

# Чеклист готовности к требованиям Приказа ФСТЭК России No117

Требования по безопасности информации при создании и эксплуатации значимых объектов КИИ

Экспресс-чеклист: охватывает 29 ключевых требований из 6 блоков. Полный аудит включает 80+ проверочных пунктов.

Организация: \_\_\_\_\_

Объект КИИ / ИС: \_\_\_\_\_

Дата проверки: \_\_\_\_\_ Ответственный: \_\_\_\_\_

Обозначения: V — выполнено ~ — частично X — не выполнено — — не применимо

## 1. Инвентаризация и категорирование объектов КИИ

Требования §§ 6–8 Приказа No117, 187-ФЗ ст. 7

No	Требование	От м.	Документ / Свидетельство	Примечание
1.1	Определён перечень объектов КИИ организации		Перечень объектов КИИ	
1.2	Проведено категорирование объектов КИИ, акты утверждены		Акты категорирования	
1.3	Сведения о категорировании направлены во ФСТЭК в 10-дневный срок		Уведомление ФСТЭК + квитанция	
1.4	Категорирование актуализировано при изменениях ИС		Протокол пересмотра	
1.5	Реестр ИТ-активов объекта КИИ ведётся и актуален		Реестр активов / ИТАМ-система	
No	Требование	От м.	Документ / Свидетельство	Примечание
1.1	Определён перечень объектов КИИ организации		Перечень объектов КИИ	
1.2	Проведено категорирование объектов КИИ, акты утверждены		Акты категорирования	
1.3	Сведения о категорировании направлены во ФСТЭК в 10-дневный срок		Уведомление ФСТЭК + квитанция	
1.4	Категорирование актуализировано при изменениях ИС		Протокол пересмотра	
1.5	Реестр ИТ-активов объекта КИИ ведётся и актуален		Реестр активов / ИТАМ-система	

## 2. Модель угроз и нарушителя

Требования §§ 11–14 Приказа No117, Методика ФСТЭК 2021

No	Требование	От м.	Документ / Свидетельство	Примечание
2.1	Разработана и утверждена модель угроз для каждого значимого объекта КИИ		Модель угроз (документ)	
2.2	Модель угроз разработана по методике ФСТЭК 2021 года		Ссылка на методику в МУ	
2.3	Определены актуальные угрозы и нарушители		Раздел «Актуальные угрозы» МУ	
2.4	Модель угроз пересматривается при изменениях ИС или появлении новых угроз в БДУ		Протокол актуализации МУ	

№	Требование	От м.	Документ / Свидетельство	Примечание
2.1	Разработана и утверждена модель угроз для каждого значимого объекта КИИ		Модель угроз (документ)	
2.2	Модель угроз разработана по методике ФСТЭК 2021 года		Ссылка на методику в МУ	
2.3	Определены актуальные угрозы и нарушители		Раздел «Актуальные угрозы» МУ	
2.4	Модель угроз пересматривается при изменениях ИС или появлении новых угроз в БДУ		Протокол актуализации МУ	

### 3. Система защиты объекта КИИ

Требования §§ 15–30 Приказа №117

№	Требование	От м.	Документ / Свидетельство	Примечание
3.1	Разработано техническое задание на систему защиты информации (ТЗ на СЗИ)		ТЗ на СЗИ	
3.2	Выбраны и внедрены меры защиты в соответствии с уровнем значимости объекта КИИ		Перечень мер / Технический проект	
3.3	Применяемые СЗИ сертифицированы ФСТЭК или ФСБ (при необходимости)		Сертификаты ФСТЭК / ФСБ	
3.4	Проведена аттестация системы защиты (для 1 и 2 категорий — обязательно)		Аттестат соответствия	
3.5	Обеспечена физическая защита объектов КИИ		Регламент физической защиты	
№	Требование	От м.	Документ / Свидетельство	Примечание
3.1	Разработано техническое задание на систему защиты информации (ТЗ на СЗИ)		ТЗ на СЗИ	
3.2	Выбраны и внедрены меры защиты в соответствии с уровнем значимости объекта КИИ		Перечень мер / Технический проект	
3.3	Применяемые СЗИ сертифицированы ФСТЭК или ФСБ (при необходимости)		Сертификаты ФСТЭК / ФСБ	
3.4	Проведена аттестация системы защиты (для 1 и 2 категорий — обязательно)		Аттестат соответствия	
3.5	Обеспечена физическая защита объектов КИИ		Регламент физической защиты	

#### 4. Управление уязвимостями

Требования §§ 31–35 Приказа No117 | Рекомендуемые сроки: критические — 24 ч, высокие — 7 дней, средние — 30 дней (внутренний регламент)

№	Требование	От м.	Документ / Свидетельство	Примечание
4.1	Налажен процесс мониторинга уязвимостей (использование БДУ ФСТЭК)		Регламент VM / подписка на БДУ	
4.2	Соблюдаются сроки устранения уязвимостей согласно внутреннему регламенту		Отчёты о выполнении SLA	
4.3	Проводится регулярное сканирование объектов КИИ на уязвимости		Отчёты сканирования	
4.4	Ведётся реестр выявленных и устранённых уязвимостей		Реестр уязвимостей	
4.5	При невозможности устранения — применены компенсирующие меры с обоснованием		Акт о компенсирующих мерах	
№	Требование	От м.	Документ / Свидетельство	Примечание
4.1	Налажен процесс мониторинга уязвимостей (использование БДУ ФСТЭК)		Регламент VM / подписка на БДУ	
4.2	Соблюдаются сроки устранения уязвимостей согласно внутреннему регламенту		Отчёты о выполнении SLA	
4.3	Проводится регулярное сканирование объектов КИИ на уязвимости		Отчёты сканирования	
4.4	Ведётся реестр выявленных и устранённых уязвимостей		Реестр уязвимостей	
4.5	При невозможности устранения — применены компенсирующие меры с обоснованием		Акт о компенсирующих мерах	

#### 5. Реагирование на компьютерные инциденты

Требования §§ 36–40 Приказа No117, Приказ ФСБ No282, 187-ФЗ ст. 9

№	Требование	От м.	Документ / Свидетельство	Примечание
5.1	Организовано взаимодействие с ГосСОПКА (подключение или через корпоративный центр)		Договор с НКЦКИ / Соглашение	
5.2	Разработан и утверждён план реагирования на инциденты		План реагирования	
5.3	Инциденты на значимых объектах КИИ передаются в НКЦКИ		Журнал переданных инцидентов	
5.4	Уведомление НКЦКИ направлено в течение 3 ч с момента обнаружения (187-ФЗ, ст. 9, ч. 4)		Уведомление НКЦКИ + отметка времени	
5.5	Проводятся тренировки по реагированию на инциденты		Отчёты о тренировках	
№	Требование	От м.	Документ / Свидетельство	Примечание
5.1	Организовано взаимодействие с ГосСОПКА (подключение или через корпоративный центр)		Договор с НКЦКИ / Соглашение	
5.2	Разработан и утверждён план реагирования на инциденты		План реагирования	

№	Требование	От м.	Документ / Свидетельство	Примечание
5.3	Инциденты на значимых объектах КИИ передаются в НКЦКИ		Журнал переданных инцидентов	
5.4	Уведомление НКЦКИ направлено в течение 3 ч с момента обнаружения (187-ФЗ, ст. 9, ч. 4)		Уведомление НКЦКИ + отметка времени	
5.5	Проводятся тренировки по реагированию на инциденты		Отчёты о тренировках	

## 6. Организационные меры и персонал

Требования §§ 41–48 Приказа №117

№	Требование	От м.	Документ / Свидетельство	Примечание
6.1	Назначен ответственный за обеспечение безопасности объекта КИИ		Приказ о назначении	
6.2	Разработаны и утверждены организационно-распорядительные документы по ИБ		ОРД по ИБ (перечень)	
6.3	Персонал прошёл инструктаж по требованиям ИБ объекта КИИ		Журнал инструктажей	
6.4	Ведётся контроль выполнения требований безопасности		Отчёты внутреннего контроля	
№	Требование	От м.	Документ / Свидетельство	Примечание
6.1	Назначен ответственный за обеспечение безопасности объекта КИИ		Приказ о назначении	
6.2	Разработаны и утверждены организационно-распорядительные документы по ИБ		ОРД по ИБ (перечень)	
6.3	Персонал прошёл инструктаж по требованиям ИБ объекта КИИ		Журнал инструктажей	
6.4	Ведётся контроль выполнения требований безопасности		Отчёты внутреннего контроля	

Важно: Данный чеклист является вспомогательным инструментом и не заменяет официальные документы аттестации. Для полной оценки соответствия рекомендуется привлечение лицензиата ФСТЭК.

## Итоговая оценка

Категория	Пунктов	Выполнено	Частично	Не выполнено	% соотв.
1. Инвентаризация и категорирование	5				
2. Модель угроз	4				
3. Система защиты	5				
4. Управление уязвимостями	5				
5. Реагирование на инциденты	4				
6. Организационные меры	4				
<b>ИТОГО</b>	<b>27</b>				

Автоматизируйте выполнение этих требований с КиберОснова SGRC — пункты 1.5, 3.2, 4.1–4.4, 5.1–5.4 контролируются системой автоматически. Попробуйте бесплатно: [sgrc.cyberosnova.ru/platforma/fstek-117/](https://sgrc.cyberosnova.ru/platforma/fstek-117/)

---

Подпись ответственного за ИБ

---

Дата проведения проверки

---

Подпись руководителя