Выполнила Исмакова Даяна, ИСИТ 189-1

(1) Постановление Правительства от 08 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»

(2)

1. Категорирование осуществляется субъектами критической информационной инфраструктуры (КИИ\*)
2. Объекты категорирования, которые обеспечивают следующие функции:
   1. управленческие,
   2. технологические,
   3. производственные,
   4. финансово-экономические

(3) Категорирование включает в себя:

1. определение процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры
2. выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий)
3. определение объектов критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;
4. формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию
5. оценку в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры
6. присвоение каждому из объектов критической информационной инфраструктуры одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости

(4) Присвоение значений

* Объекту критической информационной инфраструктуры по результатам категорирования присваивается в соответствии с перечнем показателей критериев значимости категория значимости с наивысшим значением.
* Если ни один из показателей критериев значимости неприменим для объекта критической информационной инфраструктуры или объект критической информационной инфраструктуры не соответствует ни одному показателю критериев значимости и их значениям, категория значимости не присваивается.
* 3 категории значимости:
  + Первая – самая высокая
  + Вторая - средняя
  + Третья – самая низкая

(5) Исходные данные для категорирования

1. сведения об объекте критической информационной инфраструктуры (назначение, архитектура объекта, применяемые программные и программно-аппаратные средства, взаимодействие с другими объектами критической информационной инфраструктуры, наличие и характеристики доступа к сетям связи);
2. процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры;
3. состав информации, обрабатываемой объектами критической информационной инфраструктуры, сервисы по управлению, контролю или мониторингу, предоставляемые объектами критической информационной инфраструктуры;
4. декларация промышленной безопасности опасного производственного объекта, декларация безопасности гидротехнического сооружения и паспорт объекта топливно-энергетического комплекса в случае, если на указанных объектах функционирует объект критической информационной инфраструктуры (если разработка указанных деклараций и паспорта предусмотрена законодательством Российской Федерации);
5. сведения о взаимодействии объекта критической информационной инфраструктуры с другими объектами критической информационной инфраструктуры и (или) о зависимости функционирования объекта критической информационной инфраструктуры от других таких объектов;
6. угрозы безопасности информации в отношении объекта критической информационной инфраструктуры, а также имеющиеся данные, в том числе статистические, о компьютерных инцидентах, произошедших ранее на объектах критической информационной инфраструктуры соответствующего типа.

(6) Комиссия по категорированию включает:

* Руководителя субъекта КИИ
* Работников субъекта КИИ, являющихся специалистами в области выполняемых функций или осуществляемых видов деятельности
* Работников субъекта КИИ, на которых возложены функции обеспечения безопасности
* Работников подразделения по защите государственной тайны субъекта КИИ
* Работников структурного подразделения по гражданской обороне и защите от чрезвычайных ситуаций
* Также возможно включение представителей государственных органов

(7) Комиссия по категорированию в ходе своей работы

* определяет процессы КИИ,
* выявляет наличие критических процессов у субъекта КИИ,
* выявляет объекты критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов,
* рассматривает возможные действия нарушителей в отношении объектов критической информационной инфраструктуры,
* анализирует угрозы безопасности информации и уязвимости,
* оценивает масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ,
* устанавливает каждому из объектов КИИ одну из категорий значимости, либо принимает решение об отсутствии необходимости присвоения им категорий значимости.

(8) Сроки

* Максимальный срок категорирования не должен превышать одного года со дня утверждения субъектом КИИ перечня объектов.
* Перечень объектов в течение 5 рабочих дней после утверждения направляется в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры.
* Субъект КИИ в течение 10 дней со дня утверждения акта направляет в федеральный орган исполнительной власти сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости, либо об отсутствии необходимости присвоения ему одной из таких категорий.

(9) Показатели критериев значимости

* Социальная значимость
  + Причинение ущерба жизни и здоровью людей
  + Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения
  + Прекращение или нарушение функционирования объектов транспортной инфраструктуры
  + Прекращение или нарушение функционирования сети связи, оцениваемые
  + Отсутствие доступа к государственной услуге

(10)

* Политическая значимость
  + Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции
  + Нарушение условий международного договора Российской Федерации
* Экономическая значимость
  + Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием и др.
  + Возникновение ущерба бюджетам Российской Федерации
  + Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций

(11)

* Экологическая значимость
  + Вредные воздействия на окружающую среду
* Значимость для обеспечения обороны страны, безопасности государства и правопорядка
  + Прекращение или нарушение (невыполнение установленных показателей) функционирования пункта управления (ситуационного центра), оцениваемое в уровне (значимости) пункта управления или ситуационного центра
  + Снижение показателей государственного оборонного заказа, выполняемого субъектом критической информационной инфраструктуры
  + Прекращение или нарушение функционирования (невыполнения установленных показателей) информационной системы в области обеспечения обороны страны