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

ЗВІТ
про виконання оператором критичної інфраструктури повноважень, визначених Законом України
“Про критичну інфраструктуру” за 20\_\_\_ рік

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
(найменування оператора критичної інфраструктури)

1. Категоризація об’єкта - проведено/не проведено.

2. Подання інформації до Реєстру об’єктів критичної інфраструктури - подано/не подано.

3. Паспорт безпеки об’єкта критичної інфраструктури - розроблено/не розроблено.

4. Вимоги щодо організації захисту об’єкта критичної інфраструктури - розроблено/не розроблено.

5. Об’єктовий план заходів щодо забезпечення безпеки і стійкості критичної інфраструктури - розроблено/не розроблено; виконується/не виконується; оновлено/не оновлено (у разі необхідності).

6. Правила управління ризиками безпеки - розроблено/не розроблено; виконуються/не виконуються.

7. План локалізації та ліквідації наслідків аварій - розроблено/не розроблено.

8. План заходів з кіберзахисту - розроблено/не розроблено.

9. Оцінка ризиків - проведено/не проведено.

10. Обмін інформацією про ризики та загрози з іншими суб’єктами національної системи захисту критичної інфраструктури - організовано/не організовано.

11. Створення умов для належного виконання правоохоронними органами, розвідувальними та контррозвідувальними органами і підрозділами своїх завдань із захисту критичної інфраструктури - створено/не створено.

12. Участь у заходах із захисту повітряного простору - залучається/не залучається.

13. Захист інформації про системи управління, зв’язку, фізичну безпеку та кібербезпеку, забезпечення виконання встановлених законодавством вимог до роботи з інформацією з обмеженим доступом про об’єкти критичної інфраструктури - забезпечено/не забезпечено; витоки інформації відсутні/були (у разі наявності).

14. Забезпечення захисту об’єктів критичної інфраструктури:

створення, налагодження та підтримання функціонування ефективної системи фізичної безпеки - забезпечено/не забезпечено;

створення, налагодження та підтримання функціонування ефективної системи безпеки операційних систем (інформаційно-комунікаційних систем) та кібербезпеки - забезпечено/не забезпечено.

15. Заходи з реагування на інциденти, кризові ситуації, а також ліквідації їх наслідків на об’єктах критичної інфраструктури у взаємодії з іншими суб’єктами національної системи захисту критичної інфраструктури - організовано/не організовано.

16. Укомплектованість структурних підрозділів з питань захисту критичної інфраструктури:

|  |  |  |
| --- | --- | --- |
| Окремі структурні підрозділи | Визначено відповідальних осіб (в разі відсутності структурного підрозділу), осіб | Посадові інструкції осіб, відповідальних за організацію та забезпечення захисту об’єктів критичної інфраструктури |
| Штатна чисельність, осіб | Фактична чисельність, осіб | наявність | відсутність |

17. Зв’язок (взаємодія) із суб’єктом національної системи захисту критичної інфраструктури: забезпечено/не забезпечено.

18. Організація підготовки персоналу, навчання та тренувань щодо забезпечення стійкості та захисту структуриних підрозділів (відповідальних осіб) критичної інфраструктури:

підготовлено:

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

проведено:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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 |  |  |  |  |  |  |
| Перевірки персоналу, який відповідає за охорону, безпеку та захист об’єктів критичної інфраструктури, кількість |
| Усього |  |  |  |  |  |  |

19. Стан захисту персоналу, організації та здійснення евакуаційних заходів у разі виникнення надзвичайних ситуацій:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Забезпечення персоналу захисними спорудами цивільного захисту та спорудами подвійного призначення, відсотків | Забезпечення персоналу засобами індивідуального захисту, відсотків | Забезпечення об’єкта (об’єктів) критичної інфраструктури засобами радіаційного та хімічного захисту згідно з номенклатурою та нормами забезпечення, відсотків | Урахування вимог інженерно- технічних заходів цивільного захисту під час проектування та їх здійснення під час будівництва і експлуатації об’єкта (обʼєктів) критичної інфраструктури, відсотків | Володіння персоналом навичками дій у надзвичайних ситуаціях згідно з програмами цивільного захисту, відсотків | Розроблення планів та інструкцій з евакуації персоналу у разі виникнення надзвичайних ситуацій, розроблено/не розроблено |

20. 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, відсотків |

21. Наявність в об’єктів критичної інфраструктури необхідних резервів фінансових та матеріальних ресурсів для реагування на кризові ситуації та ліквідації їх наслідків - створено/не створено; обсяг, тис. гривень; перелік матеріальних засобів (стисло зазначається інформація за кожним об’єктом).

22. Кризові ситуації, несанкціоноване втручання, інциденти безпеки та інше, що відбулися на об’єкті критичної інфраструктури:

|  |
| --- |
| Кількість  |
| протиправних дій | фізичних атак | кризових ситуацій | несанкціонованих втручань | інциденти безпеки, характеру | інше |
| природного | технічного | технологічного | внаслідок дії людського фактора |

23. Забезпечення відновлення функціонування об’єктів критичної інфраструктури у разі виникнення аварій та інших небезпечних подій, вчинення протиправних дій - забезпечено/не забезпечено.

24. Загрози та ризики диверсій, терористичних актів, актів кібертероризму проти систем управління, операційних та інших систем, надзвичайних ситуацій.

\_\_\_\_\_\_\_\_\_\_
Примітки 1. У пунктах 1-15, 17, 21, 23 стисло (одним - двома реченнями) зазначається інформація про причини невиконання (у разі невиконання).

2. У пунктах 5, 6, 9-15, 17, 21, 23, 24 стисло (одним - двома реченнями) зазначається відповідна інформація про виконання.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(найменування посади керівника об’єкта критичної інфраструктури)(підпис)(власне ім’я, прізвище)

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