Обзор практики категорирования объектов критической информационной инфраструктуры Российской Федерации

Чернов Николай Иванович
Начальник 1 отдела
Телефон: (863) 200-75-25

ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Федеральный закон от 26 июля 2017 г. № 187-ФЗ
«О безопасности критической информационной инфраструктуры Российской Федерации»

вступил в силу 1 января 2018 г.

Сфера здравоохранения

Банковская сфера и иные сферы финансового рынка

Сфера горнодобывающей промышленности

Сфера науки

Сфера энергетики и топливно-энергетического комплекса

Сфера металлургической промышленности

Сфера транспорта

Сфера атомной энергии

Сфера химической промышленности

Сфера связи

Сфера ракетно-космической промышленности

Сфера оборонной промышленности

Первоочередные меры по обеспечению безопасности критической информационной инфраструктуры

Федеральный закон От 26 июля 2017 г. № 187

«О безопасности критической информационной инфраструктуры Российской Федерации»

Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127

Приказ ФСТЭК России от 21 декабря 2017 г. № 235

Приказ ФСТЭК России от 22 декабря 2017 г. № 236

Приказ ФСТЭК России от 25 декабря 2017 г. № 239

Приказ ФСТЭК России от 6 декабря 2017 г. № 227

Категорирование объектов КИИ

Создание систем безопасности значимых объектов

Реализация требований по обеспечению безопасности значимых объектов

Обеспечение взаимодействия с ГосСОПКА

Наделение ФСТЭК России полномочиями в области обеспечения безопасности критической информационной инфраструктуры

Федеральный закон от 26 июля 2017 г. № 187

«О безопасности критической информационной инфраструктуры Российской Федерации»

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

ФСТЭК России – федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

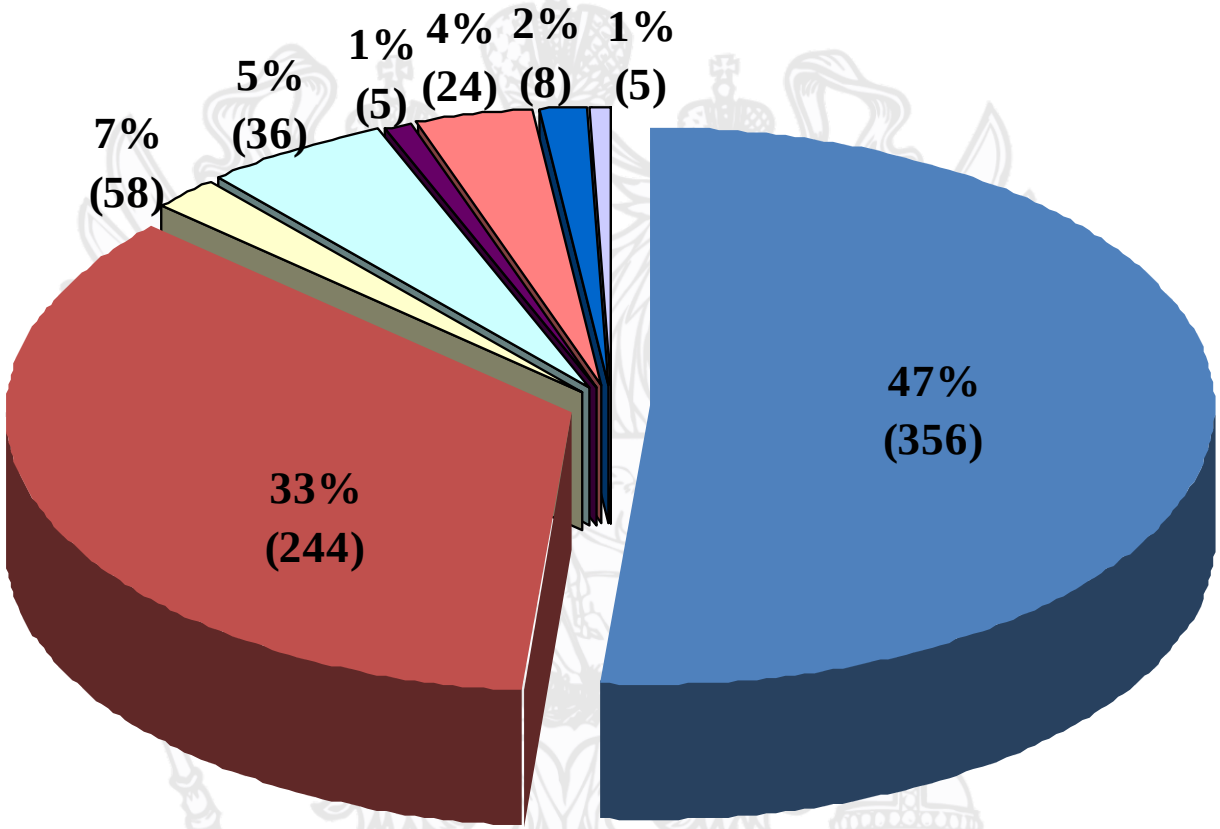
Указ Президента Российской Федерации от 22 декабря 2017 г. № 620

О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

ФСБ России – федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Перечень объектов, подлежащих категорированию

На сегодняшний день более 700 объектов



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»**

Подготовлено в соответствии с пунктом 1 части 2 статьи 6 Федерального закона № 187-ФЗ

Утверждает:

Правила категорирования объектов КИИ РФ

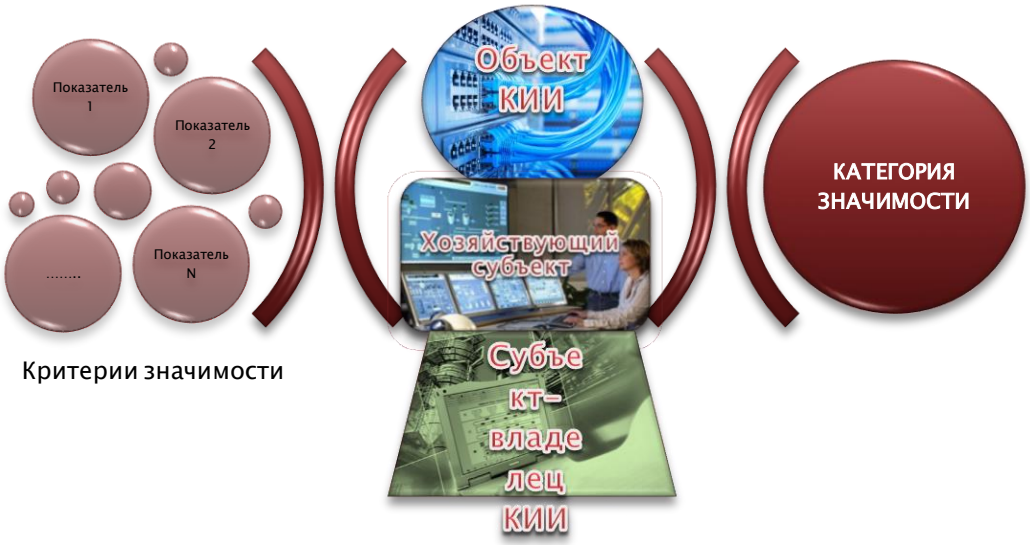
Перечень показателей критериев значимости объектов КИИ РФ и их значения

К обсуждению привлечены представители более 40 организаций

Согласовано с 12 ФОИВ, ЦБ РФ, ГК «Росатом», ГК «Роскосмос»

Правила категорирования объектов КИИ РФ

п. 9 Правил категорирования объектов КИИ РФ: категорирование осуществляется субъектом-владельцем объекта КИИ на основании исходных данных, предоставляемых субъектом-владельцем оборудования



Правила категорирования объектов КИИ РФ

Категорирование – это установление соответствия

<u>КАЖДОГО</u> объекта КИИ

критериям значимости и их показателям

осуществляется <u>субъектами</u> КИИ в отношении <u>принадлежащих</u> им на праве собственности, аренды или ***ином законном основании объектов КИИ***

Порядок категорирования объектов критической информационной инфраструктуры

Пересмотр категории значимости осуществляется не реже, чем раз в 5 лет

Формирование комиссии по категорированию

Подготовка перечня объектов КИИ, подлежащих категорированию

5 дней

ФСТЭК России

(центральный аппарат)

Категорирование объектов КИИ

Исходные данные для категорирования

не более 1 года

Формирование Акта категорирования объекта КИИ

10 дней

Направление сведений о результатах категорирования в ФСТЭК России

Состав комиссии по категорированию объектов критической информационной инфраструктуры

Решением руководителя субъекта КИИ ***создается единственная комиссия для каждого субъекта***

руководитель субъекта КИИ или уполномоченное им лицо

работники субъекта КИИ, являющиеся специалистами в области выполняемых функций, осуществляемых видов деятельности, в области ИТ, по эксплуатации технологического оборудования

работники субъекта КИИ, на которых возложены функции обеспечения безопасности объектов КИИ

работники подразделения по защите государственной тайны субъекта КИИ

работники структурного подразделения по ГО и ЧС или работники, уполномоченные на решение задач в этой области

В состав <u>могут</u> включаться представители гос. органов и российских юридических лиц, выполняющих функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, <u>по согласованию с ними</u> (не ФСТЭК России)

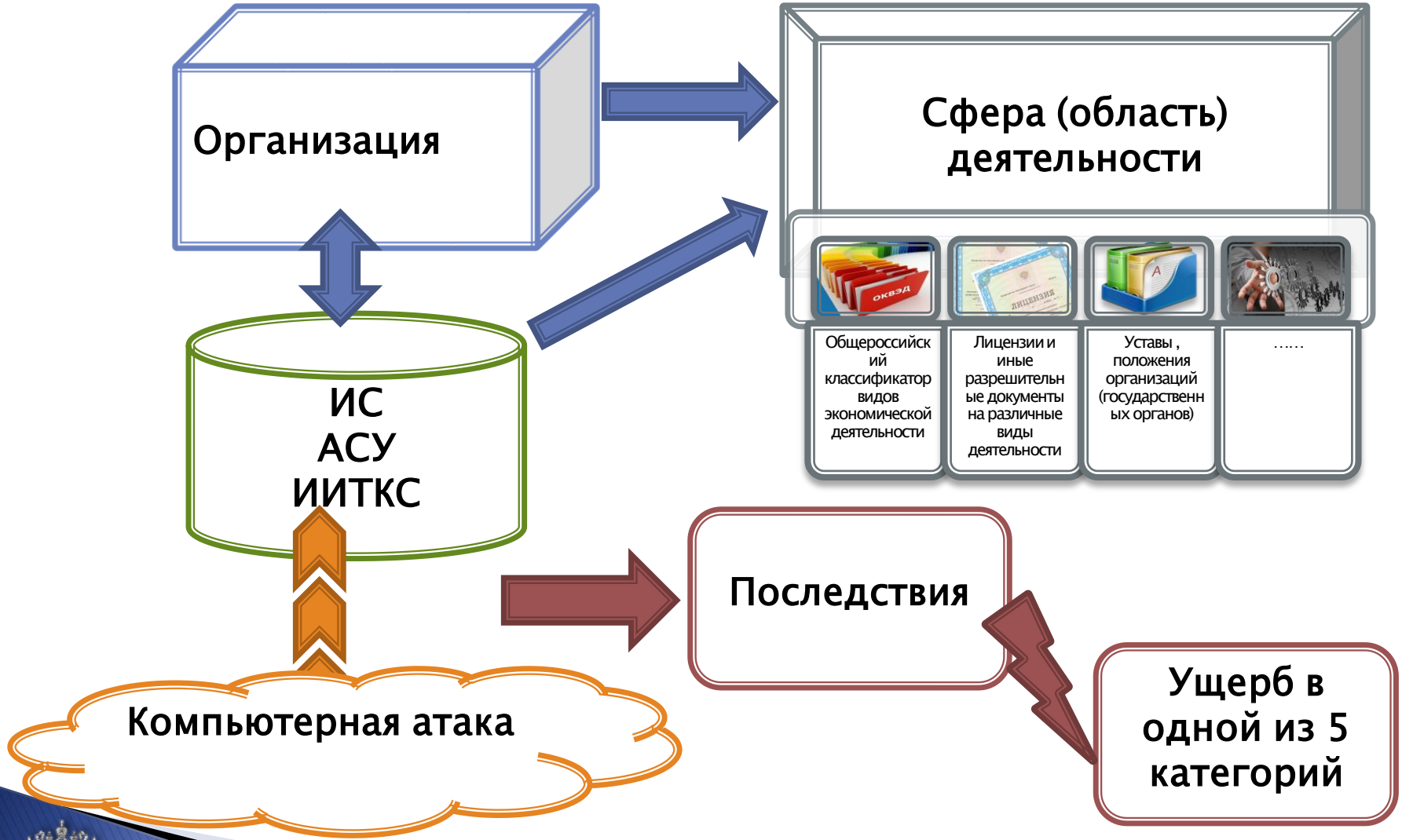
Мероприятия, проводимые комиссией по категорированию объектов критической информационной инфраструктуры

1. определяет процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта КИИ
2. выявляет наличие критических процессов у субъекта КИИ
3. выявляет объекты КИИ, которые обрабатывают информацию, необходимую для выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов
4. готовит предложения для включения в перечень объектов
5. рассматривает возможные действия нарушителей в отношении объектов КИИ, а также иные источники УБИ
6. анализирует УБИ и уязвимости, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ
7. оценивает масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ
8. устанавливает каждому из объектов КИИ одну из категорий значимости либо принимает решение об отсутствии необходимости присвоения им категорий значимости

Исходные данные для категорирования объектов критической информационной инфраструктуры

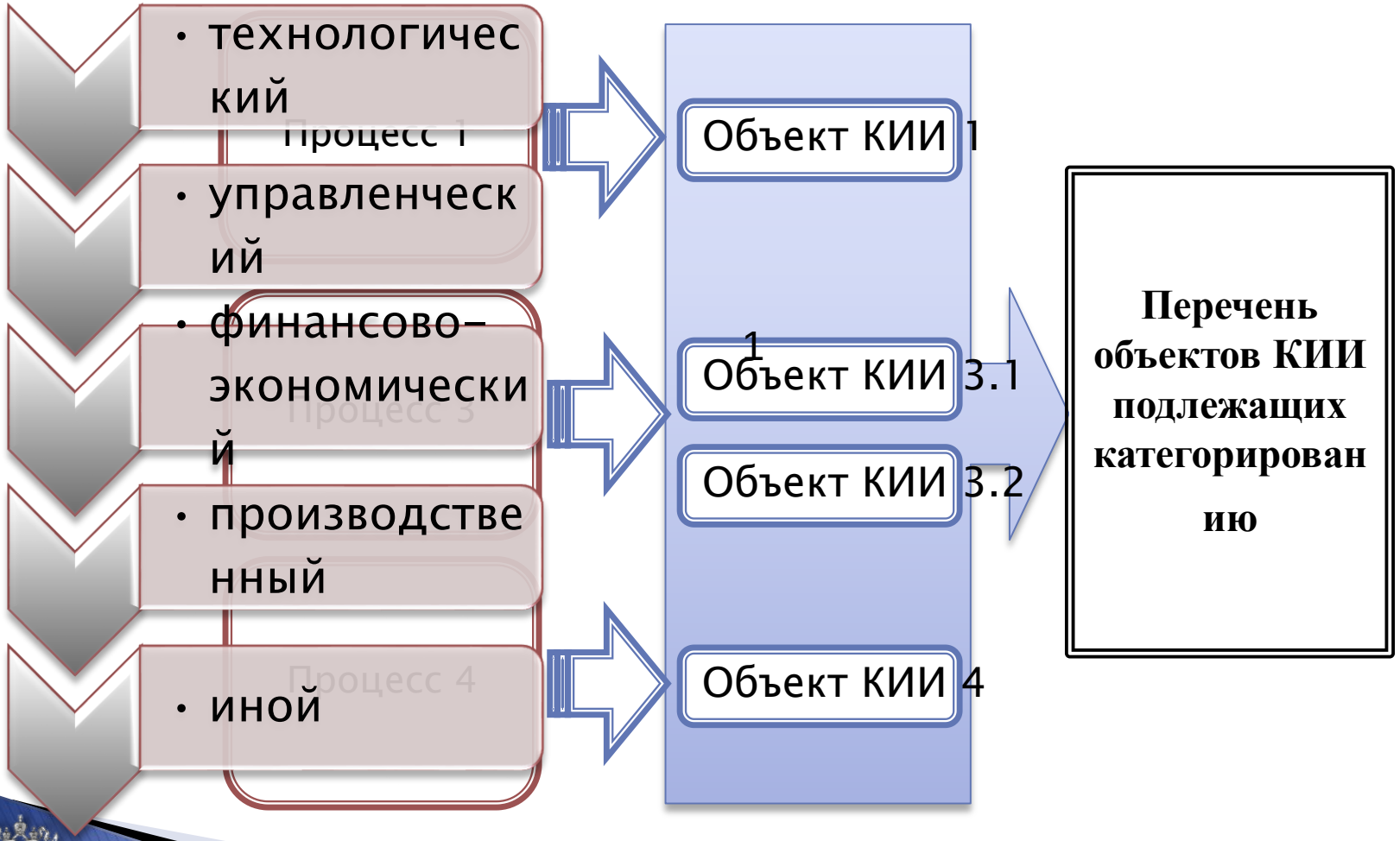
- сведения об объекте КИИ
- процессы в рамках выполнения функций субъекта КИИ
- сервисы, предоставляемые объектами КИИ
- состав информации, обрабатываемой объектами КИИ
- декларация промышленной безопасности, декларация безопасности, паспорт объекта, на которых функционирует объект КИИ
- сведения о взаимодействии объекта КИИ с другими объектами КИИ
- угрозы безопасности информации, а также данные о компьютерных инцидентах, произошедших ранее на объектах КИИ данного типа

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



Правила категорирования объектов КИИ РФ

определение объектов КИИ, связанных с критическими процессами



Что такое «принадлежащих на … ином законном основании»?

Статья 209 Гражданского кодекса РФ «Содержание права собственности»

Основание	**это документ, в котором определено, что пользователь получил от владельца объекта право на его использование в течении определенного периода на условиях, установленных собственником**
Пример	**договор пользования, договор на право хозяйственного ведения, договор на право оперативного управления и т.п.**

Какова степень детализации объектов КИИ?

Детализация	На основании эксплуатационной и технической документации объект КИИ
	С учетом обеспечиваемых критических процессов
Объединение в один объект	Если объекты взаимосвязаны
	Если обеспечивают хотя бы один общий критический процесс
Определение масштаба последствий	Будет осуществляться как от нарушения функционирования единого (объединенного) объекта, а не отдельных его узлов

Правила категорирования объектов КИИ РФ

Утверждается субъектом КИИ

Перечень объектов КИИ подлежащих категорированию

Направляется в центральный аппарат ФСТЭК России
Срок: 5 дней

Обязательное согласование только для организаций, подведомственных (п. 15 Порядка категорирования)

Рекомендация: форма Перечня в информационном сообщении

Рекомендация: указывать планируемые сроки категорирования объектов КИИ

Рекомендация: прилагать электронный вид Перечня

Рекомендуемая форма перечня

Информационное сообщение 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.

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 (водоканалы, 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

Порядок категорирования объектов критической информационной инфраструктуры

Пересмотр категории значимости осуществляется не реже, чем раз в 5 лет

Формирование комиссии по категорированию

Подготовка перечня объектов КИИ, подлежащих категорированию

5 дней

ФСТЭК России

(центральный аппарат)

Категорирование объектов КИИ

Исходные данные для категорирования

не более 1 года

Формирование Акта категорирования объекта КИИ

10 дней

Направление сведений о результатах категорирования в ФСТЭК России

Перечень показателей критериев значимости объектов КИИ РФ и их значения

I социальная значимо

1.1 | 1.2 | 1.3 | 1.4 | 1.5

II политическая знач

2.1 | 2.2

III экономическая

3.1 | 3.2 | 3.3

IV экологическая зна

4.1

V значимость для обеспечения обороны страны, безопасности а и правопорядка

5.1 | 5.2 | 5.3

2.	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения, гидротехнических сооружений, оцениваемые:			
	а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения;	вся территория одного муниципального образования или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта Российской Федерации или территории города федерального значения	выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения
	б) по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек)	более или равно 50, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000

Оценка производится по каждому из значений!

Категория присваивается по наивысшему значению

Правила категорирования объектов КИИ РФ

На основании оценки масштаба возможных последствий
осуществляется присвоение одной из категорий значимости путем
установления соответствия каждого объекта КИИ критериям значимости и их показателям

ПЕРЕЧЕНЬ

показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значения

Показатель	Значение показателя		
	III категория	II категория	I категория
I. Социальная значимость			
1. Причинение ущерба жизни и здоровью людей (человек)	более или равно 1, но менее или равно 50	более 50, но менее или равно 500	более 500
2. Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения, гидротехнических сооружений, оцениваемые:			
а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения;	вся территория одного муниципального образования или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта Российской Федерации или территории города федерального значения	выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения

Категория значимости объекта КИИ

или

Отсутствие необходимости присвоения категории

Порядок категорирования объектов критической информационной инфраструктуры

Пересмотр категории значимости осуществляется не реже, чем раз в 5 лет

Формирование комиссии по категорированию

Подготовка перечня объектов КИИ, подлежащих категорированию

5 дней

ФСТЭК России

(центральный аппарат)

Категорирование объектов КИИ

Исходные данные для категорирования

не более 1 года

Формирование Акта категорирования объекта КИИ

10 дней

Направление сведений о результатах категорирования в ФСТЭК России

Результат категорирования объектов критической информационной инфраструктуры

Утверждаю
руководитель субъекта КИИ

Акт категорирования субъекта КИИ

…

Член комиссии № 1	**подпись**
Член комиссии № 2	**подпись**
Член комиссии № 3	**подпись**
…	
Член комиссии № n	**подпись**

Форма Акта категорирования определяется субъектом КИИ

Акт НЕ ПРЕДСТАВЛЯЕТСЯ в ФСТЭК России

Сведения об объекте КИИ

Результаты анализа угроз БИ объекта КИИ

Реализованные меры по обеспечению безопасности объекте КИИ

I II III

Сведения о присвоенной объекту КИИ категории значимости

Сведения о необходимых мерах по обеспечению безопасности объекта КИИ

Направление сведений о результатах категорирования в ФСТЭК России

Пункт 17
Правил категорирования

ФСТЭК России

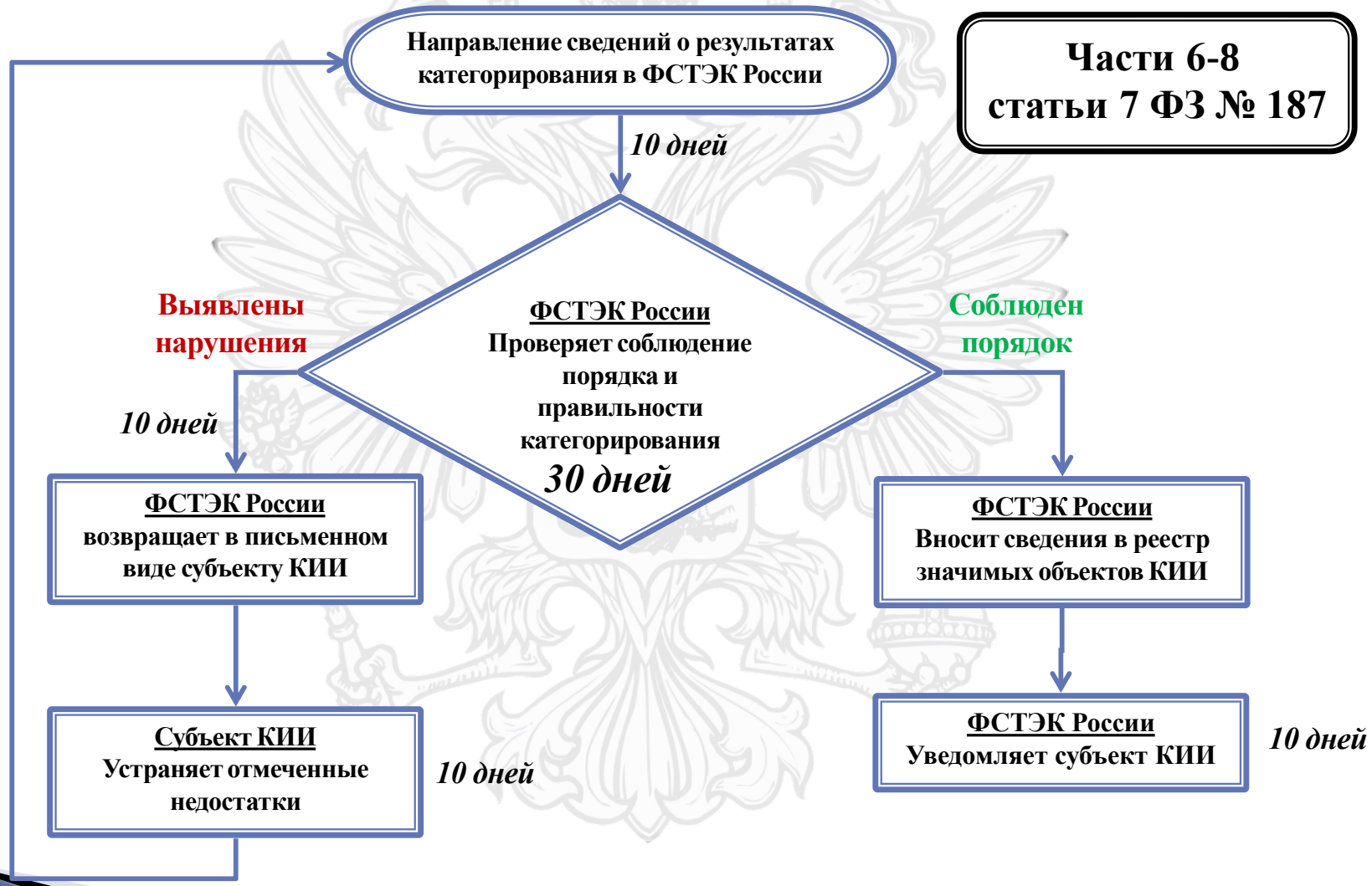
ПРИКАЗ
от 22 декабря 2017 г.
№ 236

Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры Российской Федерации одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

Рекомендуется прикладывать СВЕДЕНИЯ В ЭЛЕКТРОННОМ ВИДЕ

- **сведения об объекте КИИ**
- **сведения о субъекте КИИ**
- **сведения о взаимодействии объекта КИИ и сетей электросвязи**
- **сведения о лице, эксплуатирующем объект КИИ**
- **сведения о программных и программно-аппаратных средствах, используемых на КИИ**
- **сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта КИИ**
- **возможные последствия в случае возникновения компьютерных инцидентов на объекте КИИ**
- **категория значимости, которая присвоена объекту КИИ, а также сведения о результатах оценки показателей критериев значимости**
- **организационные и технические меры, применяемые для обеспечения безопасности объекта КИИ**

Проверка ФСТЭК России результатов категорирования



Части 6-8 статьи 7 ФЗ № 187

МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ ФСТЭК РОССИИ ДЛЯ МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

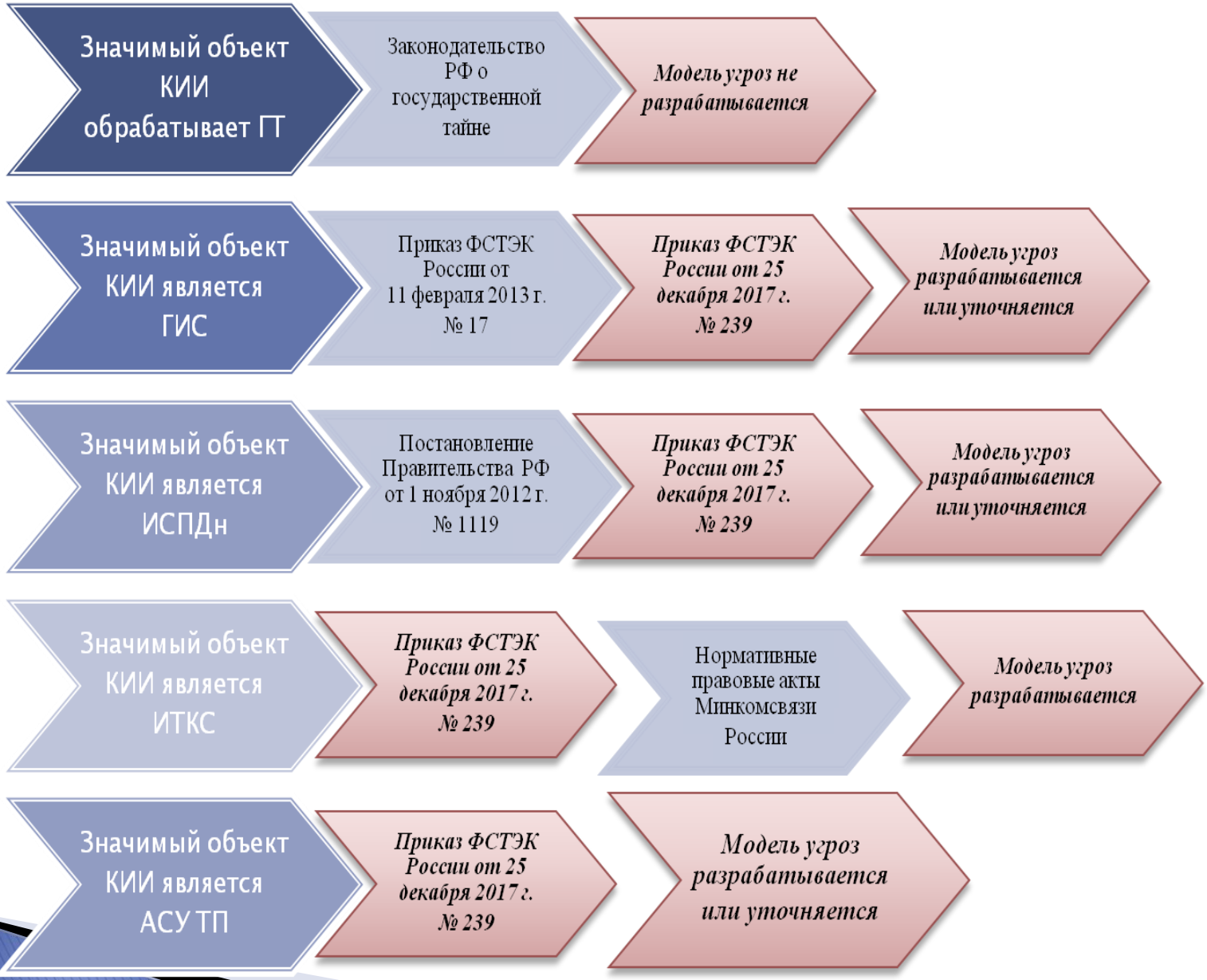
Модели угроз безопасности информации значимых объектов, являющихся информационными системами, информицонно-коммукационными сетями

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена ФСТЭК России 14 февраля 2008 г.)
- Методика определения актуальных угроз безопасности персональных данны при их обработке в информационных системах персональных данны (утверждена ФСТЭ России 14 февраля 2008 г.
- Методика определения угроз безопасности информации в информационных системах (проект)

Модели угроз безопасности информации значимых объектов, являющихся автоматизированными системами управления

- Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России 18 мая 2007 г.
- Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России 18 мая 2007 г.

Особенности моделирования угроз безопасности информации



Система нормативных правовых актов в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

Федеральный закон от 26 июля 2017 г. № 187-ФЗ
«О безопасности критической информационной инфраструктуры Российской Федерации»

Нормативные правовые акты Президента Российской Федерации

Указ Президента РФ 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 РФ «О внесении изменений в Указ Президента РФ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации компьютерных атак»

Указ Президента РФ от 2 марта 2018 г. № 98 «О внесении изменений в Перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента РФ от 30 ноября 1995 г. № 1203»

Нормативные правовые акты Правительства Российской Федерации

Постановление Правительства РФ 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 РФ от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры»

Проект постановления Правительства РФ «Об утверждении порядка подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов КИИ»

Нормативные правовые акты федеральных органов исполнительной власти

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)

Приказ ФСБ России «Об утверждении Положения о Национальном координационном центре по компьютерным инцидентам» от 24 июля 2018 г. №366

Приказ ФСБ России «Об утверждении перечня информации, представляемой в ГосСОПКА и порядка ее представления» от 24 июля 2018 г. №367

Приказ ФСБ России «Об утверждении порядка информирования ФСБ России о компьютерных инцидентах и реагирования на них»

Приказ ФСБ России «Об утверждении порядка, технических условий, установки и эксплуатации средств обнаружения, предупреждения и ликвидации компьютерных атак»

Приказ ФСБ России «Об утверждении порядка об обмене информации о компьютерных инцидентах между субъектами КИИ» от 24 июля 2018 г. № 368

Приказ Минкомсвязи России «Об утверждении порядка, технических условий, установки и эксплуатации средств обнаружения, предупреждения и ликвидации компьютерных атак на сетях связи»

Приказ ФСБ России «Об утверждении требований к средствам обнаружения, предупреждения и ликвидации компьютерных атак»

- готовит ФСТЭК России
- готовит ФСБ России
- готовит Минкомсвязи России

Спасибо за внимание!

Вопросы?

Обзор практики категорирования объектов критической информационной инфраструктуры Российской Федерации

Чернов Николай Иванович
Начальник 1 отдела
Телефон: (863) 200-75-25