Редакція:

14.10.2022

КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 14 жовтня 2022 р. N 1175

Київ

Деякі питання подання інформації у сфері захисту критичної інфраструктури

Відповідно до частини другої статті 19 та пункту 4 частини четвертої статті 21 Закону України "Про критичну інфраструктуру" Кабінет Міністрів України **постановляє**:

Затвердити такі, що додаються:

форму річного звіту про виконання секторальним органом повноважень, визначених Законом України "Про критичну інфраструктуру";

форму річного звіту про виконання оператором критичної інфраструктури повноважень, визначених Законом України "Про критичну інфраструктуру".

Установити, що:

секторальні органи у сфері захисту критичної інфраструктури щороку до 30 січня подають уповноваженому органу у сфері захисту критичної інфраструктури України звіт про виконання повноважень, визначених Законом України "Про критичну інфраструктуру", за минулий рік;

оператори критичної інфраструктури щороку до 15 січня подають секторальним органам у сфері захисту критичної інфраструктури звіт про виконання повноважень, визначених Законом України "Про критичну інфраструктуру", за минулий рік.

Прем'єр-міністр України Д. ШМИГАЛЬ

Інд. 49

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 14 жовтня 2022 р. N 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	Ча фак чисе від
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 пр 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	Ча фак чисе від
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	Найменування заходу із забезпечення силами, засобами і ресурсами функціонування системи	Обсяг фінансування, тис. гривень	Частка загальної потреби фінансування заходів із

оператора критичної інфраструктури, кредити банків, кошти міжнародної технічної допомоги, інше)	захисту критичної інфраструктури		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 (стисло 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 підрозділу з питань захисту критичної інфраструктури) (підпис) (власне ім'я, прізвище)

___ _____ 20__ р.

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 14 жовтня 2022 р. N 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	Посадові інструкції осіб,

		відповідальних осіб (в разі відсутності структурного підрозділу), 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 структурних 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	Ча фак чисе від
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	Забезпечення персоналу засобами індивідуального захисту, відсотків	Забезпечення об'єкта (об'єктів) критичної інфраструктури засобами радіаційного та хімічного	Урахування вимог інженерно-технічних заходів цивільного захисту під час проектування	Володіння персоналом навичками дій у надзвичайних ситуаціях згідно з програмами	Розробл планів інструкц евакуа персона раз виникн надзвича

призначення, відсотків		захисту згідно з номенклатурою та нормами забезпечення, відсотків	та їх здійснення під час будівництва і експлуатації об'єкта (об'єктів) критичної інфраструктури, відсотків	цивільного захисту, відсотків	ситуац розробл не розробл

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						
				інциденти безпеки, хара		
протиправних дій	фізичних атак	кризових ситуацій	несанкціонованих втручань	природного	технічного	технологі

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.

_____