МІНІСТЕРСТВО РОЗВИТКУ ГРОМАД ТА ТЕРИТОРІЙ УКРАЇНИ
пр-т Берестейський, 14, м. Київ, 01135,
тел.: (044) 351-40-96, (044) 351-40-35, (044) 351-40-01,
E-mail: miu@mtu.gov.ua, сайт: www.mtu.gov.ua, код згідно з ЄДРПОУ 37472062

від _____ 20__ р. № _____ На № _____ від _____ 20__ р.

Державна регуляторна служба
України

Про погодження проєкту наказу

Міністерство розвитку громад та територій України з метою приведення нормативно-правових актів у сфері діяльності, пов'язаної з об'єктами критичної інфраструктури, у відповідність до вимог законодавства розробило проєкт наказу Міністерства розвитку громад та територій України «Про затвердження вимог до захисту об'єктів критичної інфраструктури у секторах транспорту і пошти та системи життєзабезпечення» та просить погодити його у п'ятиденний термін.

Додатки: 1. Проєкт наказу на 8 арк. в 1 прим.
2. Пояснювальна записка на 3 арк. в 1 прим.
3. Аналіз регуляторного впливу на 13 в 1 прим.
4. Повідомлення про оприлюднення на 1 арк. в 1 прим.

Віце-прем'єр-міністр з відновлення
України – Міністр Олексій КУЛЕБА

Юрій Михайлов 351 41 19

Проект

МІНІСТЕРСТВО РОЗВИТКУ ГРОМАД ТА ТЕРИТОРІЙ УКРАЇНИ

НАКАЗ

_____ Київ № _____

Про затвердження вимог до захисту об’єктів критичної інфраструктури у секторах транспорту і пошти та системи життєзабезпечення

Відповідно до пункту 4 частини першої статті 19 Закону України «Про критичну інфраструктуру», пункту 8 Положення про Міністерство розвитку громад та територій України, затвердженого постановою Кабінету Міністрів України від 30 червня 2015 року № 460 (в редакції постанови Кабінету Міністрів України від 17 грудня 2022 року № 1400), з урахуванням абзацу третього підпункту 5 пункту 1 рішення Ради національної безпеки і оборони України від 17 жовтня 2023 року «Про організацію захисту та забезпечення безпеки функціонування об’єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій», уведеного в дію Указом Президента України від 17 жовтня 2023 року № 695/2023,

НАКАЗУЮ:

1. Затвердити вимоги до захисту об’єктів критичної інфраструктури у секторах транспорту і пошти та системи життєзабезпечення, що додаються.

2. Департаменту впровадження пріоритетних проектів регіонального розвитку та критичної інфраструктури забезпечити в установленому порядку подання цього наказу на державну реєстрацію до Міністерства юстиції України.

3. Сектору зовнішніх комунікацій забезпечити оприлюднення цього наказу на офіційному веб-сайті Міністерства розвитку громад та територій України.

4. Контроль за виконанням цього наказу на заступника Міністра відповідно до розподілу обов’язків.

Віце-прем’єр-міністр з відновлення України – Міністр Олексій КУЛЕБА

ЗАТВЕРДЖЕНО

Наказ Міністерства розвитку громад та територій України

___ _____ 2025 року №___

Вимоги
до захисту об’єктів критичної інфраструктури у секторах транспорту і пошти та системи життєзабезпечення

Загальні положення

1. Ці Вимоги встановлюють порядок створення, налагодження та підтримання безперервного функціонування систем фізичної безпеки об’єктів критичної інфраструктури у секторах транспорту і пошти та системи життєзабезпечення операторами об’єктів критичної інфраструктури, які забезпечують реалізацію заходів щодо захисту об’єктів критичної інфраструктури.

2. У цих Вимогах терміни вживаються у таких значеннях:

система фізичної безпеки об’єктів критичної інфраструктури – сукупність організаційно-правових та інженерно-технічних заходів, що здійснюються операторами об’єктів критичної інфраструктури з метою створення умов, спрямованих на мінімізацію можливості вчинення диверсії, терористичних актів, крадіжки або будь-яких інших протиправних дій, зміцнення режиму охорони та захищеності об’єктів критичної інфраструктури;

фізичний захист – діяльність операторів об’єктів критичної інфраструктури щодо захисту об’єктів критичної інфраструктури, спрямована на оперативне реагування на протиправні дії та фізичні атаки, запобігання неправомірного втручання в роботу операційних систем чи систем фізичної безпеки об’єкта критичної інфраструктури, забезпечення організації охорони та захищеності об’єктів критичної інфраструктури;

підрозділ реагування на об’єкті критичної інфраструктури – підрозділ, який цілодобово забезпечує оперативне реагування на повідомлення про протиправні дії або події, у межах компетенції здійснює комплекс превентивних заходів шляхом патрулювання території об’єкта (зони обслуговування), виявлення та припинення протиправних дій, застосування визначених законодавством інших заходів реагування;

підрозділ фізичного захисту (охорони) об’єкта критичної інфраструктури – підрозділ призначений для здійснення діяльності з підтримання безперервного

функціонування систем фізичної безпеки об’єктів критичної інфраструктури, забезпечення охорони та захищеності об’єктів критичної інфраструктури;

персонал підрозділу фізичного захисту (охорони) – особи, посадові обов’язки яких пов’язані зі здійсненням заходів із забезпечення фізичного захисту на конкретних об’єктах критичної інфраструктури.

Інші терміни у цих Вимогах вживаються у значеннях, наведених в Законі України «Про критичну інфраструктуру».

3. Оператори об’єктів критичної інфраструктури забезпечують:

заходи безпеки та стійкості критичної інфраструктури, зокрема створення, налагодження та підтримання безперервного функціонування систем фізичної безпеки, безпеки операційних систем та кібербезпеки;

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

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

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

створення структурного підрозділу або визначення відповідальної особи за організацію захисту критичної інфраструктури та забезпечення постійного зв’язку з відповідними суб’єктами національної системи захисту критичної інфраструктури (далі – відповідальна особа);

негайне інформування уповноваженого органу у сфері захисту критичної інфраструктури України та відповідних функціональних органів у сфері захисту критичної інфраструктури про інциденти, пов’язані з порушеннями систем фізичної безпеки та кібербезпеки;

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

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

4. Оператори об’єктів критичної інфраструктури забезпечують належний рівень захищеності, розробляють і здійснюють заходи із захисту критичної інфраструктури на етапах будівництва та експлуатації об’єктів критичної інфраструктури.

Організація та завдання системи фізичної безпеки об’єктів критичної інфраструктури

5. Керівники операторів об’єктів критичної інфраструктури створюють та забезпечують функціонування системи фізичної безпеки.

6. На об’єктах критичної інфраструктури визначаються відповідальні особи за забезпечення та підтримання безперервного функціонування систем фізичної безпеки.

7. Система фізичної безпеки об’єктів критичної інфраструктури створюється, виходячи з принципів:

глибокоешелонованого захисту (сукупність послідовних фізичних бар’єрів на шляху сторонніх осіб у зони обмеженого доступу об’єктів критичної інфраструктури в сукупності з технічними засобами і організаційними заходами, що спрямовані на недопущення відхилення від нормальних умов експлуатації об’єктів критичної інфраструктури, запобігання кризовим ситуаціям і обмеження їх наслідків);

диференційованого підходу, згідно з яким забезпечується відповідність рівня фізичного захисту об’єктів критичної інфраструктури та потенційним наслідкам вчинення протиправних дій щодо системи фізичної безпеки об’єктів критичної інфраструктури;

збалансованого захисту;

мінімізації наслідків при відмові одного елемента системи.

системності (функціонування системи фізичної безпеки об’єктів критичної інфраструктури має системний, упорядкований та постійний характер);

запобігання вчиненню протиправних дій, згідно з яким забезпечується виявлення потенційних загроз щодо об’єктів критичної інфраструктури та вжиття заходів для успішної протидії таким загрозам;

адаптивності, згідно з яким забезпечується виконання завдань системи фізичної безпеки об’єктів критичної інфраструктури у разі зміни проектної загрози;

адекватності (умови функціонування системи фізичної безпеки об’єктів критичної інфраструктури відповідають рівню наявних загроз щодо об’єктів критичної інфраструктури);

інформованості (оператори критичної інфраструктури своєчасно забезпечуються інформацією про наявні та потенційні загрози щодо об’єктів критичної інфраструктури в обсягах, що дають змогу операторам критичної інфраструктури вживати відповідних заходів для успішної протидії таким загрозам);

виявлення та усунення причин протиправних дій, згідно з яким забезпечується здійснення постійного контролю за відповідністю системи

фізичної безпеки об’єктів критичної інфраструктури вимогам законодавства та вжиття заходів з усунення виявлених невідповідностей.

8. Завданнями системи фізичної безпеки об’єктів критичної інфраструктури є:

виявлення вторгнення сторонніх осіб у зони обмеженого доступу об’єктів критичної інфраструктури;

запобігання просуванню та здійсненню сторонніми особами протиправних дій щодо об’єктів критичної інфраструктури;

реагування на протиправні дії сторонніх осіб на об’єктах критичної інфраструктури;

пом’якшення наслідків незаконних дій сторонніх осіб щодо об’єктів критичної інфраструктури.

9. Виявлення вторгнення сторонніх осіб у зони обмеженого доступу об’єктів критичної інфраструктури забезпечується:

обладнанням зон обмеженого доступу та контрольно-пропускних пунктів інженерно-технічними засобами системи фізичної безпеки;

установленням на пультах системи фізичної безпеки засобів відображення та оцінки сигналу тривоги, запису інформації, зв’язку з постами варти підрозділу фізичного захисту (охорони) об’єкта критичної інфраструктури (патрулями), персоналом підрозділу фізичного захисту (охорони) об’єктів критичної інфраструктури;

перевіркою осіб, їх особистих речей, транспортних засобів, вантажів на наявність речовин і предметів, вільне пересування з якими в межах зон обмеженого доступу забороняється;

патрулюванням території об’єктів критичної інфраструктури;

установлення маршрутів проходу осіб у зонах обмеженого доступу.

10. Запобігання просуванню та здійсненню сторонніми особами незаконних дій щодо об’єктів критичної інфраструктури забезпечується:

створенням зон обмеження доступу;

організацією доступу в зони обмеження доступу;

організацією пропускного та внутрішньооб’єктового режиму;

організацією охорони та оборони;

дотриманням процедур системи фізичної безпеки.

11. Затримка просування сторонніх осіб зонами обмеженого доступу на об’єктах критичної інфраструктури забезпечується:

установленням фізичних бар’єрів на ймовірних маршрутах просування сторонніх осіб;

виконанням підрозділом фізичного захисту (охорони) об’єкта критичної інфраструктури затримки просування сторонніх осіб.

12. Реагування на дії сторонніх осіб на об’єктах критичної інфраструктури забезпечується:

обладнанням пультів системи фізичної безпеки засобами оповіщення про тривогу та технічними засобами електронних комунікацій;

діями операторів пульта системи фізичної безпеки відповідно до встановлених процедур;

підготовкою та оснащенням сил реагування;

своєчасними та ефективними діями сил реагування.

13. Пом’якшення наслідків протиправних дій на об’єктах критичної інфраструктури забезпечується:

наявністю резервного пульта системи фізичної безпеки;

здатністю системи фізичної безпеки функціонувати в умовах кризових ситуацій;

включенням заходів із фізичного захисту, протидії загрозам, ефективного зниження та контролю за ризиками безпеки в об’єктових планах заходів;

наявністю висококваліфікованого, підготовленого до дій в умовах кризових ситуацій персоналу підрозділу фізичного захисту (охорони) об’єктів критичної інфраструктури, особового складу підрозділу реагування.

14. Оператори об’єктів критичної інфраструктури здійснюють заходи зі створення та безперервного функціонування систем фізичної безпеки відповідно до об’єктових планів заходів.

Рівень систем фізичної безпеки визначається операторами об’єктів критичної інфраструктури відповідно до категорії критичності об’єктів критичної інфраструктури.

На об’єктах критичної інфраструктури оператори можуть передбачати фізичну охорону або комплексну систему безпеки із застосуванням інженерних та технічних засобів охорони.

15. При розробленні об’єктових планів заходів враховуються заходи із захисту критичної інфраструктури з метою підтримання безперервного функціонування систем фізичної безпеки в умовах кризових ситуацій.

16. Заходи із захисту критичної інфраструктури не повинні погіршувати стан безпеки (радіаційна, кібер, пожежна, екологічна, техногенна, транспортна, виробнича, трудова, та інші) на об’єктах критичної інфраструктури.

Створення систем фізичної безпеки

17. Створення систем фізичної безпеки здійснюється керівниками операторів об’єктів критичної інфраструктури під час будівництва об’єктів

критичної інфраструктури, а також технічного переоснащення систем фізичної безпеки діючих об’єктів критичної інфраструктури.

18. Створення систем фізичної безпеки полягає в:

установленні вихідних даних для проектування системи на основі проектної загрози (визначення завдань системи та її конфігурації);

переліку процедур з фізичної безпеки;

критеріїв ефективності системи, характеристик об’єктів критичної інфраструктури;

здійсненні комплексу організаційно-правових та інженерно-технічних заходів на об’єктах критичної інфраструктури.

функцій підрозділу фізичного захисту (охорони) об’єктів критичної інфраструктури, особового складу підрозділу реагування.

Підтримання безперервного функціонування систем фізичної безпеки

19. Оператори об’єктів критичної інфраструктури підтримують безперервне функціонування систем фізичної безпеки шляхом здійснення комплексу організаційно-правових та інженерно-технічних заходів.

20. Оператори об’єктів критичної інфраструктури забезпечують виконання процедур з фізичної безпеки шляхом:

навчання персоналу об’єкта критичної інфраструктури щодо дотримання вимог захисту критичної інфраструктури;

перевірки дієздатності процедур з фізичної безпеки та внесення (у разі необхідності) відповідних змін до них;

належного виконання обов’язків персоналом підрозділу фізичного захисту (охорони) та особовим складом підрозділу реагування.

21. Підтримання безперервного функціонування систем фізичної безпеки здійснюється за допомогою застосування інженерно-технічних заходів на об’єктах критичної інфраструктури, які включають:

випробування інженерно-технічних засобів;

технічне обслуговування та ремонт інженерно-технічних засобів;

матеріально-технічне забезпечення експлуатації інженерно-технічних засобів;

забезпечення працездатності та надійності;

розроблення програми (плану) реконструкції та технічного переоснащення інженерно-технічних засобів.

22. Безперервне функціонування інженерно-технічних засобів систем фізичної безпеки об’єктів критичної інфраструктури забезпечується їх належним технічним обслуговуванням, що включає:

огляд стану інженерно-технічних засобів;

проведення регламентних і ремонтних робіт;

періодичні функціональні випробування інженерно-технічних засобів;

усунення наслідків природного та техногенного впливу;

підтримання в робочому стані визначених у проектній документації резервних інженерно-технічних засобів та їх комплектуючих;

перевірку наявності необхідних інструментів;

контроль стану вимірювальних приладів і процедур їх калібрування.

23. Оператори пультів систем фізичної безпеки об’єктів критичної інфраструктури здійснюють оперативне управління інженерно-технічними засобами систем фізичної безпеки, оцінку сигналів тривоги та оповіщень про тривогу.

Перевірка систем фізичної безпеки об’єктів критичної інфраструктури

24. Перевірка стану безперервного функціонування систем фізичної безпеки об’єктів критичної інфраструктури здійснюється раз на півріччя відповідальною особою оператора критичної інфраструктури або із залученням фахівців спеціалізованих організацій.

25. Відповідальні особи операторів об’єктів критичної інфраструктури за результатами перевірки системи фізичної безпеки розробляють та здійснюють коригувальні заходи з усунення виявлених недоліків та надають керівнику оператора критичної інфраструктури пропозиції щодо здійснення реконструкції або технічного переоснащення системи фізичної безпеки.

Директор Департаменту впровадження
пріоритетних проектів регіонального
розвитку та критичної інфраструктури Леся ДІДЕНКО

ПОЯСНЮВАЛЬНА ЗАПИСКА
до проекту наказу Міністерства розвитку громад та територій України «Про затвердження вимог до захисту об'єктів критичної інфраструктури у секторах транспорту і пошти та системи життєзабезпечення»

1. Мета

Проект наказу Міністерства розвитку громад та територій України «Про затвердження вимог до захисту об'єктів критичної інфраструктури у секторах транспорту і пошти та системи життєзабезпечення» (далі – проект акта) з метою реалізації пункту 4 частини першої статті 19 Закону України «Про критичну інфраструктуру» та виконання абзацу третього підпункту 5 пункту 1 рішення Ради національної безпеки і оборони України від 17 жовтня 2023 року «Про організацію захисту та забезпечення безпеки функціонування об'єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій», уведеного в дію Указом Президента України від 17 жовтня 2023 року № 695/2023 (далі – Рішення).

2. Обґрунтування необхідності прийняття акта

Відповідно до статті 5 Закону України «Про критичну інфраструктуру» (далі – Закон) метою державної політики у сфері захисту критичної інфраструктури є забезпечення безпеки об'єктів критичної інфраструктури, запобігання проявам несанкціонованого втручання в їх функціонування, прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури. До завдань формування і реалізації державної політики у сфері захисту критичної інфраструктури належать, зокрема встановлення обов'язкових вимог із забезпечення безпеки об'єктів критичної інфраструктури, їх захищеності на всіх етапах життєвого циклу, у тому числі під час створення, прийняття в експлуатацію, модернізації.

Відповідно до пункту 4 частини першої статті 19 Закону державні органи, визначені відповідальними за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури розробляють та затверджують вимоги до захисту об'єктів критичної інфраструктури відповідно до їх категорій.

Частиною першою статті 21 Закону встановлено, що до основних завдань операторів критичної інфраструктури належать, зокрема:

створення, налагодження та підтримання функціонування ефективної системи фізичної безпеки, безпеки операційних систем та кібербезпеки;

оперативне реагування на протиправні дії, фізичні атаки, спрямовані на відключення або пошкодження роботи операційних систем чи систем забезпечення фізичної безпеки об'єкта критичної інфраструктури.

Абзацом третім підпункту 5 пункту 1 Рішення Кабінету Міністрів України доручено забезпечити затвердження нормативно-правового акта щодо вимог до систем фізичного захисту об'єктів критичної інфраструктури.

Відповідно до підпункту 2 пункту 3 Положення про Міністерство розвитку громад та територій України, затвердженого постановою Кабінету Міністрів України від 30 червня 2015 року № 460 (в редакції постанови Кабінету Міністрів України від 17 грудня 2022 року № 1400), одним із основних завдань Мінрозвитку є забезпечення формування та реалізації державної політики з питань захисту критичної інфраструктури у секторах, за які відповідальне Міністерство.

Таким чином виникла необхідність розроблення проекту акта.

3. Основні положення проекту акта

Проектом акта передбачається затвердити вимоги до захисту об'єктів критичної інфраструктури у секторах транспорту і пошти та системи життєзабезпечення, в яких, зокрема, передбачити положення щодо організації та завдань системи фізичної безпеки об'єктів критичної інфраструктури, створення систем фізичної безпеки, підтримання безперервного функціонування систем фізичної безпеки, перевірки систем фізичної безпеки об'єктів критичної інфраструктури.

4. Правові аспекти

Проект акта розроблено відповідно до Закону України «Про критичну інфраструктуру», рішення Ради національної безпеки і оборони України від 17 жовтня 2023 р. «Про організацію захисту та забезпечення безпеки функціонування об'єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій», уведеного в дію Указом Президента України від 17 жовтня 2023 р. № 695/2023.

5. Фінансово-економічне обґрунтування

Реалізація акта не потребуватиме додаткових видатків із державного та місцевих бюджетів.

6. Позиція заінтересованих сторін

Проект акта не стосується питань функціонування місцевого самоврядування, прав та інтересів територіальних громад, місцевого та регіонального розвитку, соціально-трудової сфери, прав осіб з інвалідністю, функціонування і застосування української мови як державної, а тому не потребує отримання позиції уповноважених представників всеукраїнських асоціацій органів місцевого самоврядування чи відповідних органів місцевого самоврядування, уповноважених представників всеукраїнських профспілок, їх об'єднань та всеукраїнських об'єднань організацій роботодавців, Урядового уповноваженого з прав осіб з інвалідністю та всеукраїнських громадських організацій осіб з інвалідністю, їх спілок, Уповноваженого із захисту державної мови.

Проект акта не стосується сфери наукової та науково-технічної діяльності та на розгляд Наукового комітету Національної ради з питань розвитку науки і технологій не надсилався.

7. Оцінка відповідності

У проекті акта відсутні положення, що:

стосуються зобов’язань України у сфері європейської інтеграції;

стосуються прав та свобод, гарантованих Конвенцією про захист прав людини і основоположних свобод;

впливають на забезпечення рівних прав та можливостей жінок і чоловіків;

містять ризики вчинення корупційних правопорушень та правопорушень, пов’язаних з корупцією;

створюють підстави для дискримінації.

8. Прогноз результатів

Реалізація акта не впливатиме на ринкове середовище, забезпечення захисту прав та інтересів суб’єктів господарювання, громадян і держави; розвиток регіонів, підвищення чи зниження спроможності територіальних громад; ринок праці, рівень зайнятості населення; громадське здоров’я, покращення чи погіршення стану здоров’я населення або його окремих груп; екологію та навколишнє природне середовище.

Віце-прем’єр-міністр з відновлення
України – Міністр розвитку громад та
територій України Олексій КУЛЕБА

___ _____ 2025 р.

Аналіз регуляторного впливу
до проєкту наказу Міністерства розвитку громад та територій України «Про затвердження вимог до захисту об'єктів критичної інфраструктури у секторах транспорту і пошти та системи життєзабезпечення»

І. Визначення проблеми

Відповідно до статті 5 Закону України «Про критичну інфраструктуру» (далі – Закон) метою державної політики у сфері захисту критичної інфраструктури є забезпечення безпеки об'єктів критичної інфраструктури, запобігання проявам несанкціонованого втручання в їх функціонування, прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури. До завдань формування і реалізації державної політики у сфері захисту критичної інфраструктури належать, зокрема, встановлення обов'язкових вимог із забезпечення безпеки об'єктів критичної інфраструктури, їх захищеності на всіх етапах життєвого циклу, у тому числі під час створення, прийняття в експлуатацію, модернізації.

Частиною першою статті 1 Закону визначено відповідні терміни, що в ньому вживаються, зокрема:

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

ідентифікація об'єкта критичної інфраструктури – процедура віднесення об'єкта інфраструктури до об'єктів критичної інфраструктури (пункт 4);

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

категоризація об'єктів інфраструктури – віднесення об'єктів інфраструктури до категорій критичності об'єктів інфраструктури (пункт 6);

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

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

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

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

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

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

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

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

Відповідно до пункту 4 частини першої статті 19 Закону державні органи, визначені відповідальними за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури, розробляють та затверджують вимоги до захисту об’єктів критичної інфраструктури відповідно до їх категорій.

Частиною першою статті 21 Закону встановлено, що до основних завдань операторів критичної інфраструктури належать, зокрема:

створення, налагодження та підтримання функціонування ефективної системи фізичної безпеки, безпеки операційних систем та кібербезпеки;

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

Абзацом третім підпункту 5 пункту 1 рішення Ради національної безпеки і оборони України від 17 жовтня 2023 року «Про організацію захисту та забезпечення безпеки функціонування об'єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій», уведеного в дію Указом Президента України від 17 жовтня 2023 року № 695/2023, Кабінету Міністрів України доручено забезпечити затвердження нормативно-правового акта щодо вимог до систем фізичного захисту об'єктів критичної інфраструктури.

Відповідно до підпункту 2 пункту 3 Положення про Міністерство розвитку громад та територій України, затвердженого постановою Кабінету Міністрів України від 30 червня 2015 року № 460 (в редакції постанови Кабінету Міністрів України від 17 грудня 2022 року № 1400), одним із основних завдань Мінрозвитку є забезпечення формування та реалізації державної політики з питань захисту критичної інфраструктури у секторах, за які відповідальне Міністерство.

Виходячи із зазначеного, метою прийняття зазначеного проєкту наказу Мінрозвитку є реалізація пункту 4 частини першої статті 19 Закону України «Про критичну інфраструктуру» та виконання абзацу третього підпункту 5 пункту 1 рішення Ради національної безпеки і оборони України від 17 жовтня 2023 року «Про організацію захисту та забезпечення безпеки функціонування об'єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій», уведеного в дію Указом Президента України від 17 жовтня 2023 року № 695/2023.

Станом на 01.01.2025 кількість об'єктів критичної інфраструктури, що підпадають під дію регулювання наказом – 5031, з яких належать до I та II категорії критичності (великі) – 84, III категорії критичності (середні) – 1896, IV категорії критичності (малі) – 3051 та мікро – 0.

Проєкт наказу повністю враховує вимоги Закону України «Про критичну інфраструктуру».

Визначення основних груп (підгруп), на які проблема справляє вплив:

Групи (підгрупи)	Так	Ні
Громадяни	-	+
Держава	+	-
Оператори критичної інфраструктури	+	-
у тому числі суб'єкти малого підприємництва*	+	

Врегулювання зазначених проблемних питань не може бути здійснено за допомогою чинного законодавства, оскільки нормативно-правовими актами порушені питання не врегульовані.

II. Цілі державного регулювання

Цілю прийняття проєкту наказу Міністерства розвитку громад та територій України «Про затвердження вимог до захисту об'єктів критичної інфраструктури у секторах транспорту і пошти та системи життєзабезпечення» (далі – проєкт

акта) є забезпечення безпеки об’єктів критичної інфраструктури, запобігання проявам несанкціонованого втручання в їх функціонування, прогнозування та запобігання кризовим ситуаціям на об’єктах критичної інфраструктури, зокрема встановлення обов’язкових вимог із забезпечення безпеки об’єктів критичної інфраструктури, їх захищеності на всіх етапах життєвого циклу, у тому числі під час створення, прийняття в експлуатацію, модернізації.

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

Альтернативні способи розроблено за результатами обговорення на робочих зустрічах представників бізнесу та звернень суб’єктів господарювання:

Альтернатива 1 прийняття проєкту акта

Альтернатива 2 залишення існуючої ситуації без змін

Вид альтернатив	Опис альтернативи
Альтернатива 1	Запропонований спосіб вирішення зазначеної проблеми є найбільш доцільним і дасть змогу встановити обов’язкові вимоги із забезпечення безпеки об’єктів критичної інфраструктури, їх захищеності на всіх етапах життєвого циклу, у тому числі під час створення, прийняття в експлуатацію, модернізації, що, у свою чергу забезпечить безпеку об’єктів критичної інфраструктури, їх прогнозування, запобігання кризовим ситуаціям та проявам несанкціонованого втручання в їх функціонування.
Альтернатива 2	Відсутність обов’язкових вимог із забезпеченням безпеки об’єктів критичної інфраструктури, їх захищеності на всіх етапах життєвого циклу, у тому числі під час створення, прийняття в експлуатацію, модернізації може призвести до кризових ситуацій та проявам несанкціонованого втручання в їх функціонування.

Таким чином, Альтернатива 1 є прийнятним і єдиним способом досягнення зазначених цілей.

2. Оцінка вибраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернатив	Вигоди	Витрати
Альтернатива 1	Запропонований спосіб вирішення зазначеної проблеми є найбільш доцільним і дасть змогу операторам критичної інфраструктури забезпечити безпеку об’єктів критичної інфраструктури, їх	відсутні

	прогнозування, запобігання кризовим ситуаціям та проявам несанкціонованого втручання в їх функціонування.	
Альтернатива 2	відсутні	Через відсутність обов'язкових вимог із забезпечення безпеки об'єкти критичної інфраструктури залишаються незахищеними на всіх етапах життєвого циклу, у тому числі під час створення, прийняття в експлуатацію, модернізації, що може призвести до кризових ситуацій та проявам несанкціонованого втручання в їх функціонування.

Оцінка впливу на сферу інтересів громадян

Оцінка впливу на сферу інтересів громадян

Вид альтернативи	Вигоди	Витрати
Альтернатива 1 Прийняття проєкту акта	Високі Дає змогу операторам критичної інфраструктури забезпечити безпеку об'єктів критичної інфраструктури, їх прогнозування, запобігання кризовим ситуаціям та проявам несанкціонованого втручання в їх функціонування	Відсутні
Альтернатива 2 Збереження ситуації, яка існує на цей час	Відсутні Альтернатива є неприйнятною, оскільки не відповідає вимогам чинного законодавства	Відсутні

Оцінка впливу на сферу інтересів суб'єктів господарювання.

За звітними та статистичними даними під дію проєкту акта підпадають:

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість об'єктів критичної інфраструктури, що	84	1896	3051	0	5031

підпадають під дію регулювання, одиниць					
Питома вага групи у загальній кількості, відсотків	1.7 %	37.7 %	60.6 %	0 %	100 %

Вид альтернатив	Вигоди	Витрати
Альтернатива 1	Запропонований спосіб вирішення зазначеної проблеми є найбільш доцільним і дасть змогу операторам критичної інфраструктури забезпечити безпеку об’єктів критичної інфраструктури, їх прогнозування, запобігання кризовим ситуаціям та проявам несанкціонованого втручання в їх функціонування	Відсутні
Альтернатива 2	Такий спосіб є неприйнятним, оскільки він не забезпечує безпеку об’єктів критичної інфраструктури, їх прогнозування, запобігання кризовим ситуаціям та проявам несанкціонованого втручання в їх функціонування.	Відсутні

Витрати на одного оператора критичної інфраструктури, які виникають внаслідок дії регуляторного акта.

Розрахунок зроблено на підставі того, що витрати на розробку політики запобігання кризовим ситуаціям є однаковим для всіх суб’єктів господарювання як для великого, середнього та малого бізнесу та відповідно до Закону України «Про критичну інфраструктуру» умовно взято одного оператора, який забезпечує безпеку об’єктів критичної інфраструктури, їх прогнозування, запобігання кризовим ситуаціям та проявам несанкціонованого втручання в їх функціонування з періодичністю один раз на п’ять років, тому М-тест не проводився відповідно до додатка 4.

Порядковий номер	Витрати	Чинний акт/ витрати через 5 років	Проєкт акта/ витрати через 5 років
1	Витрати на придбання основних фондів, обладнання та приладів, сервісне обслуговування, навчання/підвищення кваліфікації персоналу тощо, гривень	300*/0 /0	100*/0/0

2	Витрати, пов’язані на пошук та опрацювання регуляторних актів, які містять застарілі та не актуальні обов’язкові вимоги безпеки для об’єктів критичної інфраструктури, гривень Пошук займає 3 год. [2]	144 грн	0/0
3.	Витрати, пов’язані на пошук механізмів та процедур для виконання завідомо не актуальних та застарілих регулювань, гривень Направлення займає 1 година[1]	48 грн	0 грн
4	РАЗОМ (сума рядків: 1 + 2 + 3), гривень	492 грн	100 грн
5	Кількість об'єктів критичної інфраструктури, на яких буде поширено регулювання, одиниць	5031	5031
6	Сумарні витрати операторів критичної інфраструктури на виконання регулювання (вартість регулювання) (рядок 4 х рядок 5), гривень	2 475 252 грн	503 100 грн.**

[1]Для обрахунку: приймаємо за основу мінімальну заробітну плату, визначену у погодинному розмірі, що становить 48 грн/год відповідно до Закону України «Про Державний бюджет України на 2025 рік»; час, який витрачається суб’єктами господарювання на пошук альтернативи 1 год. (за результатами консультацій).

[2] Для обрахунку: приймаємо за основу мінімальну заробітну плату, визначену у погодинному розмірі, що становить 48 грн/год відповідно до Закону України «Про Державний бюджет України на 2025 рік»; час, який витрачається суб’єктами господарювання на направлення паперовій формі 3 год. (за результатами консультацій).

* Дані, отримані за результатами консультацій з суб’єктами господарювання (в середньому 300 грн.)

** Із розрахунку видно, що в разі виконання вимог регулювання шляхом визначення заходів безпеки економія коштів становить 1 945 152 грн. Економія коштів через п’ять років становить 503 100 грн.

Проведення оцінки впливу кількісних витрат на сферу інтересів суб’єктів господарювання, які виникатимуть унаслідок дії регуляторного акта

Сумарні витрати за альтернативами	Сума витрат, гривень
Альтернатива 1. Сумарні витрати для операторів критичної інфраструктури згідно з додатком 2 Методики проведення аналізу впливу регуляторного акта «Витрати на одного суб’єкта господарювання великого і середнього підприємництва, які виникають унаслідок дії регуляторного акта»)	503 100 грн

Альтернатива 2. Сумарні витрати для операторів критичної інфраструктури згідно з додатком 2 Методики проведення аналізу впливу регуляторного акта «Витрати на одного суб'єкта господарювання великого і середнього підприємництва, які виникають унаслідок дії регуляторного акта»)	2 475 252 грн.

Отже, запровадження обов'язкових вимог із забезпечення безпеки об'єктів критичної інфраструктури, їх захищеності на всіх етапах життєвого циклу, у тому числі під час створення, прийняття в експлуатацію, модернізації, забезпечить безпеку об'єктів критичної інфраструктури, їх прогнозування, запобігання кризовим ситуаціям та проявам несанкціонованого втручання в їх функціонування, дозволить не тільки економити час оператору критичної інфраструктури, а також дозволить економити витрати на його ведення господарської діяльності, що становитиме майже 20.4 % за п'ять років.

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

Здійснити вибір оптимального альтернативного способу з урахуванням системи бальної оцінки ступеня досягнення визначених цілей.

Вартість балів визначається за чотирибальною системою оцінки ступеня досягнення визначених цілей, де:

4 – цілі прийняття регуляторного акта, які можуть бути досягнуті повною мірою (проблема більше не існуватиме);

3 – цілі прийняття регуляторного акта, які можуть бути досягнуті майже повною мірою (усі важливі аспекти проблеми не існуватимуть);

2 – цілі прийняття регуляторного акта, які можуть бути досягнуті частково (проблема значно зменшиться, деякі важливі та критичні аспекти проблеми залишаться нерозв'язаними);

1 – цілі прийняття регуляторного акта, які не можуть бути досягнуті (проблема продовжує існувати).

Рейтинг результативності (досягнення цілей під час розв'язання проблеми)	Бал результативності (за чотирибальною системою оцінки)	Коментарі щодо присвоєння відповідного бала
Альтернатива 1:	4	Проблема більше не існуватиме (зазначений спосіб повністю відповідає вимогам законодавства та сучасності, є найбільш доцільним і ефективним)
Альтернатива 2:	1	Проблема продовжує існувати

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
Альтернатива 1:	Запропонований спосіб вирішення зазначеної проблеми є найбільш доцільним і дасть змогу операторам критичної інфраструктури забезпечити безпеку об’єктів критичної інфраструктури, їх захищеність на всіх етапах життєвого циклу, у тому числі під час створення, прийняття в експлуатацію, модернізації, що, у свою чергу забезпечить запобігання кризовим ситуаціям та проявам несанкціонованого втручання в їх функціонування, а також економити витрати	відсутні	Прийняття регуляторного акта дозволить досягнути задекларованих цілей, забезпечення безпеки об’єктів критичної інфраструктури
Альтернатива 2:	відсутні	В оператора критичної інфраструктури збільшуються ризики виникнення кризових ситуацій на об’єктах критичної інфраструктури та проявам несанкціонованого втручання в їх функціонування, а також витрати на придбання основних фондів, обладнання та приладів, сервісне	У разі саморегуляції витрати продовжуватимуть існувати, що не забезпечить досягнення поставленої мети

		обслуговування та час на його направлення	

Рейтинг	Аргументи щодо переваги обраної альтернативи/причини відмови від альтернативи	Оцінка ризику зовнішніх чинників на дію запропонованого регуляторного акта
Альтернатива 1:	Реалізація регуляторного акта забезпечить досягнення поставлених цілей: забезпечить безпеку об’єктів критичної інфраструктури, їх захищеність на всіх етапах життєвого циклу, у тому числі під час створення, прийняття в експлуатацію, модернізації, що, у свою чергу, забезпечить запобігання кризовим ситуаціям та проявам несанкціонованого втручання в їх функціонування	Вплив зовнішніх факторів на дію регуляторного акта не очікується
Альтернатива 2:	Неприйнятна, тому що відсутність регулювання негативно вплине безпеку об’єктів критичної інфраструктури	Витрата часу, пов’язані на пошук та опрацювання регуляторних актів, які містять застарілі та не актуальні обов’язкові вимоги безпеки для об’єктів критичної інфраструктури та на пошук механізмів та процедур для виконання завідомо не актуальних та застарілих регулювань

V. Механізми та заходи, які забезпечать розв’язання визначеної проблеми

Основним завданням проєкту наказу є виконання вимог законодавства України у сфері захисту критичної інфраструктури.

Головною мотивацією є приведення нормативно-правової бази у відповідність до норм чинного законодавства, спрямованих на забезпечення безпеки об’єктів критичної інфраструктури, їх захищеності на всіх етапах життєвого циклу, у тому числі під час створення, прийняття в експлуатацію, модернізації, що, у свою чергу, забезпечить запобігання кризовим ситуаціям та проявам несанкціонованого втручання в їх функціонування.

Для впровадження цього регуляторного акта необхідно здійснити такі організаційні заходи:

інформувати операторів критичної інфраструктури про вимоги проєкту регуляторного акта шляхом оприлюднення його на офіційному вебсайті Міністерства розвитку громад та територій України;

погодити проєкт регуляторного акта із заінтересованими органами.

Прийняття регуляторного акта не призведе до неочікуваних результатів і не потребує додаткових витрат з державного бюджету.

Ризику впливу зовнішніх факторів на дію регуляторного акта немає.

Досягнення цілей не передбачає додаткових організаційних заходів.

Можлива шкода у разі очікуваних наслідків дії акта не прогнозується.

З боку суб'єктів господарювання відсутня необхідність вчинення додаткових дій.

VI. Оцінка виконання вимог регуляторного акта залежно від ресурсів, якими розпоряджаються органи виконавчої влади чи органи місцевого самоврядування, фізичні та юридичні особи, які повинні проваджувати або виконувати ці вимоги

Для впровадження та виконання регуляторного акта органи виконавчої влади не будуть нести додаткових витрат.

Виконання вимог регуляторного акта залежно від ресурсів, якими розпоряджаються органи виконавчої влади чи органи місцевого самоврядування, фізичні та юридичні особи, які повинні впроваджувати або виконувати ці вимоги, оцінюється вище середнього.

М-Тест не проводився у зв'язку з тим, що дія проєкту наказу однаково впливає на всіх операторів критичної інфраструктури незалежно від форми власності та рівня їх специфіки.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Строк дії регуляторного акта пропонується не обмежувати в часі. Зміна строку дії регуляторного акта можлива лише у випадку зміни законодавчих актів, які регулюють вказане питання.

Цей регуляторний акт набирає чинності з дня його офіційного опублікування.

VIII. Визначення показників результативності дії регуляторного акта

Основними показниками результативності регуляторного акта є:

1. Кількість операторів критичної інфраструктури, на яких поширюється дія акта.

2. Розмір коштів і час, що витрачатимуться операторами критичної інфраструктури, пов'язаними з виконанням вимог акта.

3. Рівень поінформованості суб'єктів господарювання стосовно основних положень регуляторного акта − високий, оскільки проєкт наказу розміщено на офіційному вебсайті Мінрозвитку.

4. Кількість кризових ситуацій на об’єктах критичної інфраструктури та проявів несанкціонованого втручання в їх функціонування.

5. Кількість розроблених заходів безпеки об’єктів критичної інфраструктури на всіх етапах життєвого циклу, у тому числі під час створення, прийняття в експлуатацію, модернізації.

Кількісні значення додаткових показників результативності буде визначено статистичним методом під час проведення базового відстеження.

IX. Визначення заходів, за допомогою яких здійснюватиметься відстеження результативності дії регуляторного акта

Строки проведення базового та повторного відстеження результативності дії регуляторного акта:

базове відстеження результативності акта здійснюватиметься після набрання чинності актом, але не пізніше дня, з якого починається проведення повторного відстеження результативності цього акта;

повторне відстеження результативності акта здійснюватиметься через рік з дня набрання чинності регуляторним актом, але не пізніше двох років з дня набрання чинності регуляторним актом, шляхом аналізу звітності про стан об’єктів критичної інфраструктури;

періодичне відстеження результативності акта здійснюватиметься раз на три роки починаючи з дня закінчення заходів з повторного відстеження результативності акта шляхом порівняння показників із аналогічними показниками, що встановлені під час повторного відстеження.

Метод проведення відстеження результативності: статистичний.

Вид даних, за допомогою яких здійснюватиметься відстеження результативності: відстеження результативності регуляторного акта буде здійснюватися Міністерством розвитку громад та територій України шляхом обробки інформації, отриманої від обласних та Київської міської державних адміністрацій та операторів критичної інфраструктури, щодо питань у сфері захисту об’єктів критичної інфраструктури.

Цільові групи осіб, що обиратимуться для участі у відповідному опитуванні, чи наукові установи, що залучатимуться для проведення відстеження: відстеження буде проводитись співробітниками Міністерства розвитку громад та територій України, для чого будуть детально вивчатися надані обласними та Київською міською державними адміністраціями та операторами критичної інфраструктури звіти про стан захисту об’єктів критичної інфраструктури.

Віце-прем’єр-міністр з відновлення
України – Міністр розвитку громад
та територій України Олексій КУЛЕБА

«___» _____ 2025 р.

Повідомлення
про оприлюднення проєкту наказу Міністерства розвитку громад та територій України «Про затвердження вимог до захисту об'єктів критичної інфраструктури у секторах транспорту і пошти та системи життєзабезпечення»

1. Розробник:
Міністерство розвитку громад та територій України

2. Обгрунтування необхідності прийняття акта
Метою прийняття проєкту наказу Міністерства розвитку громад та територій України «Про затвердження вимог до захисту об'єктів критичної інфраструктури у секторах транспорту і пошти та системи життєзабезпечення» є приведення нормативно-правової бази у відповідність до пункту 4 частини першої статті 19 Закону України «Про критичну інфраструктуру» та виконання абзацу третього підпункту 5 пункту 1 рішення Ради національної безпеки і оборони України від 17 жовтня 2023 року «Про організацію захисту та забезпечення безпеки функціонування об'єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій», уведеного в дію Указом Президента України від 17 жовтня 2023 року № 695/2023.

3. Спосіб оприлюднення проєкту регуляторного акта
Проєкт акта розміщено на офіційному вебсайті Мінрозвитку (www.mtu.gov.ua).

4. Строк, протягом якого приймаються зауваження та пропозиції до проєкту регуляторного акта від фізичних та юридичних осіб, їх об'єднань:
Пропозиції та зауваження приймаються протягом одного місяця з дня оприлюднення.

5. Зауваження та пропозиції направляти на адресу:
Зауваження та пропозиції до проєкту акта надсилати електронною поштою на адресу: vki@mtu.gov.ua.

Віце-прем'єр-міністр з відновлення
України – Міністр розвитку громад
та територій України Олексій КУЛЕБА

«___» _____ 2025 р.