

**Межпарламентская Ассамблея государств – участников
Содружества Независимых Государств**

**МОДЕЛЬНЫЙ РЕГЛАМЕНТ
административных процедур, осуществляемых уполномоченными
органами в сфере обеспечения информационной безопасности
государств – участников СНГ**

Обеспечение информационной безопасности является важной стратегической задачей государства, интересы которого предполагают реализацию механизмов защиты от внутренних и внешних угроз различных объектов информационно-коммуникационной инфраструктуры, и в первую очередь объектов, отнесенных к критически важным.

В сфере информатизации к критически важным объектам относят объекты:

- осуществляющие функции информационной системы, нарушение (прекращение) функционирования которой может привести к значительным негативным последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах;
- обеспечивающие предоставление значительного объема информационных услуг, частичное или полное прекращение оказания которых может привести к значительным негативным последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах.

Основным критерием отнесения объекта информационной инфраструктуры к критически важному является уровень возможных последствий нарушения (прекращения) его функционирования:

утрата государственного управления страной или административно-территориальной единицей;

потеря управления экономикой страны или административно-территориальной единицы;

необратимое негативное изменение (или разрушение) государственного управления или экономики страны, или административно-территориальной единицы;

существенное снижение безопасности жизнедеятельности населения, проживающего на территории страны или административно-территориальной единицы на длительный период.

№	Наименование административной процедуры	Уровни осуществления административной процедуры (инициатор)	Перечень документов и (или) сведений, представляемых в уполномоченный орган для осуществления административной процедуры	Перечень операций в рамках административной процедуры	Орган, уполномоченный на проведение административной процедуры	Срок осуществления административной процедуры	Ожидаемый результат
1	Регистрация (отнесение) объектов информационно-коммуникационной инфраструктуры к критически важным объектам (ИКИ к КВО)	<p>1. Локальный уровень (эксплуатирующая организация).</p> <p>2. Региональный уровень (местный, региональный орган государственного управления).</p> <p>3. Государственный уровень (государственный орган исполнительной власти)</p>	<p>1. Технические условия на ИКИ КВО</p> <p>2. Проект ИКИ КВО</p> <p>3. Заключение внутреннего аудита (для объектов 1-го уровня)</p> <p>4. Заявка на регистрацию КВО</p> <p>5. Заключение внешнего аудита (для объектов 2- и 3-го уровней)</p> <p>6. Протокол несоответствий в рамках аудита (при их наличии)</p> <p>7. Лист коррекции несоответствий (при их наличии)</p>	<p>1. Получение технических условий на разработку проекта ИКИ КВО.</p> <p>2. Проектирование и монтаж объекта ИКИ КВО с учетом выполнения условий промышленной, радиационной, пожарной и информационной безопасности, а также иных правил, обеспечивающих безопасный ввод в эксплуатацию, безопасную эксплуатацию и безопасный вывод из эксплуатации</p>	Уполномоченный государственный орган в сфере технической защиты информации (ТЗИ)	До одного месяца. При необходимости срок может быть продлен до трех месяцев (КВО 2- и 3-го уровней)	Включение в государственный реестр критически важных объектов информационно-коммуникационной инфраструктуры государства (Реестр)

				<p>соответствующих объектов.</p> <p>3. Осуществление внутреннего аудита о выполнении Правил.</p> <p>4. Составление заключения о соответствии правилам</p> <p>5. Подача заявки на включение в государственный реестр.</p> <p>6. Рассмотрение заявки в уполномоченном государственном органе.</p> <p>7. Внешний аудит ИКИ КВО, составление заключения.</p> <p>8. Корректировка несоответствий (при необходимости).</p> <p>9. Регистрация объекта ИКИ КВО в государственном реестре</p>			
--	--	--	--	--	--	--	--

2	Внешний аудит информационно-коммуникационной инфраструктуры критически важных объектов (ИКИ КВО)	<ol style="list-style-type: none"> 1. Локальный уровень (эксплуатирующая организация). 2. Региональный уровень (местный, региональный орган государственного управления). 3. Государственный уровень (государственный орган исполнительной власти) 	<ol style="list-style-type: none"> 1. Заявка на осуществление внешнего аудита ИКИ КВО. 2. Проект ИКИ КВО 3. Заключение внутреннего аудита (для объектов всех уровней) 	<ol style="list-style-type: none"> 1. Проведение аудита объекта на предмет выполнения условий промышленной, радиационной, пожарной и информационной безопасности, а также иных правил, обеспечивающих безопасную эксплуатацию соответствующих объектов. 2. Составление заключения о результатах внешнего аудита. 3. Выдача протокола несоответствий (при необходимости). 4. Устранение несоответствий (при необходимости). 5. Осуществление аудита по выявленным несоответствиям. 6. Составление дополнительного 	Уполномоченный государственный орган в сфере технической защиты информации (ТЗИ)	До одного месяца. (периодичность для объектов 1-го уровня – не менее одного раза в три года, 2- и 3-го уровней – не менее одного раза в год)	Составление заключения (срок действия – один год) Внесение в Реестр сведений о результатах внешнего аудита
---	--	---	--	--	--	---	---

				заклучения. 7. Регистрация заключений (основного и дополнительного) в Реестре			
3	Исключение объектов информационно-коммуникационной инфраструктуры из Реестра	1. Локальный уровень (эксплуатирующая организация). 2. Региональный уровень (местный, региональный орган государственного управления). 3. Государственный уровень (государственный орган исполнительной власти)	1. Заявка на исключение из Реестра объекта ИКИ КВО. 2. Заключение внешнего аудита о возможности исключения из Реестра (для объектов всех уровней)	1. Подача заявки на исключение из Реестра. 2. Рассмотрение заявки в уполномоченном государственном органе. 3. Внешний аудит ИКИ КВО, составление заключения о возможности исключения. 4. Корректировка несоответствий (при необходимости). 5. Исключение объекта ИКИ КВО из Реестра	Уполномоченный государственный орган в сфере технической защиты информации (ТЗИ)	До одного месяца.	Исключение из государственного реестра критически важных объектов информационно-коммуникационной инфраструктуры государства

Принят на сорок первом
 пленарном заседании
 Межпарламентской Ассамблеи
 государств – участников СНГ
 (постановление № 41-17 от 28 ноября 2014 года)