

**Вопросы реализации
Федерального закона
«О безопасности критической
информационной инфраструктуры
Российской Федерации»**



ТОРБЕНКО Елена Борисовна
Заместитель начальника управления ФСТЭК России

Нормативные правовые акты в области обеспечения безопасности КИИ, разработанные ФСТЭК России



Указ Президента
Российской Федерации
от 25 ноября 2017 г. № 569

**О внесении изменений
в Положение о
Федеральной службе по
техническому
и экспортному контролю,
утвержденное Указом
Президента Российской
Федерации
от 16 августа 2004 г.
№ 1085**



Указ Президента
Российской Федерации
от 2 марта 2018 г. № 98

**О внесении изменений
в Перечень сведений,
отнесенных к
государственной тайне,
утвержденный Указом
Президента Российской
Федерации от 30 ноября
1995 г. № 1203**



Постановление Правительства
Российской Федерации
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**



Постановление Правительства
Российской Федерации
от 17 февраля 2018 г. № 162

**Об утверждении Правил
осуществления
государственного
контроля в области
обеспечения безопасности
значимых объектов
критической
информационной
инфраструктуры**



Приказ ФСТЭК России
от 21 декабря 2017 г. № 235

**Об утверждении
требований к созданию
систем безопасности
значимых объектов КИИ**

(зарегистрирован Минюстом
России 22 февраля 2018 г.,
рег. № 50118)



Приказ ФСТЭК России
от 22 декабря 2017 г. № 236

**Об утверждении формы
направления сведений о
результатах присвоения
объекту КИИ одной из
категорий значимости**

(зарегистрирован
Минюстом России
13 апреля 2018 г., рег. № 50753)



Приказ ФСТЭК России
от 25 декабря 2017 г. № 239

**Об утверждении
требований по
обеспечению
безопасности значимых
объектов КИИ**

(зарегистрирован
Минюстом России
26 марта 2018 г., рег. № 50524)



Приказ ФСТЭК России
от 11 декабря 2017 г. № 229

**Об утверждении
формы акта
проверки**

(зарегистрирован
Минюстом России
28 декабря 2017 г., рег. № 49500)



Приказ ФСТЭК России
от 6 декабря 2017 г. № 227

**Об утверждении
порядка ведения
реестра значимых
объектов КИИ**

(зарегистрирован Минюстом
России 8 февраля 2018 г.,
рег. № 49966)



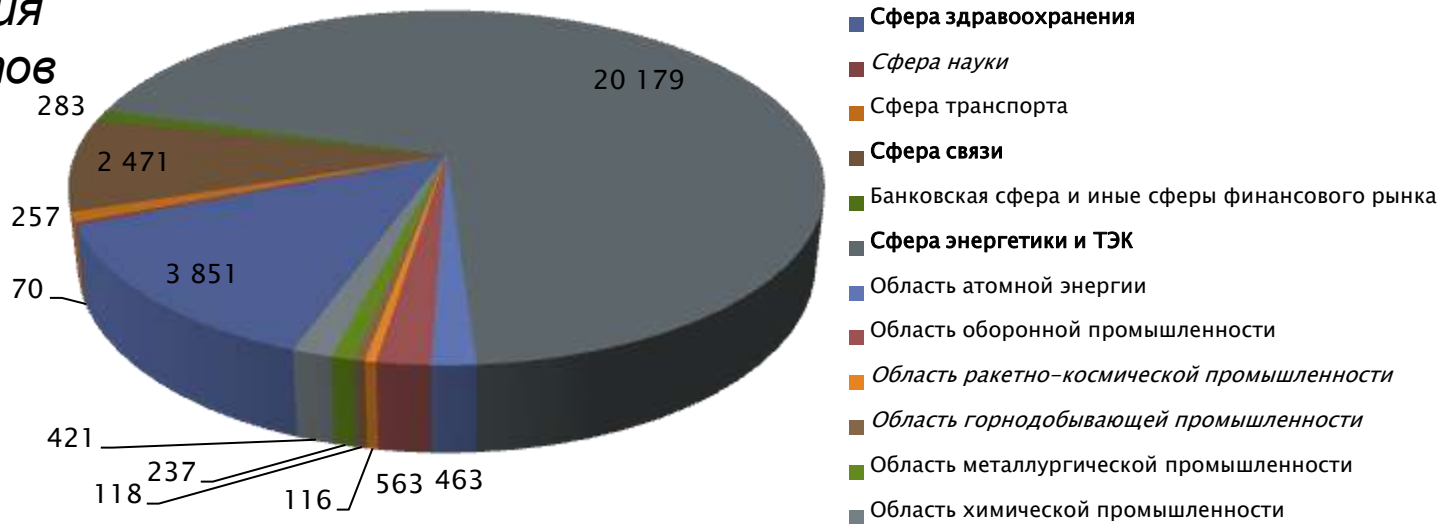
Процедура категорирования объектов КИИ РФ



Текущие результаты категорирования

Более **29 000** объектов КИИ, подлежащих категорированию

Получены сведения
от 1 100 субъектов



Получены сведения
о результатах категорирования
2 000 объектов КИИ

Результаты категорирования
630 объектов КИИ
возвращены на доработку



Проблемные вопросы категорирования объектов КИИ



Определение принадлежности к субъектам КИИ



Определение критических процессов



Определение перечня объектов КИИ, подлежащих категорированию



Определение необходимости согласования перечня объектов КИИ с государственным органом или российским юридическим лицом



Подготовка сведений о результатах категорирования объектов КИИ



Попадает ли организация по действие ФЗ-187 и что включить в перечень категорирования?



Что такое «критический процесс»?











Определение необходимости согласования перечня объектов КИИ с государственным органом или российским юридическим лицом

Наличие в уставных документах субъекта КИИ информации о его **подведомственности**

Подведомственность \neq Функционирование в сфере



Типовые недостатки при подготовке перечней объектов, подлежащих категорированию

- 
-  Вместо наименования объекта указывается место его размещения (или другая информация, в т.ч. наименование субъекта)
 -  Представляется не утвержденный перечень
 -  **ФСТЭК России не утверждает и не согласует перечни**
 -  Перечень представляется не в центральный аппарат ФСТЭК России
 -  Перечень представляется не субъектами КИИ (ОМСУ, ...)
 -  В перечне учтены не все критические процессы, учтены не все типы объектов (АСУ, ИС, ИТКС)
 -  В перечне не учтены объекты, принадлежащие на иных законных основаниях



Типовые недостатки при подготовке сведений о результатах категорирования объекта КИИ



Занижение значений показателей критериев значимости



Представление результатов оценки возможного ущерба не по всем показателям критериев значимости



Отсутствие обоснования неприменимости критериев значимости или полученных значений по результатам оценки возможного ущерба



Применение принятых мер по обеспечению безопасности объекта для обоснования неприменимости показателей критериев значимости



Представление не полных сведений



Подготовка сведений не по форме, определенной приказом ФСТЭК России № 236



Планируемые к разработке в 2019 году нормативные правовые акты в области обеспечения безопасности КИИ



Федеральный закон

«О внесении изменений в КоАП (в части установления ответственности за нарушение требований по обеспечению безопасности объектов КИИ)»



Постановление Правительства РФ

«О внесении изменений в Правила категорирования объектов КИИ и перечень показателей критериев значимости КИИ и их значений, утвержденные постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127»

Приказ ФСТЭК России

«О внесении изменений в форму направления сведений о результатах категорирования объекта КИИ, утвержденную приказом ФСТЭК России от 22 декабря 2017 г. № 236»

Приказ ФСТЭК России

«О внесении изменений в Требования по обеспечению безопасности значимых объектов КИИ, утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239»

Приказ ФСТЭК России

«О внесении изменений в Требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования, утвержденные приказом ФСТЭК России от 21 декабря 2017 г. № 235»




Изменения в Правила категорирования объектов КИИ РФ

Изменения касаются :

- ✓ Категорирование объектов КИИ 1го уровня значимости
- ✓ Категорирование вновь создаваемых объектов КИИ
- ✓ Вопросы создания и функционирования комиссии по категорированию
- ✓ Рассмотрение наихудших сценариев атак на объект КИИ
- ✓ Категорирование связанных объектов КИИ
- ✓ Срок утверждения перечня объектов, подлежащих категорированию, 1 июня 2019 г.
- ✓ Оформление 1 акта категорирования на все объекты КИИ, принадлежащие субъекту КИИ
- ✓ Сведения о категорировании направляются в печатном и электронном виде



Применяемые методические документы



Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры

Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Меры защиты информации в государственных информационных системах



Система методических документов

Методика
категорирования
ОКИИ

Методики оценки показателей



Методика
оценки
показателей
критериев
экономической
значимости
ОКИИ



Методика
оценки
показателей
критериев
социальной
значимости
ОКИИ



Методика
оценки
показателей
критериев
экологической
значимости
ОКИИ

Моделирование угроз безопасности



Типовые
модели угроз
безопасности
информации
в зависимости
от типа
систем



Базовые
модели угроз
безопасности
типичного
ОКИИ в
различных
сферах



*Требования к созданию систем
безопасности значимых объектов
критической инфраструктуры и
обеспечение безопасности объектов
критической информационной
инфраструктуры*



Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования

*Утверждены приказом ФСТЭК России от 21 декабря 2017 г. №235
(зарегистрирован Минюстом России 22 февраля 2018 г., рег. № 50118)*



I Общие положения

II Требования к силам обеспечения безопасности значимых объектов КИИ

III Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ

IV Требования к организационно-распорядительным документам по безопасности значимых объектов

V Требования к функционированию систем безопасности в части организации работ по обеспечению безопасности значимых объектов КИИ



I Общие положения. Система безопасности

С
и
с
т
е
м
а

б
е
з
о
п
а
с
н
о
с
т
и



Правовые меры



Организационные
меры



Технические меры



Другие меры

Создается в целях обеспечения **устойчивого функционирования** значимых объектов критической информационной инфраструктуры **при проведении** в отношении них **компьютерных атак**



ИС₁
ИС₂
...
ИС_n

АСУ ТП₁
АСУ ТП₂
...

АСУ ТП₁

ИТКС₁
ИТКС₂
...
ИТКС_m



I Общие положения. Система безопасности

б
е
з
о
п
а
с
н
о
с
т
и



предотвращение неправомерного доступа к информации, обрабатываемой значимыми объектами



восстановление функционирования значимых объектов



недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимых объектов

ГОССОПКА

непрерывное **взаимодействие с ГосСОПКА**



II Требования к силам обеспечения безопасности



- подразделения субъекта КИИ, ответственные за обеспечение безопасности ЗО КИИ



- подразделения, эксплуатирующие ЗО КИИ



- подразделения, обеспечивающие функционирование (сопровождение, обслуживание, ремонт) ЗО КИИ



- иные подразделения, участвующие в обеспечении безопасности ЗО КИИ



II Требования к силам обеспечения безопасности



III Требования к средствам обеспечения безопасности



встроенные в общесистемное, прикладное программное обеспечение средства защиты информации

межсетевые экраны



средства обнаружения (предотвращения) вторжений



средства антивирусной защиты



средства (системы) контроля (анализа) защищенности



средства управления событиями безопасности



средства защиты каналов передачи данных



программные и программно-аппаратные средства, применяемые для обеспечения безопасности значимых объектов

Прошли оценку соответствия в форме обязательной сертификации, приемки или испытаний

В приоритетном порядке применяются встроенные в ОПО и СПО СЗИ

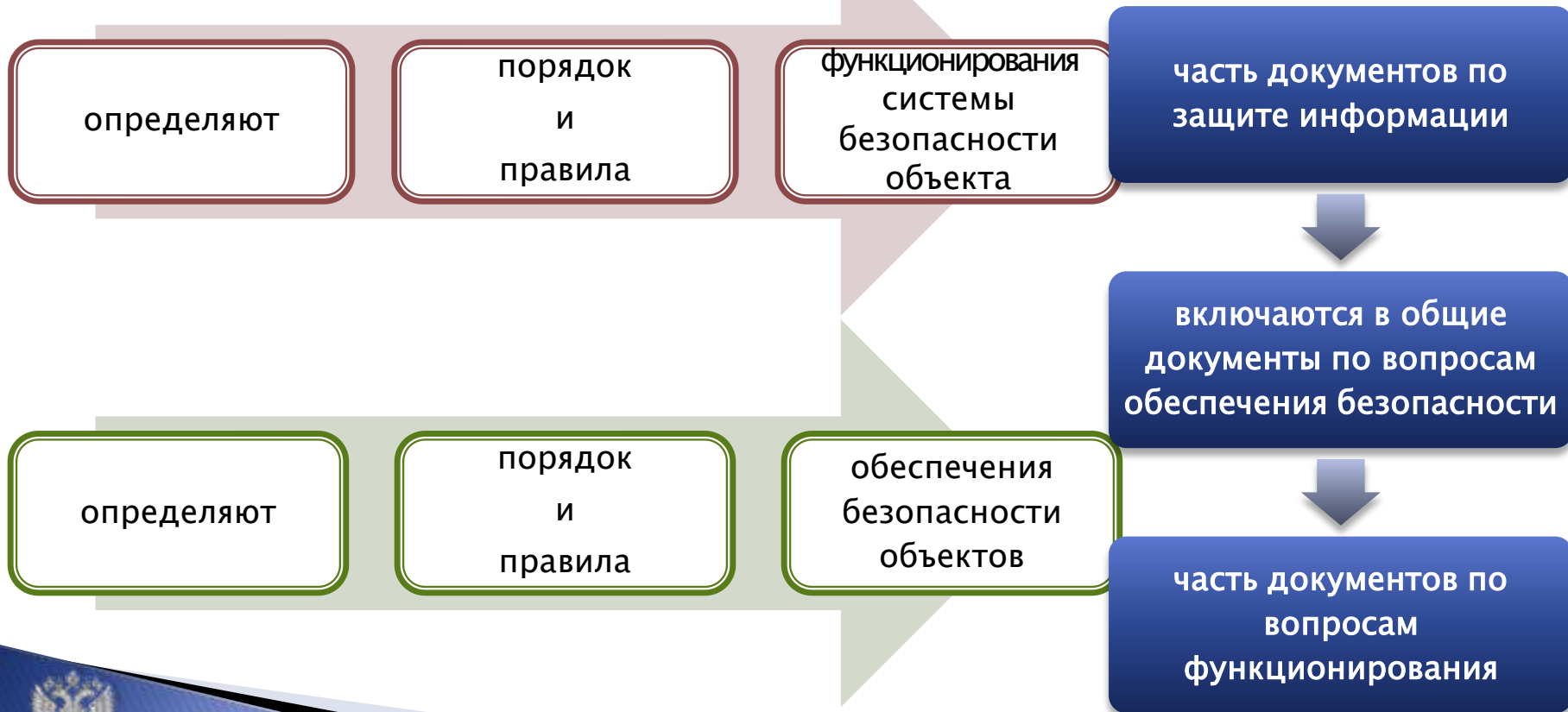
Применяются в соответствии с эксплуатационной документацией

Должна быть обеспечена поддержка СЗИ

Должны быть учтены возможные ограничения со стороны разработчика

Должны обеспечивать реализацию технических мер обеспечения безопасности

IV Требования к организационно-распорядительным документам по безопасности значимых объектов



У Требования к функционированию систем безопасности в части организации работ по обеспечению безопасности значимых объектов



планирование и разработка мероприятий по обеспечению безопасности значимых объектов



реализация (внедрение) мероприятий по обеспечению безопасности значимых объектов



контроль состояния безопасности значимых объектов



совершенствование безопасности значимых объектов



*Требования по обеспечению безопасности значимых
объектов критической информационной
инфраструктуры Российской Федерации*



Создание системы безопасности объектов КИИ и внедрение мер по обеспечению защиты объектов КИИ



**Приказ ФСТЭК России
от 25 декабря 2017 г. № 239**

**«Об утверждении Требований
по обеспечению безопасности
значимых объектов
критической информационной
инфраструктуры
Российской Федерации»**

Подготовлен в соответствии с пунктом 4 части 3 статьи 6 Федерального закона № 187-ФЗ

Общие положения

Требования к обеспечению безопасности в ходе создания, эксплуатации и вывода из эксплуатации значимых объектов

Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов

Приложение. Состав мер по обеспечению безопасности для значимых объектов соответствующей категории



Этапы реализации требований по обеспечению безопасности значимых объектов КИИ

1

- **Формирование требований к обеспечению безопасности значимого объекта**

2

- **Разработка организационных и технических мер по обеспечению безопасности значимого объекта**

3

- **Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и его ввод в эксплуатацию**

4

- **Обеспечение безопасности значимого объекта в ходе его эксплуатации**

5

- **Обеспечение безопасности значимого объекта при выводе его из эксплуатации**



Формы оценки соответствия СЗИ и подтверждения соответствия значимого объекта

Оценка соответствия средств защиты информации

Сертификация

Применяется в случаях,
установленных
законодательством РФ и по
решению субъекта КИИ

Испытания

В иных случаях и проводятся
самостоятельно или с привлечением
организаций-лицензиатов

Приемка

Подтверждение соответствия значимого объекта

Аттестация

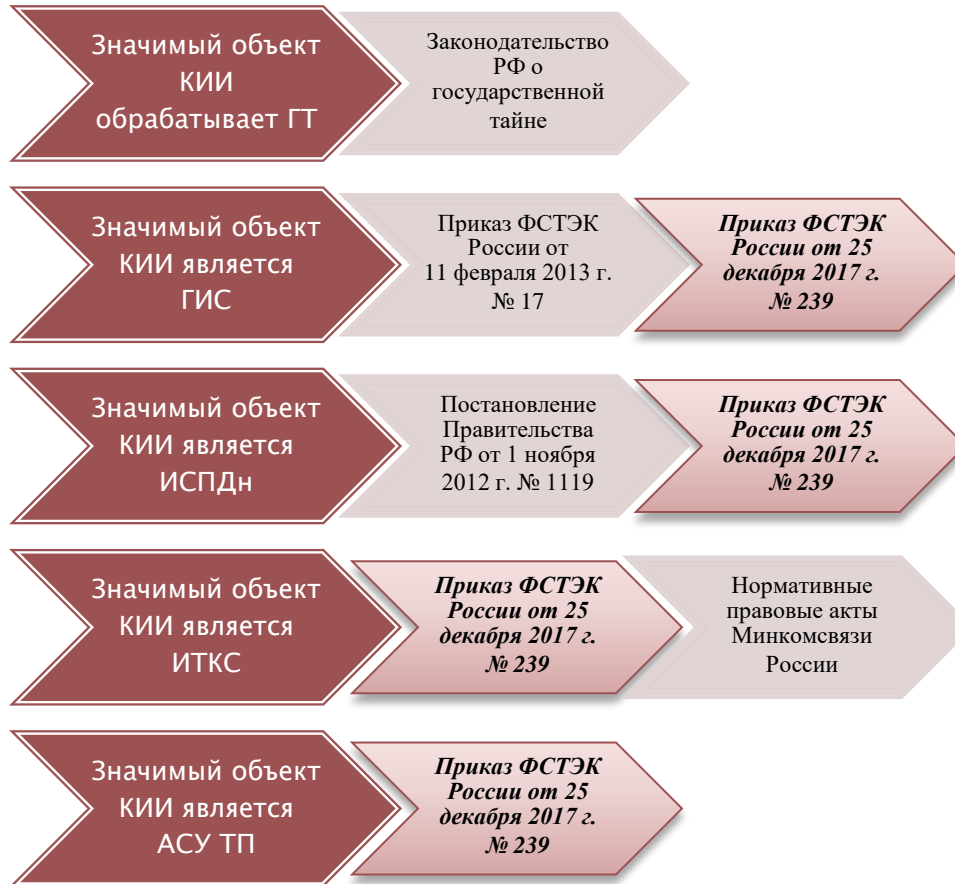
В случаях, если значимый объект – ГИС в
соответствии с законодательством РФ и по
решению субъекта КИИ

Приемочные
испытания

В иных случаях



Особенности реализации требований



СПАСИБО ЗА ВНИМАНИЕ!



ТОРБЕНКО Елена Борисовна
Заместитель начальника управления ФСТЭК России