резервів фінансових та матеріальних ресурсів, необхідних для реагування на кризові ситуації та ліквідації їх наслідків за критерієм «Рівень захисту від терористичних атак та диверсій»		x
	Забезпеченість охороною та належним інженерно-технічним оснащенням для запобігання неправомірному проникненню на об'єкті критичної інфраструктури сторонніх осіб	x	x
6.5	Наявність необхідних інженерно-технічних засобів		
6.5.1	Огорожа по всьому периметру об'єкта критичної інфраструктури не нижче 2 метрів (залізобетонна, цегляна, секційна з металевих прутів, із металевої сітки на стовпах)		
6.5.2	Підступи до об'єкта критичної інфраструктури розчищені від кущів та чагарників до 50 метрів від зовнішнього периметра огорожі, проріджені дерева, нижні сучки та гілки обрізані до висоти 2.5 метра, трава скошена, зайвих предметів немає		
6.5.3	Підступи до об'єкта критичної інфраструктури, освітлюються світильниками, прожекторами направленої дії		
6.6	Наявність режиму контрольованого допуску осіб і транспортних засобів		
6.7	Наявність технічних засобів охорони локального рівня		
6.8	Наявність на об'єктах засобів охоронного призначення, на тривожні сповіщення яких реагують органи державної влади, підприємства та організації		
6.9	Наявність автономного електроживлення		
	Наявність погоджених/затверджених Антитерористичним центром при Службі безпеки України або його координаційними групами інструкцій з питань реагування на загрозу вчинення або вчинення терористичного акту/диверсії на об'єкті критичної інфраструктури	x	x
6.10	Наявність інструкцій щодо порядку дій персоналу у разі встановлення керівником Антитерористичного центру при Службі безпеки України відповідних рівнів терористичної загрози		
6.11	Наявність інструкцій щодо порядку дій персоналу у разі отримання погроз терористичного характеру		
6.12	Наявність інструкцій щодо порядку дій персоналу у разі виявлення підозрілих предметів з ознаками вибухового чи іншого небезпечного пристрою		
6.13	Наявність інструкцій щодо порядку дій персоналу у разі вчинення на об'єкті критичної інфраструктури чи прилеглої території вибуху чи інших дій, які спричинили людські жертви		
6.14	Наявність інструкцій щодо порядку дій персоналу у разі вчинення терористичного акту шляхом захоплення та утримання заручників		
	Стан організації фізичної охорони об'єкта критичної інфраструктури	x	x

№ з/п	Найменування критерію/показника оцінювання	Так/ні/частково	Кількість балів
6.15	Наявність озброєної охорони, яка в установленому законодавством порядку має право на використання та застосування зброї і застосування заходів примусу в разі визначення на об'єкті першочергових дій, яких необхідно вжити для недопущення збільшення негативних наслідків		
6.16	Наявність структурного підрозділу/відповідальних осіб з питань забезпечення антитерористичної захищеності		
6.17	Проведено перевірку знань персоналу об'єкта критичної інфраструктури щодо реагування на можливі загрози під час тренувань, командно-штабних і тактико-спеціальних навчань з антитерористичної тематики		
6.18	Наявність на постах охорони об'єктів ручних систем тривожної сигналізації, на тривожні сповіщення яких реагують органи державної влади, підприємства та організації		
	Кількість балів, знятих за невідповідність інформації:	x	
	Всього балів за критерієм:	x	
	Максимально можлива кількість балів за критерієм:	x	
	Критерій відповідає ознаці:		
7	Забезпечення кіберзахисту об'єкта критичної інфраструктури	x	x
7.1	Наявність визначеної посадової особи, відповідальної за кіберзахист об'єкта критичної інфраструктури, та наявність підрозділу, відповідального за кіберзахист об'єкта критичної інфраструктури		
7.2	Забезпечено виконання Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518		
7.3	Проведено оцінку ризиків інформаційної безпеки об'єкта критичної інфраструктури		
7.4	Затверджено політику інформаційної безпеки на об'єкті критичної інфраструктури		
7.5	Проведено внутрішній та незалежний аудити інформаційної безпеки на об'єкті критичної інфраструктури		
7.6	Забезпечено зв'язок (взаємодію) та обмін інформацією з функціональним органом (функціональними органами)		x
7.7	Проведено перевірку ефективності заходів щодо захисту мереж та систем об'єкта критичної інфраструктури від зовнішнього проникнення шляхом виконання тесту на проникнення (Penetration test)		
7.8	Забезпечено належний рівень фінансування та засобами і ресурсами функціонування системи захисту критичної інфраструктури за критерієм «Забезпечення кіберзахисту об'єкта критичної інфраструктури»		x
7.9	Наявність резервів фінансових та матеріальних ресурсів, необхідних для реагування на кризові ситуації та ліквідації їх наслідків за критерієм «Забезпечення кіберзахисту об'єкта критичної інфраструктури»		x
	Кількість балів, знятих за невідповідність інформації:	x	
	Всього балів за критерієм:	x	

№ з/п	Найменування критерію/показника оцінювання	Так/ні/частково	Кількість балів
	Максимально можлива кількість балів за критерієм:	х	
	Критерій відповідає ознаці:		
8	Цивільний захист, пожежна та техногенна безпека	х	х
8.1	Утримання території	х	х
8.1.1	Під час експлуатації об'єкта не зменшено мінімальні протипожежні відстані між будівлями, спорудами, установками, відкритими майданчиками, місцями для зберігання матеріалів		х
8.1.2	Автомобільні дороги, проїзди й проходи до будівель, споруд, пожежних вододжерел, підступи до зовнішніх стаціонарних пожежних драбин, пожежного інвентарю, обладнання та засобів пожежогасіння вільні, утримуються справними, взимку очищаються від снігу		х
8.1.3	Автомобільні дороги та проїзди для пожежних машин мають дорожнє покриття, придатне для їх проїзду		х
8.1.4	Протипожежні відстані між будівлями, спорудами не використовуються для складування матеріалів, устаткування, стоянок транспорту, будівництва та встановлення тимчасових будинків і споруд, у тому числі мобільних (інвентарних) будівель, окрім захисних інженерних споруд		
8.1.5	На території об'єкта забезпечено освітлення зовнішніх пожежних драбин, протипожежного обладнання, входів до будинків та споруд		
8.1.6	Забезпечено інженерний захист наземних будівель (споруд) насосної станції пожежогасіння, наземних резервуарів запасів вогнегасних речовин для цілей пожежогасіння, трубопроводів (сухотрубів) систем пожежогасіння, а також розподільчих вузлів систем пожежогасіння трансформаторів		
8.1.7	Забезпечено улаштування та належне утримання додаткових проходів (отворів) у захисті, що забезпечують доступ пожежно-рятувальних підрозділів для можливості подачі вогнегасних речовин для цілей пожежогасіння		
8.1.8	Під час улаштування додаткового протиуламкового захисту у верхній частині захисних конструкцій із габіонів використано негорючі матеріали		
8.1.9	Забезпечено влаштування автоматичних систем пожежогасіння трансформаторів та вибухо-, пожежонебезпечного обладнання, розташованого під захисними конструкціями типу «Шелтер»		
8.1.10	Передбачено заходи з блискавкозахисту та захисту від вторинних проявів блискавки захисної конструкції типу «Шелтер»		
8.1.11	Передбачено додатковий захист пультів управління з використанням протипожежних дверей, вікон та клапанів систем вентиляції з класом вогнестійкості не нижче EI 90.		
8.1.12	Передбачено влаштування додаткових незалежних джерел електроживлення (дизельних генераторів) для насосів систем протипожежного водопостачання та стаціонарних систем пожежогасіння для забезпечення безперебійної подачі вогнегасних речовин для цілей пожежогасіння в		

№ з/п	Найменування критерію/показника оцінювання	Так/ні/частково	Кількість балів
	умовах повного знеструмлення об'єкта критичної інфраструктури		
8.1.13	Наявність інженерного захисту приміщень, будинків та зовнішніх установок категорій А, Б за вибухопожежною та пожежною небезпекою		
8.1.14	Вжиття додаткових інженерних заходів щодо обмеження можливого поширення пожежі на суміжні об'єкти (влаштування додаткових бар'єрів, обвалування, протипожежних стін тощо)		
8.2	Утримання будинків, приміщень та споруд	x	x
8.2.1	Керівник об'єкта забезпечив утримання засобів протипожежного захисту у справному стані та їх технічне обслуговування		
8.2.2	Протипожежні двері, ворота, вікна, люки, клапани, завіси (екрани) у протипожежних перешкодах утримуються у справному стані. Будь-які пристрої, предмети тощо, що перешкоджають їх зачиненню, не встановлено		
8.2.3	У будинках, крім будинків V ступеня вогнестійкості, дерев'яні елементи горищних покриттів (крокви, лати) оброблені засобами вогнезахисту, які забезпечують I групу вогнезахисної ефективності		
8.2.4	Класи вогнестійкості будівельних конструкцій і групи поширення вогню по цих конструкціях відповідають будівельним нормам. Вогнезахист металевих конструкцій забезпечено згідно з вимогами законодавства у сфері цивільного захисту, пожежної та техногенної безпеки		
8.2.5	Горища, технічні, підвальні, цокольні та інші приміщення (у тому числі вентиляційні камери, електрощитові) використовуються за призначенням, виробничі і складські дільниці в них не розміщуються, сторонніми предметами їх не засмічено та не захащено		
8.2.6	Стационарні зовнішні пожежні сходи, сходи на перепадах висот і огорожі на покриттях будівель та споруд утримуються справними		
8.2.7	У разі потреби встановлення на вікнах приміщень, де перебувають люди, ґрат вони розкриваються, розсуваються або знімаються		
8.3	Утримання евакуаційних шляхів і виходів	x	x
8.3.1	Кількість та розміри евакуаційних виходів з будівель і приміщень не зменшено		
8.3.2	У приміщенні, яке має один евакуаційний вихід, одночасно розміщено (перебуває) не більше ніж 50 осіб		
8.3.3	Двері на шляхах евакуації відчиняються в напрямку виходу з будівель (приміщень)		
8.3.4	Сходові марші і площадки мають справні огорожі із поручнями, котрі не зменшують ширину сходових маршів і площадок		
8.3.5	Сходові клітки, внутрішні відкриті та зовнішні сходи, коридори, проходи та інші шляхи евакуації забезпечені евакуаційним освітленням		
8.3.6	Індивідуальні технічні рішення щодо евакуаційних шляхів і виходів, які передбачені концепцією протипожежного		

№ з/п	Найменування критерію/показника оцінювання	Так/ні/частково	Кількість балів
	захисту об'єкта або визначені за результатами обґрунтування відхилень від вимог нормативних документів у сфері цивільного захисту, пожежної та техногенної безпеки, виконуються		
8.4	Стан утримання електроустановок	x	x
8.4.1	Електричні машини, апарати, обладнання, електропроводи та кабелі за виконанням та ступенем захисту відповідають класу зони згідно з правилами улаштування електроустановок, мають апаратуру захисту від струмів короткого замикання та інших аварійних режимів		
8.4.2	З'єднання, відгалуження та окінцювання жил проводів і кабелів здійснено за допомогою опресування, зварювання, паяння або затискачів		
8.4.3	В електропроводах вибухонебезпечних і пожежонебезпечних зон відгалужувальні та з'єднувальні коробки закриті кришками з негорючих або важкогорючих матеріалів		
8.4.4	Відстань від кабелів та ізолюваних проводів, прокладених відкрито, до місць відкритого зберігання (розміщення) горючих матеріалів, становить не менше ніж 1 метр		
8.4.5	Електророзетки, вимикачі, перемикачі та інші подібні апарати встановлені на не горючі основи (конструкції)		
8.4.6	Замірювання опору ізоляції і перевірка спрацювання приладів захисту електричних мереж та електроустановок від короткого замикання проводяться 1 раз на 2 роки		
8.4.7	Захист будівель, споруд та зовнішніх установок від прямих попадань блискавки і вторинних її проявів, а також їх перевірку виконано відповідно до вимог ДСТУ EN 62305:2012 «Захист від блискавки» та ДСТУ EN 62305-3:2021 «Блискавкозахист. Частина 3. Фізичні пошкодження будівель (споруд) та небезпека для життя»		
8.4.8	Розміщення електрогенеруючого обладнання (генераторів) та його експлуатація відповідають вимогам правил улаштування електроустановок та інструкції виробника з експлуатації відповідного електрогенеруючого обладнання		
8.4.9	Зберігання палива для електрогенеруючого обладнання (генераторів) здійснюється відповідно до вимог нормативних документів у сфері цивільного захисту, пожежної та техногенної безпеки		
8.4.10	Забезпечено виконання вимог пожежної безпеки щодо утримання електроустановок		
8.5	Системи протипожежного захисту та засоби зв'язку	x	x
8.5.1	Усі системи протипожежного захисту (далі – СПЗ) справні і утримуються в постійній готовності до виконання роботи		
8.5.2	Будинки, приміщення та споруди обладнано СПЗ відповідно до ДБН В.2.5-56:2014 «Системи протипожежного захисту»		
8.5.3	Підтримання експлуатаційної придатності СПЗ проводиться відповідно до вимог технічної документації підприємств-виготовлювачів та затверджених регламентів робіт з технічного обслуговування		
8.5.4	Об'єкти, розташовані за межами населених пунктів, забезпечено засобами зв'язку, які дають можливість		

№ з/п	Найменування критерію/показника оцінювання	Так/ні/частково	Кількість балів
	використання їх для передавання повідомлення про пожежу в будь-який час доби		
8.5.5	СПЗ забезпечені виведенням сигналу пожежної сигналізації на пульт пожежного спостереження		
8.6	Джерела зовнішнього протипожежного водопостачання	x	x
8.6.1	Пожежні гідранти та пожежні резервуари справні і утримуються таким чином, щоб забезпечити безперешкодний забір води пожежними автомобілями		
8.6.2	Протипожежний запас води в резервуарах та штучних водоймах знаходиться на належному рівні		
8.6.3	Пожежні гідранти і водойми мають під'їзди з твердим покриттям. Природні та штучні вододжерела (за наявності) облаштовано майданчиками для забору води		
8.6.4	Пожежні резервуари (водойми) та їх обладнання захищено від замерзання води		
8.6.5	Водонапірні башти забезпечені під'їздом з твердим покриттям і пристосовані для відбору води пожежно-рятувальною технікою будь-якої пори року		
8.6.6	У приміщенні насосної станції наявні: загальна схема протипожежного водопостачання, схема обв'язки насосів і порядок увімкнення насосів-підвищувачів		
8.7	Система внутрішнього протипожежного водопроводу	x	x
8.7.1	Внутрішні пожежні кран-комплекти встановлено в доступних місцях. При цьому їх розміщення не заважає евакуації людей		
8.7.2	Кожен пожежний кран-комплект укомплектовано пожежним рукавом однакового з ним діаметра та стволом, кнопкою дистанційного запуску пожежних насосів (за наявності таких насосів), а також важелем для полегшення відкривання вентиля. Елементи з'єднання пожежного крана, рукавів та ручного пожежного ствола однотипні		
8.7.3	Пожежні кран-комплекти розміщуються у вбудованих або навісних шафках, які мають отвори для провітрювання, і пристосовані для опломбування та візуального огляду їх без розкривання		
8.7.4	Технічне обслуговування і перевірка на справність шляхом пуску води з реєстрацією результатів перевірки у спеціальному журналі обліку технічного обслуговування пожежних кран-комплектів проводяться не рідше одного разу на рік. Пожежні кран-комплекти справні і доступні для використання		
8.7.5	Насосні станції та запірні арматура знаходяться в справному стані		
8.8	Пожежна техніка та первинні засоби пожежогасіння	x	x
8.8.1	Пожежна техніка, у тому числі пожежне обладнання, інвентар та інструменти, використовуються за призначенням		
8.8.2	Територію підприємств, а також будинки, споруди, приміщення, технологічні установки забезпечено первинними засобами пожежогасіння		
8.8.3	Первинні засоби пожежогасіння встановлено в легкодоступних і видимих місцях, а також у		

№ з/п	Найменування критерію/показника оцінювання	Так/ні/частково	Кількість балів
	пожежонебезпечних місцях, де найбільш вірогідна поява осередків пожежі		
8.8.4	Здійснюється технічне обслуговування вогнегасників		
8.9	Стан готовності до дій за призначенням та укомплектованість пожежно-рятувальних підрозділів відомчої пожежної охорони (далі – ВПО) та добровільної пожежної охорони (далі – ДПО)	x	x
8.9.1	У пожежно-рятувальному підрозділі ВПО, ДПО наявна протипожежна техніка забезпечена необхідним пожежно-рятувальним обладнанням та оснащенням		
8.9.2	На об'єкті утворено державні пожежно-рятувальні підрозділи (частини) Оперативно-рятувальної служби цивільного захисту		
8.10	Організаційні заходи щодо забезпечення пожежної безпеки	x	x
8.10.1	На об'єкті наявні розпорядчі документи та інформаційні показники з питань пожежної безпеки		
8.10.2	На об'єкті на видимих місцях вивішені плани (схеми) евакуації людей на випадок пожежі		
8.10.3	Посадові особи та працівники пройшли навчання, протипожежний інструктаж і перевірку знань з питань пожежної безпеки		
8.10.4	Забезпечено дотримання працівниками об'єкта встановленого протипожежного режиму		
8.11	Індивідуальні (типові) технічні рішення щодо додаткових організаційних та інженерних заходів, які передбачені в рамках реалізації Концепції «Країна-фортеця», схваленої постановою Кабінету Міністрів України від 26 квітня 2024 року № 471, та/або концепції протипожежного захисту об'єкта, та/або визначені за результатами обґрунтування відхилень від вимог нормативних документів у сфері цивільного захисту, пожежної та техногенної безпеки, виконуються		
	Техногенна безпека	x	x
8.12	На об'єкті наявні плани локалізації та ліквідації аварій та їх наслідків (у разі віднесення об'єкта до об'єктів підвищеної небезпеки 1, 2 та 3 класів)		
8.13	На об'єкті немає об'єктів з критичним станом виробничих фондів і порушенням умов їх експлуатації		
8.14	Працівників об'єкта забезпечено засобами індивідуального захисту		
8.15	Для інформування населення про небезпеку забезпечено встановлення по периметру небезпечних об'єктів (небезпечних територій) попереджувальних знаків, електронних інформаційних табло тощо		
8.16	Дотримано умови утримання та організації експлуатації автоматизованих систем раннього виявлення загрози виникнення надзвичайних ситуацій (у разі віднесення об'єкта до об'єктів підвищеної небезпеки 1 та 2 класів)		
8.17	Створено об'єктовий матеріальний резерв для запобігання і ліквідації наслідків надзвичайних ситуацій та проведення невідкладних відновлювальних робіт		

№ з/п	Найменування критерію/показника оцінювання	Так/ні/частково	Кількість балів
8.18	Дотримано норми (регламенти) утримання та об'єми зберігання небезпечних хімічних речовин		
8.19	На об'єкті організовано аварійно-рятувальне обслуговування		
8.20	На об'єкті створена та функціонує диспетчерська служба		
8.21	Індивідуальні технічні рішення щодо забезпечення техногенної безпеки, які передбачені концепцією протипожежного захисту об'єкта або визначені за результатами обґрунтування відхилень від вимог нормативних документів у сфері цивільного захисту, пожежної та техногенної безпеки, виконуються		
	Цивільний захист	x	x
8.22	На об'єкті наявні захисні споруди цивільного захисту або споруди подвійного призначення		
8.23	Забезпечено належний стан готовності об'єктів фонду захисних споруд цивільного захисту		
8.24	На об'єкті передбачено використання захисних споруд інших суб'єктів і ці споруди знаходяться в належному стані готовності		
8.25	На об'єкті проведено об'єктові тренування і навчання з питань цивільного захисту		
8.26	Організовано заходи щодо оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій		
8.27	Проведено заходи щодо інженерного захисту джерел водопостачання (захист резервуарів запасу питної води, водозабірних споруд, насосних станцій)		
8.28	На об'єктах фонду захисних споруд цивільного захисту забезпечено наявність недоторканого запасу технічної води та речей першої необхідності		
8.29	На об'єктах підвищеної небезпеки організовано проведення заходів щодо зменшення обсягу запасів небезпечних хімічних, вибухо- і пожежонебезпечних речовин		
8.30	Система опалення, система електроживлення, система водопостачання, система вентиляції, система каналізації захисної споруди цивільного захисту знаходяться у справному стані		
8.31	Вжито заходів для відновлення критично важливих елементів об'єкта критичної інфраструктури, які були пошкоджені		
8.32	Утримання маршрутів виходу до безпечних місць збору у випадку виникнення аварії у належному стані		
8.33	Індивідуальні технічні рішення щодо забезпечення цивільного захисту, які передбачені концепцією протипожежного захисту об'єкта або визначені за результатами обґрунтування відхилень від вимог нормативних документів у сфері цивільного захисту, пожежної та техногенної безпеки, виконуються		
	Кількість балів, знятих за невідповідність інформації:	x	
	Всього балів за критерієм:	x	
	Максимально можлива кількість балів за критерієм:	x	
	Критерій відповідає ознаці:		

№ з/п	Найменування критерію/показника оцінювання	Так/ні/частково	Кількість балів
9	Рівень захисту від епідемії	x	x
9.1	Охоплення персоналу об'єкта критичної інфраструктури профілактичними щепленнями відповідно до календаря профілактичних щеплень проти дифтерії та правця		
9.2	Охоплення персоналу об'єкта критичної інфраструктури щепленнями за станом здоров'я проти грипу		
9.3	Охоплення персоналу об'єкта критичної інфраструктури щепленнями за станом здоров'я проти COVID-19		
9.4	Проходження персоналом об'єкта критичної інфраструктури профілактичних медичних оглядів		
9.5	Незнижувальний запас засобів індивідуального захисту (захисних масок або респіраторів) забезпечено		
9.6	Незнижувальний запас миючих та дезінфекційних засобів для обробки рук персоналу, миття підлоги та обробки робочих поверхонь забезпечено		
9.7	Забезпечено зв'язок (взаємодію) та обмін інформацією функціональним органом (функціональними органами)		x
9.8	Забезпечено належний рівень фінансування та засобами і ресурсами функціонування системи захисту критичної інфраструктури за критерієм «Рівень захисту від епідемії»		x
9.9	Наявність резервів фінансових та матеріальних ресурсів, необхідних для реагування на кризові ситуації та ліквідації їх наслідків за критерієм «Рівень захисту від епідемії»		x
	Кількість балів, знятих за невідповідність інформації:	x	
	Всього балів за критерієм:	x	
	Максимально можлива кількість балів за критерієм:	x	
	Критерій відповідає ознаці:		
10	Рівень захисту від економічного тероризму	x	x
10.1	Виробничі процеси об'єкта критичної інфраструктури не залежать від іноземних суб'єктів господарювання або суб'єктів господарювання із часткою іноземних інвестицій		
10.2	Сировина, обладнання, устаткування або інші матеріали, що необхідні для безперервної роботи об'єкта критичної інфраструктури, не закуповуються в іноземних суб'єктів господарювання або суб'єктів господарювання із часткою іноземних інвестицій		
10.3	Наявність на об'єкті критичної інфраструктури та/або в оператора критичної інфраструктури незнижувального (мобілізаційного) запасу (резерву) речовин, запасних частин, устаткування та обладнання, які повинні забезпечити стаке функціонування об'єкта критичної інфраструктури залежно від часу безперервного функціонування об'єкта критичної інфраструктури		
10.4	Достатня кількість співробітників, які повинні забезпечити стаке функціонування об'єкта критичної інфраструктури залежно від необхідного рівня		
10.5	Відсутність виконавчих проваджень щодо оператора критичної інфраструктури, його основних фондів, оборотних чи необоротних активів, що забезпечують стаке функціонування об'єкта критичної інфраструктури		
10.6	Відсутність заборгованості в оператора критичної інфраструктури		

№ з/п	Найменування критерію/показника оцінювання	Так/ні/частково	Кількість балів
10.7	Виконання оператором критичної інфраструктури зобов'язань за кредитними правочинами		
10.8	Забезпечено зв'язок (взаємодію) та обмін інформацією функціональним органом (функціональними органами)		x
10.9	Забезпечено належний рівень фінансування та засобами і ресурсами функціонування системи захисту критичної інфраструктури за критерієм «Рівень захисту від економічного тероризму»		x
10.10	Наявність резервів фінансових і матеріальних ресурсів, необхідних для реагування на кризові ситуації та ліквідації їх наслідків за критерієм «Рівень захисту від економічного тероризму»		x
	Кількість балів, знятих за невідповідність інформації:	x	
	Всього балів за критерієм:	x	
	Максимально можлива кількість балів за критерієм:	x	
	Критерій відповідає ознаці:		
	Всього балів при оцінці захищеності об'єкта критичної інфраструктури в цілому:	x	
	Максимально можлива сума балів:	x	
	За результатами оцінки захищеності об'єкта критичної інфраструктури присвоюється ознака:		

Дата складання: _____ 20__ року

(голова Комісії з оцінки стану захищеності об'єктів критичної інфраструктури)

(підпис)

(власне ім'я та прізвище)

(найменування посади уповноваженої посадової особи)

(підпис)

(власне ім'я та прізвище)

(найменування посади уповноваженої посадової особи)

(підпис)

(власне ім'я та прізвище)

Додаток 2
до Методики оцінки стану
захищеності об'єктів критичної
інфраструктури
(пункт 16)

**Розрахунок стану захищеності об'єкта критичної інфраструктури за
критерієм «Рівень захисту від епідемії»**

№ з/п	Показник	Ознака	Якщо	Розрахунок, %
1	Охоплення персоналу об'єкта критичної інфраструктури профілактичними щепленнями відповідно до календаря профілактичних щеплень проти дифтерії та правця	так	$\geq 95\%$	від кількості працівників на об'єкті критичної інфраструктури
		частково	$\geq 75\%$ та $< 95\%$	
		ні	$< 75\%$	
2	Охоплення персоналу об'єкта критичної інфраструктури щепленнями за станом здоров'я проти грипу	так	$\geq 95\%$	щеплених від загальної кількості групи ризику
		частково	$\geq 75\%$ та $< 95\%$	
		ні	$< 75\%$	
3	Охоплення персоналу об'єкта критичної інфраструктури щепленнями за станом здоров'я проти COVID-19	так	$\geq 95\%$	щеплених від загальної кількості групи ризику
		частково	$\geq 75\%$ та $< 95\%$	
		ні	$< 75\%$	
4	Проходження персоналом об'єкта критичної інфраструктури профілактичних медичних оглядів	так	100 %	від кількості працівників на об'єкті критичної інфраструктури
		частково	$\geq 85\%$ та $< 100\%$	
		ні	$< 85\%$	
5	Незнижувальний запас засобів індивідуального захисту (захисних масок або респіраторів) забезпечено	так	100 %	відсоток від розрахунку
		частково	$\geq 90\%$ та $< 100\%$	
		ні	$< 90\%$	

6	Незнижувальний запас миючих та дезінфекційних засобів для обробки рук персоналу, миття підлоги та обробки робочих поверхонь забезпечено	так	100 %	відсоток від розрахунку
		частково	$\geq 90\%$ та $< 100\%$	
		ні	$< 90\%$	

Додаток 3
до Методики оцінки стану
захищеності об'єктів критичної
інфраструктури
(пункт 17)

**Розрахунок стану захищеності об'єкта критичної інфраструктури за
критерієм «Забезпечення кіберзахисту об'єкта критичної інфраструктури»**

№ з/п	Показник	Ознака	Якщо	Розрахунок, %
1	Наявність визначеної посадової особи, відповідальної за кіберзахист об'єкта критичної інфраструктури, та наявність підрозділу, відповідального за кіберзахист об'єкта критичної інфраструктури	так	Обидва показники виконуються	—
		частково	Виконується один з показників	
		ні	Не виконується жоден з показників	
2	Забезпечено виконання загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518	так	$\geq 70\%$ та $< 100\%$	Відсоток виконаних вимог від загальної кількості вимог до кіберзахисту
		частково	$\geq 30\%$ та $< 70\%$	
		ні	$< 30\%$	
3	Затверджено політику інформаційної безпеки на об'єкті критичної інфраструктури, що включає: парольну політику; порядок управління обліковими записами; порядок резервування даних та компонентів, зберігання резервних копій даних; порядок відновлення даних з резервних копій та заміни компонентів у випадку виходу їх з ладу;	так	7 пунктів	—
		частково	< 7 пунктів	
		ні	не затверджено	

№ з/п	Показник	Ознака	Якщо	Розрахунок, %
	план забезпечення безперервної діяльності; порядок управління оновленнями; порядок реагування на кіберінциденти/кібератаки			
4	Проведено оцінку ризиків інформаційної безпеки об'єкта критичної інфраструктури	так	Ризики ідентифікован о, проаналізован о, оцінено та вжито заходів щодо їх прийняття та/або пом'якшення	—
		частково	Ризики ідентифікован о, проаналізован о	
		ні	Оцінка ризиків не проведена	
5	Проведено внутрішній та незалежний аудити інформаційної безпеки на об'єкті критичної інфраструктури	так	Проведено 2 види аудиту інформаційної безпеки (відповідно до перелічених)	—
		частково	Проведено 1 вид аудиту інформаційної безпеки (відповідно до перелічених)	

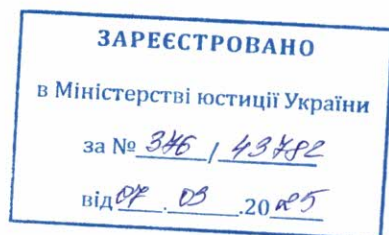
№ з/п	Показник	Ознака	Якщо	Розрахунок, %
		ні	Не проведено жоден з перелічених видів аудиту інформаційної безпеки	
6	Проведено перевірку ефективності заходів щодо захисту мереж та систем об'єкта критичної інфраструктури від зовнішнього проникнення шляхом виконання тесту на проникнення (Penetration test)	так	Перевірка проводиться щорічно (протягом останніх трьох років)	—
		частково	Проведено лише одну перевірку за останні три роки	
		ні	Не проведено жодної перевірки за останні три роки	

Додаток 4
до Методики оцінки стану
захищеності об'єктів критичної
інфраструктури
(пункт 18)

**Розрахунок стану захищеності об'єкта критичної інфраструктури за
критерієм «Рівень захисту від економічного тероризму»**

№ з/п	Показник	Ознака	Якщо	Розрахунок, %
1	Виробничі процеси об'єкта критичної інфраструктури не залежать від іноземних суб'єктів господарювання або суб'єктів господарювання із часткою іноземних інвестицій	так	$\geq 50\%$	до загального обсягу виробничих процесів
		частково	$\geq 25\%$ та $< 50\%$	
		ні	$< 25\%$	
2	Сировина, обладнання, устаткування або інші матеріали, що необхідні для безперервної роботи об'єкта критичної інфраструктури, не закуповуються в іноземних суб'єктів господарювання або суб'єктів господарювання із часткою іноземних інвестицій	так	$\geq 50\%$	до загального обсягу необхідного обсягу
		частково	$\geq 25\%$ та $< 50\%$	
		ні	$< 25\%$	
3	Наявність на об'єкті критичної інфраструктури та/або в оператора критичної інфраструктури незнижувального (мобілізаційного) запасу (резерву) речовин, запасних частин, устаткування та обладнання, які повинні забезпечити стаке функціонування об'єкта критичної інфраструктури залежно від часу безперервного функціонування об'єкта критичної інфраструктури	так	≥ 3 тижні	—
		частково	≥ 2 та < 3 тижнів	
		ні	< 2 тижнів	

	Показник	Ознака	Якщо	Розрахунок, %
4	Достатня кількість співробітників, які повинні забезпечити стає функціонування об'єкта критичної інфраструктури залежно від необхідного рівня	так	$\geq 90\%$	до загальної кількості необхідних працівників
		частково	$\geq 50\%$ та $< 90\%$	
		ні	$< 50\%$	
5	Відсутність виконавчих проваджень щодо оператора критичної інфраструктури, його основних фондів, оборотних чи необоротних активів, що забезпечують стає функціонування об'єкта критичної інфраструктури	так	так	—
		частково	на суму до 5 млн грн	
		ні	на суму понад 5 млн грн	
6	Відсутність заборгованості в оператора критичної інфраструктури	так	так	—
		частково	буде погашена протягом 3 місяців	
		ні	буде погашена у період 3 місяців і більше	
7	Виконання оператором критичної інфраструктури зобов'язань за кредитними правочинами	так	так	від доходу оператора критичної інфраструктури
		частково	кредитні зобов'язання до 40%	
		ні	кредитні зобов'язання понад 40%	



ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної
служби спеціального зв'язку та
захисту інформації України
14 січня 2025 року № 17

**Критерії і показники
оцінки стану захищеності об'єктів критичної інфраструктури**

№ з/п	Критерій оцінювання	Показник оцінювання
1	Документальне оформлення оператором критичної інфраструктури заходів із забезпечення захисту та стійкості об'єкта критичної інфраструктури	Наявність структурного підрозділу режимно-секретного органу (РСО)
1.1		Наявність паспорта безпеки на об'єкт критичної інфраструктури
1.2		Наявність загальної характеристики об'єкта критичної інфраструктури
1.3		Наявність ідентифікованих проектних загроз національного, секторального (у разі затвердження) та об'єктового (за наявності) рівнів
1.4		Наявність розробленого плану захисту об'єкта критичної інфраструктури за кожною із проектних загроз національного, секторального (у разі затвердження) та об'єктового (за наявності) рівнів
1.5		Наявність розроблених вимог щодо організації захисту об'єкта критичної інфраструктури
1.6		Виконано заходи, рекомендовані оператору критичної
1.7		

№ з/п	Критерій оцінювання	Показник оцінювання
		інфраструктури за результатами проведення попереднього моніторингу рівня безпеки об'єкта критичної інфраструктури
1.8		Наявність розробленого об'єктового плану заходів щодо захисту і забезпечення стійкості об'єкта критичної інфраструктури
1.9		Наявність розроблених правил управління ризиками безпеки
1.10		Наявність розробленого плану локалізації та ліквідації наслідків аварій
1.11		Оператором критичної інфраструктури розроблено політику інформаційної безпеки, політику управління ризиками інформаційної безпеки, методику оцінювання та оброблення ризиків інформаційної безпеки
1.12		Наявність посадових інструкцій осіб, відповідальних за організацію та забезпечення захисту об'єкта критичної інфраструктури
1.13		Забезпечено постійну взаємодію з підприємствами, які забезпечують централізоване водопостачання, централізоване водовідведення, постачання теплової енергії, енергопостачання, функціонування електронних комунікаційних мереж, транспортне обслуговування, медичну допомогу, безпеку та

№ з/п	Критерій оцінювання	Показник оцінювання
		інші послуги, від яких залежить процес реагування на кризові ситуації та відновлення функціонування об'єктів критичної інфраструктури (наявність договорів з підприємствами/надавачами послуг)
1.14		Погоджено план захисту об'єкта критичної інфраструктури за кожною з проектних загроз відповідним функціональним органом (органами)
1.15		Погоджено паспорт безпеки на об'єкт критичної інфраструктури відповідним секторальним органом
1.16		Забезпечено належний рівень фінансування заходів безпеки об'єкта критичної інфраструктури та матеріально-технічної спроможності
2	Рівень фінансування об'єкта критичної інфраструктури	
2.1		Забезпечено належний рівень фінансування та засобами і ресурсами функціонування системи захисту критичної інфраструктури
2.2		Наявність резервів фінансових та матеріальних ресурсів, необхідних для реагування на кризові ситуації та ліквідації їх наслідків
3.	Рівень взаємодії оператора критичної інфраструктури з іншими суб'єктами національної системи захисту критичної	
3.1		Забезпечено зв'язок (взаємодію) із суб'єктами національної системи захисту критичної

№ з/п	Критерій оцінювання	Показник оцінювання
	інфраструктури	інфраструктури
3.2		Організовано обмін інформацією про ризики та загрози з іншими суб'єктами національної системи захисту критичної інфраструктури
3.3		Створено умови для належного виконання правоохоронними органами, розвідувальними органами та органами, що здійснюють контррозвідувальну діяльність, і їх підрозділами завдань із захисту об'єкта критичної інфраструктури
3.4		Організовано заходи з реагування на інциденти, кризові ситуації, а також ліквідації їх наслідків на об'єкті критичної інфраструктури у взаємодії з іншими суб'єктами національної системи захисту критичної інфраструктури
4	Загальний рівень забезпечення захисту та стійкості об'єкта критичної інфраструктури	
4.1		Проведено оцінку ризиків
4.2		Забезпечується виконання вимог щодо організації захисту об'єкта критичної інфраструктури
4.3		Розроблені вимоги щодо організації захисту об'єкта критичної інфраструктури відповідають вимогам секторального органу (за наявності таких вимог)
4.4		Забезпечується виконання вимог секторального органу щодо захисту об'єкта критичної інфраструктури (за наявності

№ з/п	Критерій оцінювання	Показник оцінювання
		таких вимог)
4.5		Забезпечується виконання плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «Удари засобами повітряного нападу та ракетно-артилерійські удари (обстріли)»
4.6		Забезпечується виконання плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «Терористичний акт або диверсія»
4.7		Забезпечується виконання плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «Кібератака/кіберінцидент»
4.8		Забезпечується виконання плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «Пожежі та вибухи»
4.9		Забезпечується виконання плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «Епідемія»
4.10		Забезпечується виконання плану захисту об'єкта критичної інфраструктури за проектною загрозою національного рівня «Економічний тероризм»
4.11		Забезпечується виконання плану захисту об'єкта критичної інфраструктури за проектними загрозами секторального рівня (у разі затвердження)

№ з/п	Критерій оцінювання	Показник оцінювання
4.12		Забезпечується виконання плану захисту об'єкта критичної інфраструктури за проектними загрозами об'єктового рівня (за наявності)
4.13		Забезпечується виконання правил управління ризиками безпеки
4.14		Забезпечується виконання об'єктового плану заходів щодо захисту і забезпечення стійкості об'єкта критичної інфраструктури
4.15		Забезпечується виконання плану локалізації та ліквідації наслідків аварій
5	Стан інженерного захисту об'єкта критичної інфраструктури	Оцінка за Методикою оцінювання стану інженерного захисту об'єктів критичної інфраструктури, затвердженою постановою Кабінету Міністрів України від 26 квітня 2024 року № 471
5.1		
5.2		
5.3		
5.4		
		Забезпечено зв'язок (взаємодію) та обмін інформацією з функціональним органом (функціональними органами)
		Забезпечено належний рівень фінансування та засобами і ресурсами функціонування системи захисту критичної інфраструктури за критерієм «Стан інженерного захисту об'єкта критичної інфраструктури»
		Наявність резервів фінансових та матеріальних ресурсів,

№ з/п	Критерій оцінювання	Показник оцінювання
		необхідних для реагування на кризові ситуації та ліквідації їх наслідків за критерієм «Стан інженерного захисту об'єкта критичної інфраструктури»
6	Рівень захисту від терористичних актів та диверсій	
6.1		Наявність витягу з превентивного плану проведення антитерористичної операції на об'єкті критичної інфраструктури в частині дій персоналу та охорони
6.2		Забезпечено зв'язок (взаємодію) та обмін інформацією з функціональним органом (функціональними органами)
6.3		Забезпечено належний рівень фінансування та засобами і ресурсами функціонування системи захисту критичної інфраструктури за критерієм «Рівень захисту від терористичних атак та диверсій»
6.4		Наявність резервів фінансових і матеріальних ресурсів, необхідних для реагування на кризові ситуації та ліквідації їх наслідків за критерієм «Рівень захисту від терористичних атак та диверсій»
Забезпеченість охороною та належним інженерно-технічним оснащенням для запобігання неправомірному проникненню на об'єкті критичної інфраструктури сторонніх осіб		
6.5		Наявність необхідних інженерно-технічних засобів
6.5.1		Огорожа по всьому периметру об'єкта критичної

№ з/п	Критерій оцінювання	Показник оцінювання
		інфраструктури не нижче 2 метрів (залізобетонна, цегляна, секційна з металевих прутів, із металевої сітки на стовпах)
6.5.2		Підступи до об'єкта критичної інфраструктури розчищені від кущів та чагарників до 50 метрів від зовнішнього периметра огорожі, проріджені дерева, нижні сучки та гілки обрізані до висоти 2,5 метра, трава скошена, зайвих предметів немає
6.5.3		Підступи до об'єкта критичної інфраструктури освітлюються світильниками, прожекторами направленої дії
6.6		Наявність режиму контролюваного допуску осіб і транспортних засобів
6.7		Наявність технічних засобів охорони локального рівня
6.8		Наявність на об'єктах засобів охоронного призначення, на тривожні сповіщення яких реагують органи державної влади, підприємства та організації
6.9		Наявність автономного електроживлення
Наявність погоджених/затверджених Антитерористичним центром при Службі безпеки України або його координаційними групами інструкцій з питань реагування на загрозу вчинення або вчинення терористичного акту/диверсії на об'єкті критичної інфраструктури		
6.10		Наявність інструкцій щодо порядку дій персоналу у разі встановлення керівником Антитерористичного центру при

№ з/п	Критерій оцінювання	Показник оцінювання
		Службі безпеки України відповідних рівнів терористичної загрози
6.11		Наявність інструкцій щодо порядку дій персоналу у разі отримання погроз терористичного характеру
6.12		Наявність інструкцій щодо порядку дій персоналу у разі виявлення підозрілих предметів з ознаками вибухового чи іншого небезпечного пристрою
6.13		Наявність інструкцій щодо порядку дій персоналу у разі вчинення на об'єкті критичної інфраструктури чи прилеглий території вибуху чи інших дій, які спричинили людські жертви
6.14		Наявність інструкцій щодо порядку дій персоналу у разі вчинення терористичного акту шляхом захоплення та утримання заручників
Стан організації фізичної охорони об'єкта критичної інфраструктури		
6.15		Наявність озброєної охорони, яка в установленому законодавством порядку має право на використання та застосування зброї і застосування заходів примусу в разі визначення на об'єкті першочергових дій, яких необхідно вжити для недопущення збільшення негативних наслідків
6.16		Наявність структурного підрозділу/відповідальних осіб з питань забезпечення

№ з/п	Критерій оцінювання	Показник оцінювання
		антитерористичної захищеності
6.17		Проведено перевірку знань персоналу об'єкта критичної інфраструктури щодо реагування на можливі загрози під час тренувань, командно-штабних і тактико-спеціальних навчань з антитерористичної тематики
6.18		Наявність на постах охорони об'єктів ручних систем тривожної сигналізації, на тривожні сповіщення яких реагують органи державної влади, підприємства та організації
7	Забезпечення кіберзахисту об'єкта критичної інфраструктури	
7.1		Наявність визначеної посадової особи, відповідальної за кіберзахист об'єкта критичної інфраструктури, та наявність підрозділу, відповідального за кіберзахист об'єкта критичної інфраструктури
7.2		Забезпечено виконання Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518
7.3		Проведено оцінку ризиків інформаційної безпеки об'єкта критичної інфраструктури
7.4		Затверджено політику інформаційної безпеки на об'єкті критичної інфраструктури
7.5		Проведено внутрішній та незалежний аудити

№ з/п	Критерій оцінювання	Показник оцінювання
		інформаційної безпеки на об'єкті критичної інфраструктури
7.6		Забезпечено зв'язок (взаємодію) та обмін інформацією з функціональним органом (функціональними органами)
7.7		Проведено перевірку ефективності заходів щодо захисту мереж і систем об'єкта критичної інфраструктури від зовнішнього проникнення шляхом виконання тесту на проникнення (Penetration test)
7.8		Забезпечено належний рівень фінансування та засобами і ресурсами функціонування системи захисту критичної інфраструктури за критерієм «Забезпечення кіберзахисту об'єкта критичної інфраструктури»
7.9		Наявність резервів фінансових та матеріальних ресурсів, необхідних для реагування на кризові ситуації та ліквідації їх наслідків за критерієм «Забезпечення кіберзахисту об'єкта критичної інфраструктури»
8	Цивільний захист, пожежна та техногенна безпека	
8.1	Утримання території	
8.1.1		Під час експлуатації об'єкта не зменшено мінімальні протипожежні відстані між будівлями, спорудами, установками, відкритими

№ з/п	Критерій оцінювання	Показник оцінювання
		майданчиками, місцями для зберігання матеріалів
8.1.2		Автомобільні дороги, проїзди й проходи до будівель, споруд, пожежних вододжерел, підступи до зовнішніх стаціонарних пожежних драбин, пожежного інвентарю, обладнання та засобів пожежогасіння вільні, утримуються справними, взимку очищаються від снігу
8.1.3		Автомобільні дороги та проїзди для пожежних машин мають дорожнє покриття, придатне для їх проїзду
8.1.4		Протипожежні відстані між будівлями, спорудами не використовуються для складування матеріалів, устаткування, стоянок транспорту, будівництва та встановлення тимчасових будинків і споруд, у тому числі мобільних (інвентарних) будівель, окрім захисних інженерних споруд
8.1.5		На території об'єкта забезпечено освітлення зовнішніх пожежних драбин, протипожежного обладнання, входів до будинків та споруд
8.1.6		Забезпечено інженерний захист наземних будівель (споруд) насосної станції пожежогасіння, наземних резервуарів запасів вогнегасних речовин для цілей пожежогасіння, трубопроводів (сухотрубів) систем

№ з/п	Критерій оцінювання	Показник оцінювання
		пожежогасіння, а також розподільчих вузлів систем пожежогасіння трансформаторів
8.1.7		Забезпечено улаштування та належне утримання додаткових проходів (отворів) у захисті, що забезпечують доступ пожежно-рятувальних підрозділів для можливості подачі вогнегасних речовин для цілей пожежогасіння.
8.1.8		Під час улаштування додаткового протиуламкового захисту у верхній частині захисних конструкцій із габіонів використано негорючі матеріали
8.1.9		Забезпечено влаштування автоматичних систем пожежогасіння трансформаторів та вибухо-, пожежонебезпечного обладнання, розташованого під захисними конструкціями типу «Шелтер»
8.1.10		Передбачено заходи з блискавкозахисту та захисту від вторинних проявів блискавки захисної конструкції типу «Шелтер»
8.1.11		Передбачено додатковий захист пультів управління з використанням протипожежних дверей, вікон та клапанів систем вентиляції з класом вогнестійкості не нижче EI 90.
8.1.12		Передбачено влаштування додаткових незалежних джерел електроживлення (дизельних генераторів) для насосів систем

№ з/п	Критерій оцінювання	Показник оцінювання
		протипожежного водопостачання та стаціонарних систем пожежогасіння для забезпечення безперебійної подачі вогнегасних речовин для цілей пожежогасіння в умовах повного знеструмлення об'єкта критичної інфраструктури
8.1.13		Наявність інженерного захисту приміщень, будинків та зовнішніх установок категорій А, Б за вибухопожежною та пожежною небезпекою
8.1.14		Вжиття додаткових інженерних заходів щодо обмеження можливого поширення пожежі на суміжні об'єкти (влаштування додаткових бар'єрів, обвалування, протипожежних стін тощо)
8.2	Утримання будинків, приміщень і споруд	
8.2.1		Керівник об'єкта забезпечив утримання засобів протипожежного захисту у справному стані та їх технічне обслуговування
8.2.2		Протипожежні двері, ворота, вікна, люки, клапани, завіси (екрани) у протипожежних перешкодах утримуються у справному стані. Будь-які пристрої, предмети тощо, що перешкоджають їх зачиненню, не встановлено
8.2.3		У будинках, крім будинків V ступеня вогнестійкості, дерев'яні елементи горищних покриттів (крокви, лати) оброблені засобами

№ з/п	Критерій оцінювання	Показник оцінювання
		вогнезахисту, які забезпечують I групу вогнезахисної ефективності
8.2.4		Класи вогнестійкості будівельних конструкцій і групи поширення вогню по цих конструкціях відповідають будівельним нормам. Вогнезахист металевих конструкцій забезпечено згідно з вимогами законодавства у сфері цивільного захисту, пожежної та техногенної безпеки
8.2.5		Горища, технічні, підвальні, цокольні та інші приміщення (у тому числі вентиляційні камери, електрощитові) використовуються за призначенням, виробничі і складські дільниці в них не розміщуються, сторонніми предметами їх не засмічено та не захащено
8.2.6		Стаціонарні зовнішні пожежні сходи, сходи на перепадах висот і огорожі на покриттях будівель та споруд утримуються справними
8.2.7		У разі потреби встановлення на вікнах приміщень, де перебувають люди, ґрат вони розкриваються, розсуваються або знімаються
8.3	Утримання евакуаційних шляхів і виходів	
8.3.1		Кількість та розміри евакуаційних виходів з будівель і приміщень не зменшено
8.3.2		У приміщенні, яке має один евакуаційний вихід, одночасно

№ з/п	Критерій оцінювання	Показник оцінювання
		розміщено (перебуває) не більше ніж 50 осіб
8.3.3		Двері на шляхах евакуації відчиняються в напрямку виходу з будівель (приміщень)
8.3.4		Сходові марші і площадки мають справні огорожі із поручнями, котрі не зменшують ширину сходових маршів і площадок
8.3.5		Сходові клітки, внутрішні відкриті та зовнішні сходи, коридори, проходи та інші шляхи евакуації забезпечені евакуаційним освітленням
8.3.6		Індивідуальні технічні рішення щодо евакуаційних шляхів і виходів, які передбачені концепцією протипожежного захисту об'єкта або визначені за результатами обґрунтування відхилень від вимог нормативних документів у сфері цивільного захисту, пожежної та техногенної безпеки виконуються
8.4	Стан утримання електроустановок	
8.4.1		Електричні машини, апарати, обладнання, електропроводи та кабелі за виконанням та ступенем захисту відповідають класу зони згідно з правилами улаштування електроустановок, мають апаратуру захисту від струмів короткого замикання та інших аварійних режимів
8.4.2		З'єднання, відгалуження та окінцювання жил проводів і кабелів здійснено за допомогою

№ з/п	Критерій оцінювання	Показник оцінювання
		опресування, зварювання, паяння або затискачів
8.4.3		В електропроводках вибухонебезпечних і пожежонебезпечних зон відгалужувальні та з'єднувальні коробки закриті кришками з негорючих або важкогорючих матеріалів
8.4.4		Відстань від кабелів та ізолюваних проводів, прокладених відкрито, до місць відкритого зберігання (розміщення) горючих матеріалів не менше ніж 1 метр
8.4.5		Електророзетки, вимикачі, перемикачі та інші подібні апарати встановлені на не горючі основи (конструкції)
8.4.6		Замірювання опору ізоляції і перевірка спрацювання приладів захисту електричних мереж та електроустановок від короткого замикання проводяться 1 раз на 2 роки
8.4.7		Захист будівель, споруд та зовнішніх установок від прямих попадань блискавки і вторинних її проявів, а також їх перевірку виконано відповідно до вимог ДСТУ EN 62305:2012 «Захист від блискавки» та ДСТУ EN 62305-3:2021 «Блискавкозахист. Частина 3. Фізичні пошкодження будівель (споруд) та безпека для життя»
8.4.8		Розміщення електрогенеруючого обладнання (генераторів) та його

№ з/п	Критерій оцінювання	Показник оцінювання
		експлуатація відповідають вимогам правил улаштування електроустановок та інструкції виробника з експлуатації відповідного електрогенеруючого обладнання
8.4.9		Зберігання палива для електрогенеруючого обладнання (генераторів) здійснюється відповідно до вимог нормативних документів у сфері цивільного захисту, пожежної та техногенної безпеки
8.4.10		Забезпечено виконання вимог пожежної безпеки щодо утримання електроустановок
8.5	Системи протипожежного захисту та засоби зв'язку	
8.5.1		Усі системи протипожежного захисту (далі – СПЗ) справні і утримуються в постійній готовності до виконання роботи
8.5.2		Будинки, приміщення та споруди обладнано СПЗ відповідно до ДБН В.2.5-56:2014 «Системи протипожежного захисту»
8.5.3		Підтримання експлуатаційної придатності СПЗ проводиться відповідно до вимог технічної документації підприємств-виготовлювачів та затверджених регламентів робіт з технічного обслуговування
8.5.4		Об'єкти, розташовані за межами населених пунктів, забезпечено засобами зв'язку, які дають можливість використання їх для передавання повідомлення про

№ з/п	Критерій оцінювання	Показник оцінювання
		пожежу в будь-який час доби
8.5.5		СПЗ забезпечені виведенням сигналу пожежної сигналізації на пульт пожежного спостерігання
8.6	Джерела зовнішнього протипожежного водопостачання	
8.6.1		Пожежні гідранти та пожежні резервуари справні і утримуються таким чином, щоб забезпечити безперешкодний забір води пожежними автомобілями
8.6.2		Протипожежний запас води в резервуарах і штучних водоймах знаходиться на належному рівні
8.6.3		Пожежні гідранти і водойми мають під'їзди з твердим покриттям. Природні та штучні вододжерела (за наявності) облаштовано майданчиками для забору води
8.6.4		Пожежні резервуари (водойми) та їх обладнання захищено від замерзання води
8.6.5		Водонапірні башти забезпечені під'їздом з твердим покриттям і пристосовані для відбору води пожежно-рятувальною технікою будь-якої пори року
8.6.6		У приміщенні насосної станції наявні: загальна схема протипожежного водопостачання, схема обв'язки насосів і порядок увімкнення насосів-підвищувачів

№ з/п	Критерій оцінювання	Показник оцінювання
8.7	Система внутрішнього протипожежного водопроводу	
8.7.1		Внутрішні пожежні кран-комплекти встановлено в доступних місцях. При цьому їх розміщення не заважає евакуації людей
8.7.2		Кожен пожежний кран-комплект укомплектовано пожежним рукавом однакового з ним діаметра та стволом, кнопкою дистанційного запуску пожежних насосів (за наявності таких насосів), а також важелем для полегшення відкривання вентилі. Елементи з'єднання пожежного крана, рукавів та ручного пожежного ствола однотипні
8.7.3		Пожежні кран-комплекти розміщуються у вбудованих або навісних шафках, які мають отвори для провітрювання і пристосовані для опломбування та візуального огляду їх без розкривання
8.7.4		Технічне обслуговування і перевірка на справність шляхом пуску води з реєстрацією результатів перевірки в спеціальному журналі обліку технічного обслуговування пожежних кран-комплектів проводяться не рідше одного разу на рік. Пожежні кран-комплекти справні і доступні для використання
8.7.5		Насосні станції та запірна арматура знаходяться в справному стані

№ з/п	Критерій оцінювання	Показник оцінювання
8.8	Пожежна техніка та первинні засоби пожежогашіння	
8.8.1		Пожежна техніка, у тому числі пожежне обладнання, інвентар та інструменти, використовуються за призначенням
8.8.2		Територію підприємств, а також будинки, споруди, приміщення, технологічні установки забезпечено первинними засобами пожежогашіння
8.8.3		Первинні засоби пожежогашіння встановлено в легкодоступних та видимих місцях, а також у пожежонебезпечних місцях, де найбільш вірогідна поява осередків пожежі
8.8.4		Здійснюється технічне обслуговування вогнегасників
8.9	Стан готовності до дій за призначенням та укомплектованість пожежно-рятувальних підрозділів відомчої пожежної охорони (далі – ВПО) та добровільної пожежної охорони (далі – ДПО)	
8.9.1		У пожежно-рятувальному підрозділі ВПО, ДПО наявна протипожежна техніка забезпечена необхідним пожежно-рятувальним обладнанням та оснащенням
8.9.2		На об'єкті утворено державні пожежно-рятувальні підрозділи (частини) Оперативно-рятувальної служби цивільного захисту
8.10	Організаційні заходи щодо забезпечення пожежної безпеки	
8.10.1		На об'єкті наявні розпорядчі документи та інформаційні

№ з/п	Критерій оцінювання	Показник оцінювання
		покажчики з питань пожежної безпеки
8.10.2		На об'єкті на видимих місцях вивішені плани (схеми) евакуації людей на випадок пожежі
8.10.3		Посадові особи та працівники пройшли навчання, протипожежний інструктаж і перевірку знань з питань пожежної безпеки
8.10.4		Забезпечено дотримання працівниками об'єкта встановленого протипожежного режиму
8.11		Індивідуальні (типові) технічні рішення щодо додаткових організаційних та інженерних заходів, які передбачені в рамках реалізації Концепції «Країна фортеця», схваленої постановою Кабінету Міністрів України від 26 квітня 2024 року № 471, та/або концепції протипожежного захисту об'єкта, та/або визначені за результатами обґрунтування відхилень від вимог нормативних документів у сфері цивільного захисту, пожежної та техногенної безпеки, виконуються
Техногенна безпека		
8.12		На об'єкті наявні плани локалізації та ліквідації аварій та їх наслідків (у разі віднесення об'єкта до об'єктів підвищеної небезпеки 1, 2 та 3 класів)
8.13		На об'єкті немає об'єктів з критичним станом виробничих

№ з/п	Критерій оцінювання	Показник оцінювання
		фондів і порушенням умов їх експлуатації
8.14		Працівників об'єкта забезпечено засобами індивідуального захисту
8.15		Для інформування населення про небезпеку забезпечено встановлення по периметру небезпечних об'єктів (небезпечних територій) попереджувальних знаків, електронних інформаційних табло тощо
8.16		Дотримано умови утримання та організації експлуатації автоматизованих систем раннього виявлення загрози виникнення надзвичайних ситуацій (у разі віднесення об'єкта до об'єктів підвищеної небезпеки 1 та 2 класів)
8.17		Створено об'єктовий матеріальний резерв для запобігання і ліквідації наслідків надзвичайних ситуацій і проведення невідкладних відновлювальних робіт
8.18		Дотримано норми (регламенти) утримання та об'єми зберігання небезпечних хімічних речовин
8.19		На об'єкті організовано аварійно-рятувальне обслуговування
8.20		На об'єкті створена та функціонує диспетчерська служба
8.21		Індивідуальні технічні рішення щодо забезпечення техногенної

№ з/п	Критерій оцінювання	Показник оцінювання
		безпеки, які передбачені концепцією протипожежного захисту об'єкта або визначені за результатами обґрунтування відхилень від вимог нормативних документів у сфері цивільного захисту, пожежної та техногенної безпеки, виконуються
Цивільний захист		
8.22		На об'єкті наявні захисні споруди цивільного захисту або споруди подвійного призначення
8.23		Забезпечено належний стан готовності об'єктів фонду захисних споруд цивільного захисту
8.24		На об'єкті передбачено використання захисних споруд інших суб'єктів і ці споруди знаходяться в належному стані готовності
8.25		На об'єкті проведено об'єктові тренування і навчання з питань цивільного захисту
8.26		Організовано заходи щодо оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій
8.27		Проведено заходи щодо інженерного захисту джерел водопостачання (захист резервуарів запасу питної води, водозабірних споруд, насосних станцій)
8.28		На об'єктах фонду захисних споруд цивільного захисту забезпечено наявність

№ з/п	Критерій оцінювання	Показник оцінювання
		недоторканого запасу технічної води та речей першої необхідності
8.29		На об'єктах підвищеної небезпеки організовано проведення заходів щодо зменшення обсягу запасів небезпечних хімічних, вибухо- і пожежонебезпечних речовин
8.30		Система опалення, система електроживлення, система водопостачання, система вентиляції, система каналізації захисної споруди цивільного захисту знаходяться у справному стані
8.31		Вжито заходів для відновлення критично важливих елементів об'єкта критичної інфраструктури, які були пошкоджені
8.32		Утримання маршрутів виходу до безпечних місць збору у випадку виникнення аварії в належному стані
8.33		Індивідуальні технічні рішення щодо забезпечення цивільного захисту, які передбачені концепцією протипожежного захисту об'єкта або визначені за результатами обґрунтування відхилень від вимог нормативних документів у сфері цивільного захисту, пожежної та техногенної безпеки, виконуються

№ з/п	Критерій оцінювання	Показник оцінювання
9	Рівень захисту від епідемії	
9.1		Охоплення персоналу об'єкта критичної інфраструктури профілактичними щепленнями відповідно до календаря профілактичних щеплень проти дифтерії та правця
9.2		Охоплення персоналу об'єкта критичної інфраструктури щепленнями за станом здоров'я проти грипу
9.3		Охоплення персоналу об'єкта критичної інфраструктури щепленнями за станом здоров'я проти COVID-19
9.4		Проходження персоналом об'єкта критичної інфраструктури профілактичних медичних оглядів
9.5		Незнижувальний запас засобів індивідуального захисту (захисних масок або респіраторів) забезпечено
9.6		Незнижувальний запас миючих та дезінфекційних засобів для обробки рук персоналу, миття підлоги та обробки робочих поверхонь забезпечено
9.7		Забезпечено зв'язок (взаємодію) та обмін інформацією функціональним органом (функціональними органами)
9.8		Забезпечено належний рівень фінансування та засобами і ресурсами функціонування системи захисту критичної

№ з/п	Критерій оцінювання	Показник оцінювання
		інфраструктури за критерієм «Рівень захисту від епідемії»
9.9		Наявність резервів фінансових та матеріальних ресурсів, необхідних для реагування на кризові ситуації та ліквідації їх наслідків за критерієм «Рівень захисту від епідемії»
10	Рівень захисту від економічного тероризму	
10.1		Виробничі процеси об'єкта критичної інфраструктури не залежать від іноземних суб'єктів господарювання або суб'єктів господарювання із часткою іноземних інвестицій
10.2		Сировина, обладнання, устаткування або інші матеріали, що необхідні для безперервної роботи об'єкта критичної інфраструктури, не закуповуються в іноземних суб'єктів господарювання або суб'єктів господарювання із часткою іноземних інвестицій
10.3		Наявність на об'єкті критичної інфраструктури та/або в оператора критичної інфраструктури незнижувального (мобілізаційного) запасу (резерву) речовин, запасних частин, устаткування та обладнання, які повинні забезпечити стаłe функціонування об'єкта критичної інфраструктури залежно від часу безперервного функціонування об'єкта

№ з/п	Критерій оцінювання	Показник оцінювання
		критичної інфраструктури
10.4		Достатня кількість співробітників, які повинні забезпечити стає функціонування об'єкта критичної інфраструктури залежно від необхідного рівня
10.5		Відсутність виконавчих проваджень щодо оператора критичної інфраструктури, його основних фондів, оборотних чи необоротних активів, що забезпечують стає функціонування об'єкта критичної інфраструктури
10.6		Відсутність заборгованості в оператора критичної інфраструктури
10.7		Виконання оператором критичної інфраструктури зобов'язань за кредитними правочинами
10.8		Забезпечено зв'язок (взаємодію) та обмін інформацією функціональним органом (функціональними органами)
10.9		Забезпечено належний рівень фінансування та засобами і ресурсами функціонування системи захисту критичної інфраструктури за критерієм «Рівень захисту від економічного тероризму»
10.10		Наявність резервів фінансових і матеріальних ресурсів, необхідних для реагування на кризові ситуації та ліквідації їх наслідків за критерієм «Рівень

№ з/п	Критерій оцінювання	Показник оцінювання
		захисту від економічного тероризму»

Директор Департаменту
захисту критичної інфраструктури
Адміністрації Держспецзв'язку



Валерій НОВАК