
техно
2019
infotecs
фест
ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ
12
09
2019
Угрозы, требования и меры КИИ. Правильный подход к решению задач категорирования

Федеральный закон №187-ФЗ «О безопасности КИИ РФ»

ТЕХНО 2019 infotecs фест

Регулирует отношения в области **обеспечения безопасности критической информационной инфраструктуры Российской Федерации** в целях её устойчивого функционирования при проведении в отношении её компьютерных атак.

Ст.15. Федерального закона №187-ФЗ
ФЗ вступил в силу с 1 января 2018 года.

Сферы деятельности

ТЕХНО 2019 infotecs Фест


Здравоохранение


Наука


Транспорт


Связь


Энергетика


Банковская сфера


ТЭК


Атомная энергетика


Оборонная промышленность


Ракетно-космическая промышленность


Горнодобывающая промышленность


Металлургическая промышленность


Химическая промышленность


Обеспечение взаимодействия ИС/ИТКС/АСУ

Что такое Субъекты КИИ?

Государственные органы

Государственные учреждения

Российские юридические лица

Индивидуальные предприниматели

которым на праве собственности, аренды или на ином законном основании принадлежат ИС, ИТКС, АСУ

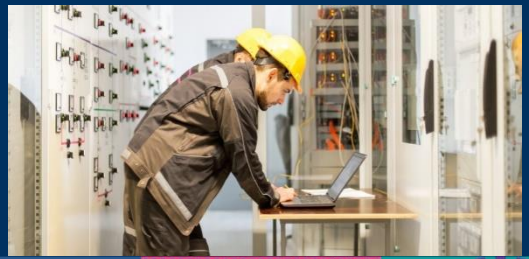
Что такое Объект КИИ?

ТехноИнфотекс Фест 2019

Информационные системы (**ИС**)

Информационно-телекоммуникационные сети (**ИТКС**)

Автоматизированные системы управления (**АСУ**)



С чего начать?

Создаём комиссию по категорированию

- Руководитель субъекта КИИ / уполномоченное им лицо

- Специалисты, участвующие в процессах

- Специалисты по ИБ

- Специалисты по защите государственной тайны

- Работники по ГО и ЧС

Комиссия по категорированию

Комиссия является **постоянно действующей**.

Комиссия по категорированию

Комиссия является **постоянно действующей**.

Может быть создана **отдельная комиссия для филиалов/представительств**.

Комиссия по категорированию

Подлежит **расформированию**, в случаях:

- **прекращение** субъектом КИИ **выполнения функций (полномочий)** или **осуществления видов деятельности** в областях (сферах)

- **ликвидация, реорганизация** субъекта КИИ и (или) изменения его организационно-правовой формы, в результате которых были утрачены признаки субъекта КИИ

Перечень объектов КИИ

1. Выделить **ИС, ИТКС, АСУ**, в которых:

✓ обрабатываемая **информация необходима для обеспечения выполнения критических процессов**

Перечень объектов КИИ

1. Выделить **ИС, ИТКС, АСУ**, в которых:

- ✓ обрабатываемая **информация необходима для обеспечения выполнения критических процессов**
- ✓ осуществляется **управление, контроль или мониторинг критических процессов**

Перечень объектов КИИ

1. Выделить **ИС, ИТКС, АСУ**, в которых:

- ✓ обрабатываемая **информация необходима для обеспечения выполнения критических процессов**
- ✓ осуществляется **управление, контроль или мониторинг критических процессов**
- ✓ существуют **угрозы безопасности информации**

Перечень объектов КИИ

1. Выделить **ИС, ИТКС, АСУ**, в которых:

- ✓ обрабатываемая **информация необходима для обеспечения выполнения критических процессов**
- ✓ осуществляется **управление, контроль или мониторинг критических процессов**
- ✓ существуют **угрозы безопасности информации**
- ✓ существуют **уязвимости**, которые могут привести к возникновению компьютерных инцидентов

Перечень объектов КИИ

1. Выделить **ИС, ИТКС, АСУ**, в которых:

- ✓ обрабатываемая **информация необходима для обеспечения выполнения критических процессов**
- ✓ осуществляется **управление, контроль или мониторинг критических процессов**
- ✓ существуют **угрозы безопасности информации**
- ✓ существуют **уязвимости**, которые могут привести к возникновению компьютерных инцидентов
- ✓ может реализовывать свои **возможности потенциальный нарушитель**

Перечень объектов КИИ

1. Выделить **ИС, ИТКС, АСУ**, в которых:

- ✓ обрабатываемая **информация необходима для обеспечения выполнения критических процессов**
- ✓ осуществляется **управление, контроль или мониторинг критических процессов**
- ✓ существуют **угрозы безопасности информации**
- ✓ существуют **уязвимости**, которые могут привести к возникновению компьютерных инцидентов
- ✓ может реализовывать свои **возможности потенциальный нарушитель**

2. Составить **перечень объектов КИИ**.

Перечень объектов КИИ

Утверждает → **Субъект КИИ**

Согласует → **Ведомство (при наличии подведомственности)**

Перечень объектов КИИ

Перечень объектов КИИ
в течение 10 рабочих дней
после утверждения и согласования направляется
в **ФСТЭК России**

В перечень объектов **включаются объекты КИИ филиалов, представительств** субъекта КИИ.

ТЕХНО 2019 infotecs ФЕСТ

Провести категорирование Объектов КИИ

согласно требованиям

Постановления Правительства РФ

от 8 февраля 2018 г. № 127

«Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»

Категории значимости

Устанавливаются **3 категории значимости**.

- Самая высокая категория - первая,
- самая низкая - третья.

Сроки проведения категорирования

Максимальный срок категорирования **не должен превышать одного года** со дня утверждения субъектом КИИ перечня объектов КИИ (внесения дополнений или изменений).

Процедура категорирования

1. **Оценить масштаб возможных последствий** в случае возникновения **компьютерных инцидентов** на объектах КИИ.

в соответствии с **перечнем показателей критериев значимости**

Критерии значимости:

- Социальная значимость (5 показателей)

Критерии значимости:

- Социальная значимость (5 показателей)
- Политическая значимость (2 показателя)

Критерии значимости:

- Социальная значимость (5 показателей)
- Политическая значимость (2 показателя)
- Экономическая значимость (3 показателя)

Критерии значимости:

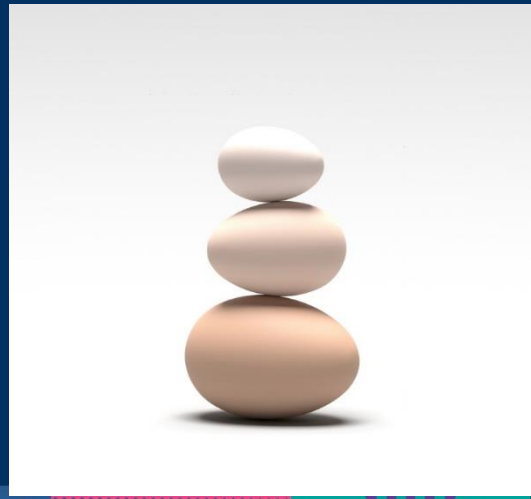
- Социальная значимость (5 показателей)
- Политическая значимость (2 показателя)
- Экономическая значимость (3 показателя)
- Экологическая значимость (1 показатель)

Критерии значимости:

- Социальная значимость (5 показателей)
- Политическая значимость (2 показателя)
- Экономическая значимость (3 показателя)
- Экологическая значимость (1 показатель)
- Значимость для обеспечения обороны страны, безопасности государства и правопорядка (3 показателя)

Процедура категорирования

2. Установить **каждому из объектов КИИ одну из категорий значимости** либо **принять решение об отсутствии** необходимости присвоения им категорий значимости.



Акт категорирования

Решение комиссии по категорированию **оформляется актом**.

Акт категорирования

Решение комиссии по категорированию **оформляется актом**.

Допускается оформление
единого акта для нескольких объектов КИИ,
принадлежащих одному субъекту КИИ.

Акт категорирования

Субъект КИИ обеспечивает **хранение акта до вывода из эксплуатации** значимого объекта КИИ или **до изменения категории значимости**.

Категория значимости может быть изменена в порядке, предусмотренном для категорирования, в случаях, предусмотренных **ч.12 ст.7** Федерального закона **№187**.

Субъект КИИ не реже чем один раз в 5 лет осуществляет **пересмотр** установленной **категории значимости** в соответствии с Правилами.

В случае изменения категории значимости сведения о результатах пересмотра категории значимости направляются в ФСТЭК России.

В какой форме направляются сведения во ФСТЭК России?

Форма направления сведений во ФСТЭК России

ПРИКАЗ ФСТЭК России
от 22 декабря 2017 г. №236
«Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»

https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1590-prikaz-fstek-rossii-ot-22-dekabrya-2017-g-n-236

Срок направления сведений во ФСТЭК России

Субъект КИИ **в течение 10 рабочих дней со дня утверждения акта** направляет в ФСТЭК России сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

Реестр объектов КИИ

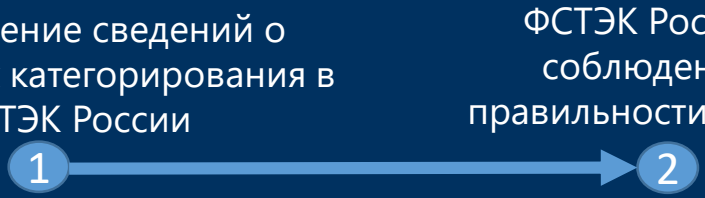
Приказ ФСТЭК России
от 6 декабря 2017 г. №227
«Об утверждении порядка ведения реестра значимых объектов критической информационной инфраструктуры РФ».

Внесение сведений в Реестр значимых объектов КИИ

Направление сведений о результатах категорирования в ФСТЭК России

1

Внесение сведений в Реестр значимых объектов КИИ



Внесение сведений в Реестр значимых объектов КИИ

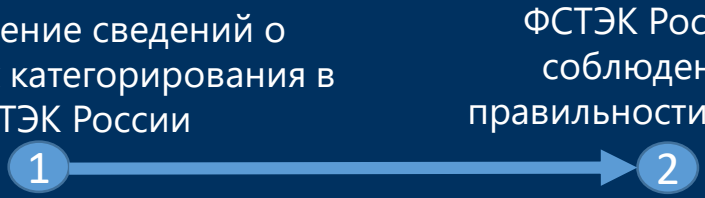
Внесение сведений в Реестр значимых объектов КИИ

Внесение сведений в Реестр значимых объектов КИИ

Направление сведений о результатах категорирования в ФСТЭК России

1

Внесение сведений в Реестр значимых объектов КИИ



Внесение сведений в Реестр значимых объектов КИИ

Внесение сведений в Реестр значимых объектов КИИ

Внесение сведений в Реестр значимых объектов КИИ

Внесение сведений в Реестр значимых объектов КИИ

Внесение сведений в Реестр значимых объектов КИИ

Реестр значимых объектов КИИ

Каждому ЗО КИИ РФ присваивается регистрационный **номер**, состоящий из групп цифр и прописных букв, разделенных косыми чертами, который имеет вид: XXXXXX/X/XX/X

- *порядковый номер;*
- *федеральный округ, на территории которого находится ЗО КИИ;*
- *сфера (область) деятельности, в которой функционирует ЗО КИИ;*
- *тип ЗО КИИ.*

Приказ ФСТЭК России от 6 декабря 2017 г. **№ 227** Об утверждении Порядка ведения реестра ЗО КИИ РФ

Организационные мероприятия

До

ПОСЛЕ

проведения процедуры категорирования и направления сведений в ФСТЭК России

Организационные меры

1. **До проведения процедуры категорирования** и направления сведений в ФСТЭК России:

- **Приказ о создании комиссии по категорированию**
- **Положение о комиссии по категорированию**
- **Перечень объектов КИИ**
- **Акт категорирования объектов КИИ**
- **Форма Приказа ФСТЭК России №236**

Организационные меры

ТЕХНО 2019 infotecs Фест

1. **После проведения процедуры категорирования**

и направления сведений в ФСТЭК России:

- **Приказ о создании структурного подразделения, ответственного за обеспечение безопасности ЗО КИИ**
- **Положение о структурном подразделении**
- **Должностные инструкции**

- **Приказ о назначении отдельных работников, ответственных за обеспечение безопасности ЗО КИИ**
- **Должностной регламент (инструкция)**

Организационные меры

Планирование мероприятий по обеспечению безопасности ЗО КИИ (**План мероприятий**).

План мероприятий содержит:
- наименование мероприятия
- срок выполнения
- наименование подразделения (ФИО работника), ответственного за реализацию мероприятия

План мероприятий разрабатывается **ежегодно**, но при наличии программ по модернизации, оснащению ЗО КИИ, **может быть разработан на более длительный срок**.

Организационные меры

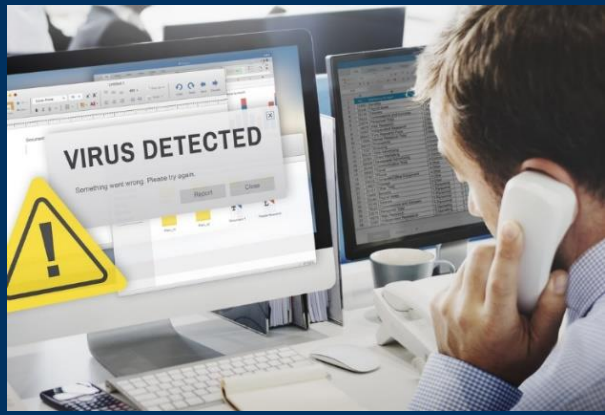
Субъект КИИ **не реже одного раза в год** должен повышать уровень знаний работников по вопросам обеспечения безопасности КИИ.

Работники должны быть ознакомлены с положениями ОРД по безопасности ЗО КИИ

- **Порядок информирования и обучения работников**

Организационно-технические меры

- Порядок реагирования на компьютерные инциденты
- Порядок взаимодействия субъекта КИИ с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ



ГОССОПКА

Обнаружение. Предупреждение. Ликвидация.

Организационные меры

Проводить внутренний контроль организации работ по обеспечению безопасности ЗО КИИ и оценку эффективности принимаемых организационных и технических мер.

- **План проведения внутреннего контроля**
- **Регламент проведения внутреннего контроля**
- **Приказ проведения внутреннего контроля**
- **Акт проведения внутреннего контроля**

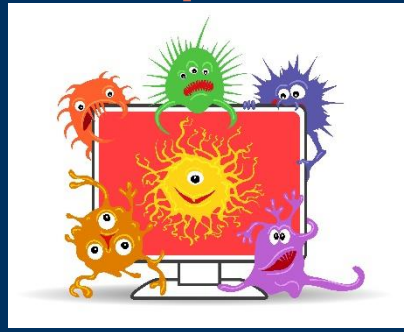
Контроль проводится ежегодно комиссией

Организационно-технические меры

Разработка организационных и технических мер по обеспечению безопасности ЗО КИИ начинается…

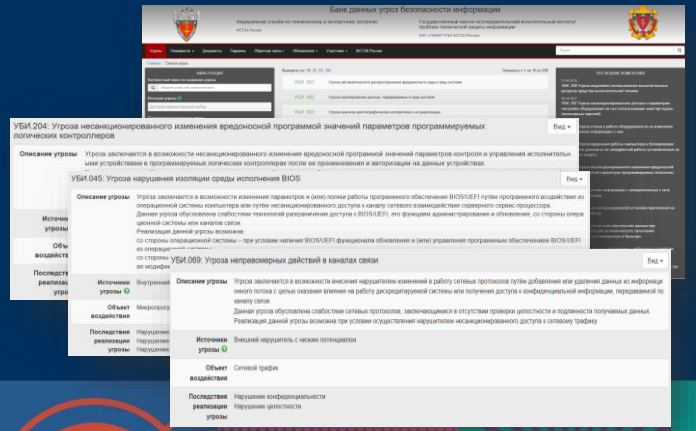
- **Модели угроз и нарушителя**

Модель угроз и нарушителя



В качестве исходных данных для анализа угроз ИБ используется **банк данных угроз безопасности информации (БДУ) ФСТЭК** России и источники, содержащие иные сведения об уязвимостях и угрозах безопасности информации.

МУиН должна содержать краткое описание архитектуры ЗО КИИ, характеристики источников угроз безопасности информации, в том числе модель нарушителя, и описание всех актуальных угроз безопасности информации.



Организационно-технические меры

Разработка организационных и технических мер по обеспечению безопасности ЗО КИИ

- **Техническое задание на создание системы безопасности**
- **Технический проект (техно-рабочий проект)**
- **Рабочая (эксплуатационная) документация**
- **…..**

Приказ ФСТЭК России №239

Приказ ФСТЭК России №235

«Об утверждении требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования».

Организационные требования

по безопасности информации

Приказ ФСТЭК России №239

«Об утверждении требований по обеспечению безопасности значимых объектов КИИ РФ».

Организационно-технические требования

по безопасности информации

Спасибо
за внимание!