Пример Приказа О создании комиссии (наименование организации, учреждения) по категорированию объектов КИИ

|  |  |  |
| --- | --- | --- |
| от «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_201\_ г. |  | г. \_\_\_\_\_\_\_\_\_ |

|  |  |
| --- | --- |
| О создании комиссии (наименование организации, учреждения) комиссия по категорированию объектов КИИ (критической информационной инфраструктуры) |  |

В соответствии с Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации", Постановление Правительства РФ от 8 февраля 2018 г. № 127 “Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений”

в целях устойчивого функционирования объектов КИИ (наименование организации, учреждения) при проведении в отношении объектов КИИ компьютерных атак

Приказываю:

1. Создать комиссию по категорированию объектов КИИ.
   1. Утвердить состав Комиссии по категорированию объектов КИИ в составе:

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| (наименование должности) |  |  | (Ф.И.О.) |
|  |  |  |  |
| (наименование должности) |  |  | (Ф.И.О.) |
|  |  |  |  |
| (наименование должности) |  |  | (Ф.И.О.) |

1. Комиссии в месячный срок провести следующие мероприятия:

а) определить процессы, указанные в Правилах категорирования объектов критической информационной инфраструктуры Российской Федерации, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры;

б) выявить наличие критических процессов;

в) выявить объекты критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, а также готовит предложения для включения в перечень объектов;

г) рассмотреть возможные действия нарушителей в отношении объектов критической информационной инфраструктуры, а также иные источники угроз безопасности информации;

д) проанализировать угрозы безопасности информации и уязвимости, которые могут привести к возникновению компьютерных инцидентов на объектах критической информационной инфраструктуры;

е) оценить в соответствии с перечнем показателей критериев значимости масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;

ж) установить каждому из объектов критической информационной инфраструктуры одну из категорий значимости либо принять решение об отсутствии необходимости присвоения им категорий значимости.

3. Контроль за выполнением настоящего приказа возложить на \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Директор \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

С приказом ознакомлены:

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| (наименование должности) |  |  | (Ф.И.О.) |
|  |  |  |  |
| (наименование должности) |  |  | (Ф.И.О.) |
|  |  |  |  |
| (наименование должности) |  |  | (Ф.И.О.) |