Проект

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

П О С Т А Н О В Л Е Н И Е

от «____» _____ 2017 г. №___

МОСКВА

Об утверждении показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, а также порядка и сроков осуществления их категорирования

В соответствии с пунктом 1 части 2 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Утвердить прилагаемые:

показатели критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значения;

порядок и сроки категорирования объектов критической информационной инфраструктуры Российской Федерации.

2. Федеральному органу исполнительной власти, уполномоченному в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, давать разъяснения по применению настоящего постановления.

3. Настоящее постановление вступает в силу с 1 января 2018 г.

Председатель Правительства
Российской Федерации Д.Медведев

УТВЕРЖДЕНЫ
постановлением Правительства
Российской Федерации
от «___»_____2017 г. №___

Показатели
критериев значимости объектов критической информационной инфраструктуры Российской Федерации
и их значения

№ п/п	Показатель	Значение показателя		
		III категория	**II категория**	**I категория**
1	**2**	**3**	**4**	**5**
I. Социальная значимость				
1.1	Возможно причинение ущерба жизни и здоровью людей, оцениваемое в количестве людей, жизни и здоровью которых возможно причинение ущерба (КЛ), человек	1<=КЛ<= 50	50<КЛ<=500	КЛ>500

1	2	3	4	5
1.2	Возможно прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, оцениваемое: а) в территории, на которой возможно нарушение обеспечения жизнедеятельности населения; б) в количестве людей, условия жизнедеятельности которых могут быть нарушены (КЛ), в тыс. чел.	затрагивает территорию одного муниципального образования или одной внутригородской территории города федерального значения; 50<=КЛ<1000	выходит за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не выходит за пределы территории одного субъекта Российской Федерации или территории города федерального значения; 1000<=КЛ<5000	выходит за пределы территории одного субъекта Российской Федерации или территории города федерального значения; КЛ=>5000
1.3	Возможно прекращение или нарушение функционирования объектов транспортной инфраструктуры, оцениваемое: а) в территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг; б) в количестве людей, для которых могут быть недоступны транспортные услуги (КЛ), в тыс. чел.	затрагивает территорию одного муниципального образования или одной внутригородской территории города федерального значения; 50<=КЛ<1000	выходит за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не выходит за пределы территории одного субъекта Российской Федерации или территории города федерального значения; 1000<=КЛ<5000	выходит за пределы территории одного субъекта Российской Федерации или территории города федерального значения; КЛ=>5000

1	2	3	4	5
1.4	Возможно прекращение или нарушение функционирования системы управления сетью связи, оцениваемое: а) в территории, на которой возможно прекращение или нарушение функционирования сети связи; б) в количестве людей, для которых могут быть не доступны услуги связи (КЛ), в тыс. чел.	затрагивает территорию одного муниципального образования или одной внутригородской территории города федерального значения; 50<=КЛ<1000	выходит за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не выходит за пределы территории одного субъекта Российской Федерации или территории города федерального значения; 1000<=КЛ<5000	выходит за пределы территории одного субъекта Российской Федерации или территории города федерального значения; КЛ=>5000
1.5	Возможно отсутствие доступа к государственным услугам, предоставляемым в электронном виде, оцениваемое в максимальном допустимом времени (Ч), в течение которого государственная услуга, предоставляемая в электронном виде, может быть недоступна для пользователей, в часах	24=>Ч>12	12=>Ч>6	6>Ч

1	2	3	4	5
II. Политическая значимость				
2.1	Возможно прекращение или нарушение функционирования более чем на 4 часа государственной информационной системы, используемой для реализации внутренней или внешней политики, оцениваемое в уровне (значимости) государственного органа	органы государственной власти субъекта Российской Федерации или города федерального значения	федеральный орган государственной власти	Администрация Президента Российской Федерации, Правительство Российской Федерации, Федеральное Собрание Российской Федерации, Совет Безопасности Российской Федерации, Верховный Суд Российской Федерации, Конституционный Суд Российской Федерации

1	2	3	4	5
2.2	Возможно прекращение и (или) нарушение функционирования более чем на 4 часа, а также подмена официального сайта государственного органа, оцениваемое в уровне (значимости) государственного органа	органы государственной власти субъекта Российской Федерации или города федерального значения	федеральный орган государственной власти	Администрация Президента Российской Федерации, Правительство Российской Федерации, Федеральное Собрание Российской Федерации, Совет Безопасности Российской Федерации, Верховный Суд Российской Федерации, Конституционный Суд Российской Федерации
2.3	Возможно нарушение условий заключенного международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемое в уровне международного договора Российской Федерации	договор межведомственного характера	межправительственный договор	межгосударствен-ный договор

1	2	3	4	5
III. Экономическая значимость				
3.1	Возможно возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным предприятием, государственной компанией, организацией с участием государства и (или) стратегическим акционерным обществом, стратегическим предприятием, оцениваемое в снижении уровня дохода (с учетом НДС, акцизов и иных обязательных платежей) по всем видам деятельности (Д), в процентах от прогнозируемого объема годового дохода по всем видам деятельности	5<Д<=10	10<Д<=15	Д>15
3.2	Возможно возникновение ущерба бюджетам Российской Федерации, оцениваемое: а) в снижении доходов федерального бюджета (ФБ), в процентах от прогнозируемого годового дохода бюджета; б) в снижении доходов бюджета субъекта Российской Федерации (РБ), в процентах от прогнозируемого годового дохода бюджета; в) в снижении доходов бюджетов государственных внебюджетных фондов (БФ), в процентах от прогнозируемого годового дохода бюджета	0,001<ФБ <=0,05; 0,001<РБ<=0,05; 0,01<БФ<=0,5	0,05<ФБ<=0,1; 0,05<РБ<=0,1; 0,5<БФ<=1	ФБ>0,1; РБ>0,1; БФ>1

1	2	3	4	5
3.3	Возможно прекращение или нарушение проведения клиентами операций по банковским счетам/без открытия банковского счета или операций, осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, оцениваемое среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций ($Н_{КО}$), в млн. единиц (расчет осуществляется по итогам года, а для создаваемых объектов на основе прогнозных значений)	$3,0< Н_{КО} <=70,0$	$70,0< Н_{КО} <=120,0$	$120,0< Н_{КО}$

1	2	3	4	5
IV. Экологическая значимость				
4.1	Возможны вредные воздействия на окружающую среду (ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосферу, ухудшение состояния площадей земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия), оцениваемое: а) в территории, на которой окружающая среда может подвергнуться вредным воздействиям; б) в количестве людей, которые могут быть подвержены вредным воздействиям (КЛ), в тыс. чел.	затрагивает территорию одного муниципального образования или одной внутригородской территории города федерального значения; 50<=КЛ<1000	выходит за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не выходит за пределы территории одного субъекта Российской Федерации или территории города федерального значения; 1000<=КЛ<5000	выходит за пределы территории одного субъекта Российской Федерации или территории города федерального значения; КЛ=>5000

1	2	3	4	5
V. Значимость для обеспечения обороны страны, безопасности государства и правопорядка				
5.1	Возможно прекращение или нарушение (в том числе невыполнение установленных временных показателей) функционирования пункта управления (ситуационного центра), оцениваемое в уровне (значимости) пункта управления или ситуационного центра (ПУ)	органы государственной власти субъекта Российской Федерации или города федерального значения	федеральный орган государственной власти или государственная корпорация	пункт управления государством или ситуационный центр Администрации Президента Российской Федерации, Правительства Российской Федерации, Федерального Собрания Российской Федерации, Совета Безопасности Российской Федерации, Верховного Суда Российской Федерации, Конституционного Суда Российской Федерации

1	2	3	4	5
5.2	Возможно снижение показателей государственного оборонного заказа, выполняемого субъектом критической информационной инфраструктуры, оцениваемое: а) в снижение объемов продукции (работ, услуг) в заданный период времени (ОП), в процентах от заданного объема продукции; б) в увеличении времени выпуска продукции (работ, услуг) с заданным объемом (ВП), в процентах от установленного времени выпуска продукции	5<ОП<=10; 3<ВП<=10	10<ОП<=15; 10<ВП<=40	ОП>15; ВП>40

Утверждены
постановлением Правительства
Российской Федерации
от «___»_____ 2017 г. №___

Порядок и сроки категорирования объектов критической информационной инфраструктуры Российской Федерации

1. Настоящий Порядок определяет состав работ и сроки категорирования объектов критической информационной инфраструктуры Российской Федерации (далее – критическая информационная инфраструктура).

2. Категорирование объектов критической информационной инфраструктуры представляет собой установление соответствия каждого объекта критической информационной инфраструктуры критериям значимости и их показателям, присвоение объекту критической информационной инфраструктуры одной из категорий значимости, а также проверку сведений о результатах присвоения категории значимости.

3. Категорирование объектов критической информационной инфраструктуры осуществляется субъектами критической информационной инфраструктуры в отношении принадлежащих им на праве собственности, аренды или на ином законном основании объектов критической информационной инфраструктуры.

4. Категорированию подлежат объекты критической информационной инфраструктуры, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы (далее – процессы) в рамках выполнения функций или осуществления видов деятельности субъектов критической информационной инфраструктуры.

5. Определение категорий значимости объектов критической информационной инфраструктуры осуществляется на основании показателей критериев значимости объектов критической информационной инфраструктуры и их значений, утвержденных Правительством Российской Федерации.

6. Категорирование объектов критической информационной инфраструктуры включает:

а) определение всех процессов в рамках выполнения функций или осуществления видов деятельности субъекта критической информационной инфраструктуры;

б) выявление процессов, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка, выраженным в показателях критериев значимости (далее - критические процессы);

в) определение объектов критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения

выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию;

г) оценку в соответствии со значениями показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;

д) установление соответствия объектов критической информационной инфраструктуры значениям показателей критериев значимости и присвоение каждому из них одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости.

7. По результатам категорирования объекту критической информационной инфраструктуры присваивается наивысшая категория, соответствующая показателю критериев значимости с наивысшим значением.

Для каждого показателя критериев значимости, для которого установлено более одного значения (территория, количество людей), оценка производится по каждому из значений, а категория присваивается по наивысшему значению показателя.

Если показатель критерия значимости неприменим для объекта критической информационной инфраструктуры или объект критической информационной инфраструктуры не соответствует ни одному показателю критериев значимости и их значениям, категория такому объекту критической информационной инфраструктуры не присваивается.

8. Устанавливаются три категории значимости объектов критической информационной инфраструктуры – первая, вторая, третья. Самая высокая категория – первая, самая низкая – третья.

9. Категория значимости вновь создаваемого объекта критической информационной инфраструктуры определяется при формировании техническим заказчиком, застройщиком или агентом требований к объекту критической информационной инфраструктуры с учетом имеющихся исходных данных о критических процессах субъекта критической информационной инфраструктуры.

Категория значимости модернизируемого объекта критической информационной инфраструктуры определяется при формировании субъектом критической информационной инфраструктуры требований на его модернизацию.

Категория значимости создаваемого или модернизируемого объекта критической информационной инфраструктуры может быть уточнена в ходе его проектирования.

10. Категорирование объектов критической информационной инфраструктуры, принадлежащих одному субъекту критической информационной инфраструктуры, но используемых для целей контроля и управления технологическим и (или) производственным оборудованием, принадлежащем другому хозяйствующему субъекту, осуществляется на основе

исходных данных, представляемых этим хозяйствующим субъектом.

11. Исходными данными для категорирования объекта критической информационной инфраструктуры являются:

а) 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);

б) процессы в рамках выполнения функций или осуществления видов деятельности субъекта критической информационной инфраструктуры;

в) виды информации, обрабатываемые объектами критической информационной инфраструктуры, сервисы по управлению, контролю или мониторингу, предоставляемые объектами критической информационной инфраструктуры;

г) декларация промышленной безопасности опасного производственного объекта, декларация безопасности гидротехнического сооружения, на которых функционируют объект критической информационной инфраструктуры, если их разработка предусмотрена законодательством Российской Федерации;

д) сведения о взаимодействии объекта критической информационной инфраструктуры с другими объектами критической информационной инфраструктуры и (или) зависимость от их функционирования;

е) модели угроз безопасности информации и нарушителей в отношении объекта критической информационной инфраструктуры, а также имеющиеся данные, в том числе статистические, о компьютерных инцидентах, произошедших ранее на объектах критической информационной инфраструктуры данного типа.

12. Для проведения категорирования объекта критической информационной инфраструктуры решением руководителя субъекта критической информационной инфраструктуры создается комиссия по категорированию (далее - комиссия), в состав которой включаются:

а) руководитель субъекта критической информационной инфраструктуры или уполномоченное им лицо;

б) работники субъекта критической информационной инфраструктуры, являющиеся специалистами в области выполняемых функций или осуществляемых видов деятельности, в области информационных технологий и связи, по эксплуатации основного технологического оборудования, технологической (промышленной) и пожарной безопасности, контролю за опасными веществами и материалами, учету опасных веществ и материалов;

в) работники субъекта критической информационной инфраструктуры, на которых возложены функции обеспечения безопасности (информационной безопасности) объектов критической информационной инфраструктуры;

г) работники подразделения по защите государственной тайны субъекта критической информационной инфраструктуры (в случае, если объект критической информационной инфраструктуры обрабатывает информацию, составляющую государственную тайну);

д) работники структурного подразделения по гражданской обороне объекта или работники, уполномоченные на решение задач в области гражданской обороны.

В состав комиссии могут включаться представители государственных органов и российских юридических лиц, выполняющих функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, по согласованию с ними.

13. Комиссию возглавляет руководитель субъекта критической информационной инфраструктуры или уполномоченное им лицо.

14. В ходе работы комиссия:

а) определяет процессы в рамках выполнения функций или осуществления видов деятельности субъекта критической информационной инфраструктуры;

б) выявляет наличие критических процессов у субъекта критической информационной инфраструктуры;

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

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

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

е) оценивает возможные последствия в случае возникновения компьютерных инцидентов на объекте критической информационной инфраструктуры в соответствии с показателями критериев значимости;

д) устанавливает соответствие объектов критической информационной инфраструктуры значениям показателей критериев значимости и присваивает каждому из них одну из категорий значимости либо не присваивает ни одной из категорий значимости.

15. Субъект критической информационной инфраструктуры в течение шести месяцев со дня вступления в силу настоящего Порядка формирует перечень объектов критической информационной инфраструктуры, подлежащих категорированию, с указанием сроков проведения их категорирования.

Максимальный срок категорирования объектов критической информационной инфраструктуры не должен превышать одного года со дня утверждения субъектом критической информационной инфраструктуры перечня объектов критической информационной инфраструктуры, подлежащих категорированию.

Перечень объектов критической информационной инфраструктуры, подлежащих категорированию, утверждается субъектом критической информационной инфраструктуры по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры, и государственным органом или российским юридическим лицом, выполняющим функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере.

16. Решение комиссии оформляется актом категорирования, который должен содержать сведения об объекте критической информационной инфраструктуры, результаты анализа угроз безопасности информации объекта критической информационной инфраструктуры, реализованные меры по обеспечению безопасности объекта критической информационной инфраструктуры, сведения о присвоенной объекту критической информационной инфраструктуры категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, а также сведения о необходимых мерах по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры.

Акт категорирования подписывается членами комиссии и утверждается руководителем субъекта критической информационной инфраструктуры.

Субъект критической информационной инфраструктуры обеспечивает хранение акта категорирования до вывода из эксплуатации объекта критической информационной инфраструктуры или до изменения категории значимости объекта критической информационной инфраструктуры.

17. Субъект критической информационной инфраструктуры в десятидневный срок со дня утверждения акта категорирования направляет в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. Указанные сведения включают:

сведения об объекте критической информационной инфраструктуры (наименование, места (адреса) размещения, сфера (область) деятельности, назначение и критические процессы, для обеспечения которых используется объект, архитектура объекта);

сведения о субъекте критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежит объект критической информационной инфраструктуры (наименование, юридический и фактический адреса, подразделение (работники), на которое (которых) возложены функции по обеспечению безопасности объекта критической информационной инфраструктуры);

сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи с указанием наименования сетей электросвязи и способов взаимодействия;

сведения о лице, эксплуатирующем объект критической информационной инфраструктуры (наименование, юридический и фактический адреса);

сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры, в том числе средствах, используемых для обеспечения безопасности объекта критической информационной инфраструктуры и их сертификатах соответствия требованиям по безопасности информации (при наличии);

сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта критической информационной инфраструктуры либо об отсутствии таких угроз;

возможные последствия в случае возникновения компьютерных инцидентов на объекте критической информационной инфраструктуры либо сведения об отсутствии таких последствий;

категория значимости, которая присвоена объекту критической информационной инфраструктуры, или сведения об отсутствии необходимости присвоения одной из категорий значимости, а также сведения о результатах оценки показателей критериев значимости;

организационные и технические меры, применяемые для обеспечения безопасности объекта критической информационной инфраструктуры, либо сведения об отсутствии необходимости применения указанных мер.

Сведения направляются по форме, утверждаемой федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры.

18. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, в тридцатидневный срок со дня получения сведений о результатах категорирования проверяет соблюдение настоящего Порядка и правильность присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо не присвоения ему ни одной из категорий значимости.

19. В случае если субъектом критической информационной инфраструктуры соблюден настоящий Порядок и объекту критической информационной инфраструктуры правильно присвоена одна из категорий значимости, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, вносит сведения о таком объекте критической информационной инфраструктуры в реестр значимых объектов критической информационной инфраструктуры, о чем в десятидневный срок уведомляется субъект критической информационной инфраструктуры.

Совокупные сведения об объектах критической информационной инфраструктуры, включенные в реестр значимых объектов, подлежат защите в соответствии с законодательством Российской Федерации о государственной

тайне.

20. В случае, если федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры, выявлены нарушения порядка осуществления категорирования и (или) объекту критической информационной инфраструктуры неправильно присвоена одна из категорий значимости и (или) необоснованно не присвоена ни одна из таких категорий и (или) субъектом критической информационной инфраструктуры представлены неполные и (или) недостоверные сведения о результатах присвоения такому объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, в десятидневный срок со дня поступления представленных сведений о результатах категорирования объекта критической информационной инфраструктуры возвращает их в письменном виде субъекту критической информационной инфраструктуры с мотивированным обоснованием причин возврата.

21. Субъект критической информационной инфраструктуры после получения мотивированного обоснования причин возврата сведений о результатах категорирования объекта критической информационной инфраструктуры не более чем в десятидневный срок устраняет отмеченные недостатки и повторно направляет такие сведения в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры.

22. В случае непредставления субъектом критической информационной инфраструктуры сведений о результатах категорирования объекта критической информационной инфраструктуры федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, направляет в адрес указанного субъекта требование о необходимости соблюдения положений статьи 7 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» и настоящего Порядка.

23. Категория значимости, к которой отнесен значимый объект критической информационной инфраструктуры, может быть изменена в порядке, предусмотренном для категорирования, в следующих случаях:

а) по мотивированному решению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры, принятому по результатам проверки, проведенной в рамках осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры;

б) в случае изменения значимого объекта критической информационной инфраструктуры, в результате которого такой объект перестал соответствовать критериям значимости и показателям их значений, на основании которых ему

была присвоена определенная категория значимости;

в) в связи с ликвидацией, реорганизацией субъекта критической информационной инфраструктуры и (или) изменением его организационно-правовой формы, в результате которых были изменены либо утрачены признаки субъекта критической информационной инфраструктуры.

24. Субъект критической информационной инфраструктуры не реже, чем один раз в 5 лет осуществляет пересмотр установленной категории значимости объекта критической информационной инфраструктуры в соответствии с настоящим Порядком. В случае изменения категории значимости объекта критической информационной инфраструктуры, сведения о результатах пересмотра категории направляются в федеральный орган, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры.