**ЗАТВЕРДЖЕНО  
постановою Кабінету Міністрів України  
від 14 жовтня 2022 р. № 1175**

ЗВІТ  
про виконання секторальним органом повноважень, визначених   
Законом України “Про критичну інфраструктуру”  
за \_\_\_\_\_\_\_ рік

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
(найменування секторального органу у сфері захисту критичної інфраструктури)

|  |  |  |  |
| --- | --- | --- | --- |
| Кількість об’єктів, одиниць | Категоризацію проведено, об’єктів | Категоризацію не проведено, об’єктів | Сплановано на \_\_\_\_\_\_\_\_ рік, об’єктів |

1. Категоризація об’єктів критичної інфраструктури:

2. Формування секторальних переліків об’єктів критичної інфраструктури - сформовано/не сформовано

3. Подання інформації до Реєстру об’єктів критичної інфраструктури:

|  |  |  |  |
| --- | --- | --- | --- |
| Кількість об’єктів, одиниць | Інформацію подано, об’єктів | Частка поданої інформації, відсотків | Сплановано на \_\_\_\_\_\_\_ рік, об’єктів |

4. Розроблення та затвердження:

1) вимоги до захисту об’єктів критичної інфраструктури відповідно до їх категорій:

|  |  |  |  |
| --- | --- | --- | --- |
| I категорія критичності | II категорія критичності | III категорія критичності | IV категорія критичності |
| розроблено/не розроблено | розроблено/не розроблено | розроблено/не розроблено | розроблено/не розроблено |

2) проектні загрози критичній інфраструктурі секторального рівня - розроблено/не розроблено

3) план взаємодії функціональних органів у сфері захисту критичної інфраструктури:

|  |  |  |  |
| --- | --- | --- | --- |
| У штатному режимі | У режимі готовності та запобігання реалізації загроз | У режимі реагування на виникнення кризової ситуації | У режимі відновлення штатного функціонування |
| розроблено/не розроблено | розроблено/не розроблено | розроблено/не розроблено | розроблено/не розроблено |

4) план взаємодії та підтримання життєво важливих функцій на випадок порушення функціонування об’єктів критичної інфраструктури - розроблено/не розроблено;

5) галузевий (регіональний) план і програми з протидії загрозам критичній інфраструктурі, включаючи аварійні плани, плани реагування на кризові ситуації, плани взаємодії, плани відновлення об’єктів критичної інфраструктури, плани проведення навчань та тренувань - розроблено/не розроблено.

5. Розроблення та впровадження норм і регламентів захисту критичної інфраструктури:

|  |  |  |
| --- | --- | --- |
| Зміст | Розроблення | Впровадження |
| Норми захисту критичної інфраструктури | розроблено/не розроблено | впроваджено/не впроваджено |
| Регламент захисту критичної інфраструктури | розроблено/не розроблено | впроваджено/не впроваджено |

6. Затвердження проектних загроз об’єктів критичної інфраструктури об’єктового рівня:

|  |  |  |  |
| --- | --- | --- | --- |
| Кількість об’єктів, одиниць | Затверджено, одиниць | Не затверджено, одиниць | Сплановано розроблення та затвердження на \_\_\_\_\_\_ рік, одиниць |

7. Погодження паспортів безпеки об’єктів критичної інфраструктури, наданих операторами критичної інфраструктури:

|  |  |  |  |
| --- | --- | --- | --- |
| Кількість об’єктів, одиниць | Погоджено, одиниць | Не погоджено, одиниць | Сплановано розроблення та погодження на \_\_\_\_\_\_\_ рік, одиниць |

8. Перевірка та оцінка стану захищеності об’єктів критичної інфраструктури:

|  |  |  |  |
| --- | --- | --- | --- |
| Кількість об’єктів, одиниць | Перевірено, об’єктів | | Сплановано перевірку  на \_\_\_\_\_\_\_\_ рік, одиниць |
| відповідає вимогам | не відповідає вимогам |

9. Організація функціонування системи обміну інформацією та взаємодії між суб’єктами національної системи захисту критичної інфраструктури - організовано/не організовано.

10. Укомплектованість структурних підрозділів з питань захисту критичної інфраструктури:

секторального органу:

|  |  |  |
| --- | --- | --- |
| Штатна чисельність, осіб | Фактична чисельність, осіб | Частка заміщених посад від штатної чисельності, відсотків |

операторів критичної інфраструктури:

|  |  |  |  |
| --- | --- | --- | --- |
| Найменування об’єкта | Окремі структурні підрозділи | | Визначено відповідальних осіб (в разі відсутності структурного підрозділу), осіб |
| штатна чисельність, осіб | фактична чисельність, осіб |
|

11. Зв’язок з об’єктами національної системи захисту критичної інфраструктури:

забезпечено на \_\_\_ об’єктах;

не забезпечено на \_\_\_ об’єктах, а саме: найменування оператора критичної інфраструктури.

12. Організація системи підготовки персоналу, навчань та тренувань щодо забезпечення стійкості та захисту секторів критичної інфраструктури:

підготовлено:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Здобувачів вищої освіти, осіб | Частка фактичної чисельності, відсотків | На курсах підвищення  кваліфікації, осіб | Частка фактичної чисельності, відсотків | У режимі відеоконференції, осіб | Частка фактичної чисельності, відсотків |

проведено:

секторальним органом

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Найменування заходу | Короткий зміст | Кількість залучених осіб | Кількість залучених відповідальних осіб | Частка  фактичної чисельності, відсотків | Кількість залучених керівників об’єктів критичної інфраструктури | Частка  фактичної чисельності, відсотків |
| Спільних командно-штабних навчань, кількість | | | | | | |
| Усього |  |  |  |  |  |  |
| Тактико-спеціальних навчань, кількість | | | | | | |
| Усього |  |  |  |  |  |  |
| Спільних тренувань, кількість | | | | | | |
| Усього |  |  |  |  |  |  |
| Занять із захисту, охорони, оборони, припинення злочинних дій, інцидентів  та кібератак проти об’єктів критичної інфраструктури, кількість | | | | | | |
| Усього |  |  |  |  |  |  |

операторами критичної інфраструктури

| Найменування заходу | Короткий зміст | Кількість залучених осіб | Кількість залучених відповідальних осіб | Частка фактичної чисельності, відсотків | Кількість залучених керівників об’єктів критичної інфраструктури | Частка фактичної чисельності, відсотків |
| --- | --- | --- | --- | --- | --- | --- |
| Навчань, кількість | | | | | | |
| Усього |  |  |  |  |  |  |
| Тренінгів, кількість | | | | | | |
| Усього |  |  |  |  |  |  |
| Практичних занять, кількість | | | | | | |
| Усього |  |  |  |  |  |  |
| Перевірок персоналу, який відповідає за охорону, безпеку та захист об’єктів критичної інфраструктури, кількість | | | | | | |
| Усього |  |  |  |  |  |  |

13. Стан фінансування, забезпечення силами, засобами і ресурсами функціонування системи захисту критичної інфраструктури:

Фінансування (витрати коштів):

|  |  |  |  |
| --- | --- | --- | --- |
| Джерело фінансування (кошти державного бюджету, місцевих бюджетів, власні кошти оператора критичної інфраструктури, кредити банків, кошти міжнародної технічної допомоги, інше) | Найменування заходу із забезпечення силами, засобами і ресурсами функціонування системи захисту критичної інфраструктури | Обсяг фінансування, тис. гривень | Частка загальної потреби фінансування заходів із забезпечення силами, засобами і ресурсами функціонування системи захисту критичної інфраструктури |

14. Наявність у об’єктів критичної інфраструктури необхідних резервів фінансових та матеріальних ресурсів для реагування на кризові ситуації та ліквідації їх наслідків - забезпечено/не забезпечено; потребує додаткового забезпечення із зазначенням об’єктів, що потребують додаткового забезпечення, прогнозована кількість ресурсів та запропоновані джерела фінансування (cтисло зазначається інформація за кожним об’єктом).

15. Проведення (участь) заходів щодо реагування на кризові ситуації, несанкціоноване втручання, інциденти безпеки:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Кількість заходів | | | | | |
| кризові ситуації | несанкціоноване втручання | інциденти безпеки, характеру | | | |
| природного | технічного | технологічного | внаслідок дії людського фактора |

16. Результати аналізу даних щодо критичної інфраструктури та її функціонування (про фактичний стан захищеності об’єкта критичної інфраструктури, дотримання вимог законодавства у сфері критичної інфраструктури, здійснення контролю за ризиками безпеки та удосконалення заходів, які здійснюються для забезпечення безпеки та стійкості об’єкта критичної інфраструктури, а також визначення перспектив подальшого функціонування і розвитку національної системи захисту критичної інфраструктури, про удосконалення системи захисту об’єктів критичної інфраструктури, а також про вжиття заходів до усунення виявлених недоліків або порушень).

17. Пропозиції до документів стратегічного планування, програмних документів щодо забезпечення стійкості та захисту критичної інфраструктури.

\_\_\_\_\_\_\_\_\_\_   
Примітки 1. У пунктах 2, 4-7, 9, 11 стисло (одним - двома реченнями) зазначається інформація про причини невиконання (у разі невиконання).

2. У пунктах 9, 11, стисло (одним - двома реченнями) зазначається відповідна інформація про виконання.

|  |  |  |
| --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (найменування посади керівника структурного підрозділуз питань захисту критичної інфраструктури) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (підпис) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (власне ім’я, прізвище) |

\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р.