infotecs

Перечень объектов КИИ утвержден. Что дальше?

Руководитель спецпроектов, к.т.н.
Валентина Миронова

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

Регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры РФ в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.



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

Срок направления перечня объектов КИИ во ФСТЭК России



Если субъект КИИ является:

- государственным органом и государственным учреждением, то перечень объектов КИИ **необходимо** утвердить перечень объектов КИИ **до 1 сентября 2019 г.**
- российским юридическим лицом и (или) индивидуальным предпринимателем, то **рекомендуется утвердить** перечень объектов КИИ **до 1 сентября 2019 г.**

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

Перечень объектов КИИ

Приложение 1
к информационному сообщению
ФСТЭК России
от 24 августа 2018 г. № 240/25/3752

Рекомендуемая форма перечня объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

УТВЕРЖДАЮ

_____
Должность руководителя субъекта критической информационной инфраструктуры Российской Федерации (далее – субъект) или уполномоченного им лица

_____ _____
Подпись руководителя субъекта или уполномоченного им лица | Фамилия, имя, отчество (при наличии) руководителя субъекта или уполномоченного им лица

«___» _____ 20___ г.
Дата утверждения перечня объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

Перечень объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

№ п/п	Наименование объекта	Тип объекта[1]	Сфера (область) деятельности, в которой функционирует объект [2]	Планируемый срок категорирования объекта	Должность, фамилия, имя, отчество (при наличии) представителя, его телефон, адрес электронной почты (при наличии)[3]
1.					
2.					
…					
n.					

[1] Указывается один из следующих типов объекта: информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть.

[2] Указывается сфера (область) в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации инфраструктуры Российской Федерации».

[3] Указываются должность, фамилия, имя, отчество (при наличии) должностного лица, с которым можно осуществить взаимодействие по вопросам категорирования объекта, его телефон, адрес электронной почты (при наличии). Для нескольких объектов может быть определено одно должностное лицо.

Что дальше?







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



3 категории значимости

Самая высокая категория - **первая**,

самая низкая - **третья**

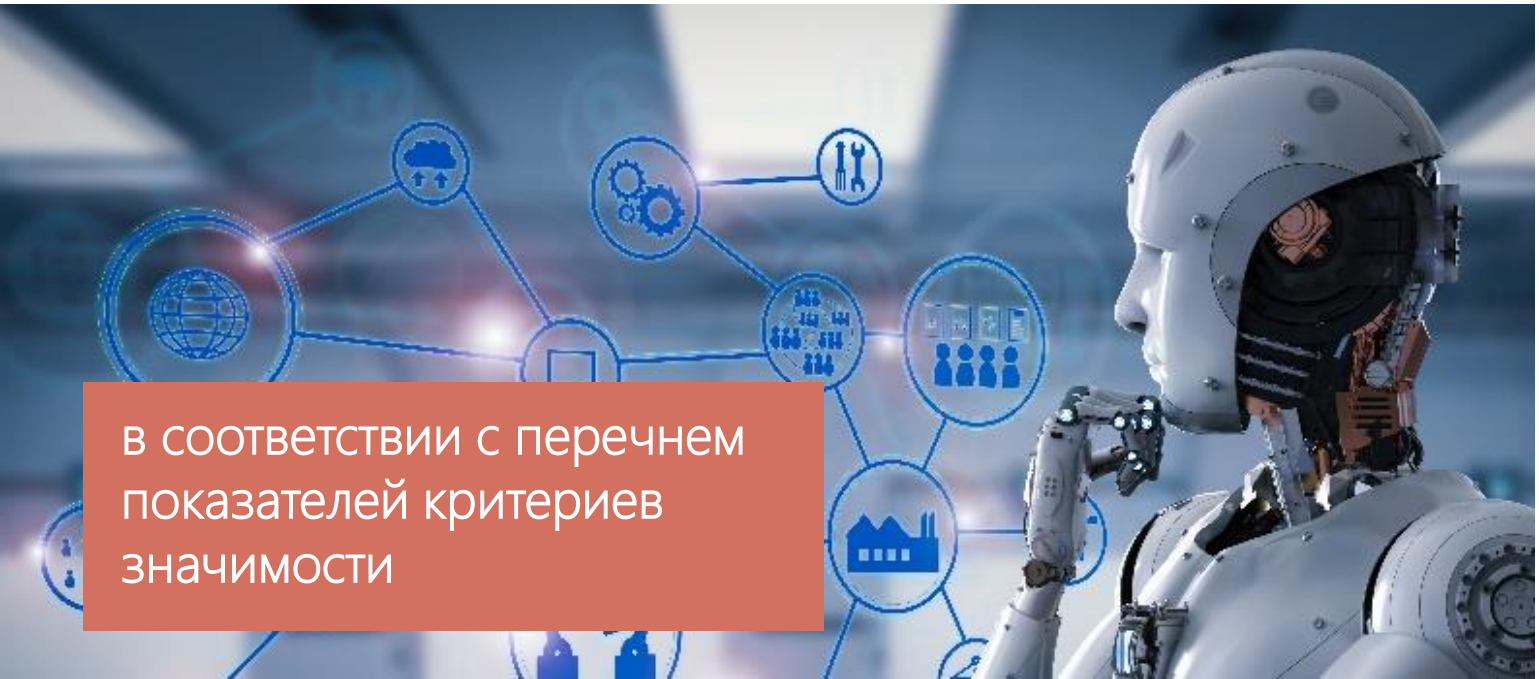
Сроки проведения категорирования



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

Процедура категорирования

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



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)

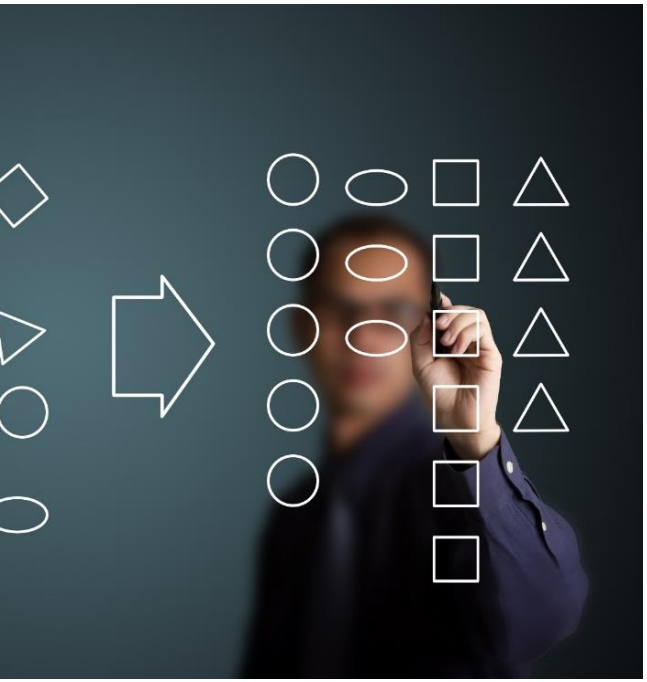








Процедура категорирования



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**.

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** ФЗ**№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 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



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

Следующий этап…

Построение системы безопасности….



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

Особенности реализации требований



Для обеспечения безопасности ЗО, которые являются:

- **ИСПДн** - учесть требования
  ПП РФ N 1119
  от 1 ноября 2012 г.

- **ГИС** - учесть требования
  Приказ N 17 ФСТЭК России
  от 11 февраля 2013 г.

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

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

Разработка организационных и технических мер по обеспечению безопасности ЗО КИИ



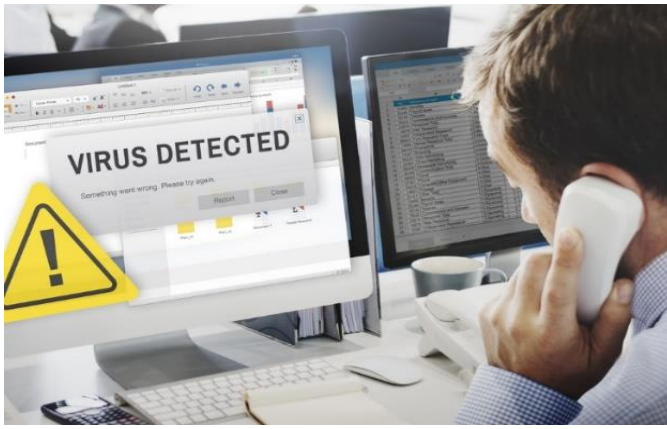
- **Модель угроз и нарушителя**
- **Техническое задание на создание системы безопасности**
- **Технический проект (техно-рабочий проект)**
- **Рабочая (эксплуатационная) документация**
- **…..**



Приказ ФСТЭК России №239

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

infotecs

Спасибо
за внимание!