

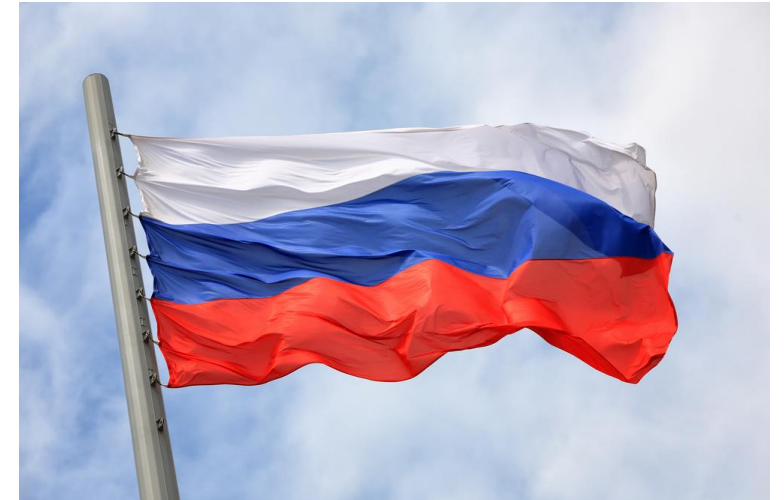
The background of the slide is a photograph of a businessman in a dark suit and blue tie, holding a large, metallic, 3D-rendered gear. The gear is semi-transparent, revealing a complex internal mechanism of smaller gears and shafts. The overall color palette is cool, with blues and greys, and a soft, ethereal glow around the gear.

О категорировании объектов КИИ

Руководитель спецпроектов, к.т.н.
Миронова Валентина Григорьевна

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

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. Федеральный закон №187-ФЗ вступает в силу с **1 января 2018 года.**

Сферы деятельности



Здравоохранение



Наука



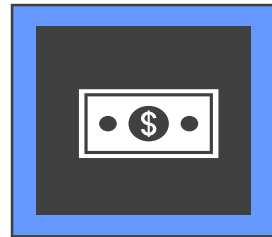
Транспорт



Связь



Энергетика



Банковская сфера



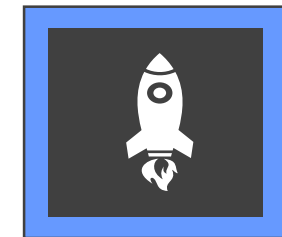
ТЭК



Атомная энергетика



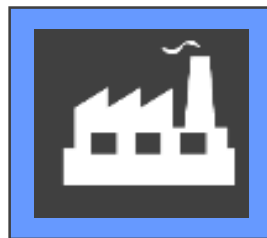
Оборонная промышленность



Ракетно-космическая промышленность



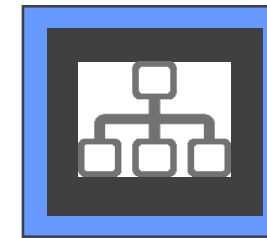
Горнодобывающая промышленность



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?

Информационные системы **(ИС)**



Информационно-телекоммуникационные сети **(ИТКС)**

Автоматизированные системы управления **(АСУ)**



С чего начать?

- Как определить, являетесь ли вы Субъектом КИИ
- И если ДА, то как выделить Объекты КИИ



Как понять, организация – Субъект КИИ или нет?

1. Определить **вид деятельности** предприятия.



- Учредительные документы организаций (уставы, положения организаций и т.д.).
- Общероссийский классификатор видов экономической деятельности (ОКВЭД), (актуальный список - в выписке ЕГРЮЛ предприятия).
- Лицензии и иные разрешительные документы на различные виды деятельности.



Как выделить Объекты КИИ?

1. Провести **инвентаризацию** следующих ресурсов:

- **Информационных** (базы данных, файлы данных и т.д. с указанием **перечня обрабатываемой информации**);
- **Программных** (системное и прикладное ПО и т.д.);
- **Технических** (компьютеры, сервера, коммутационное оборудование, носители данных и т.д.).



Как выделить Объекты КИИ?



2. Определить **цель** обработки информации.

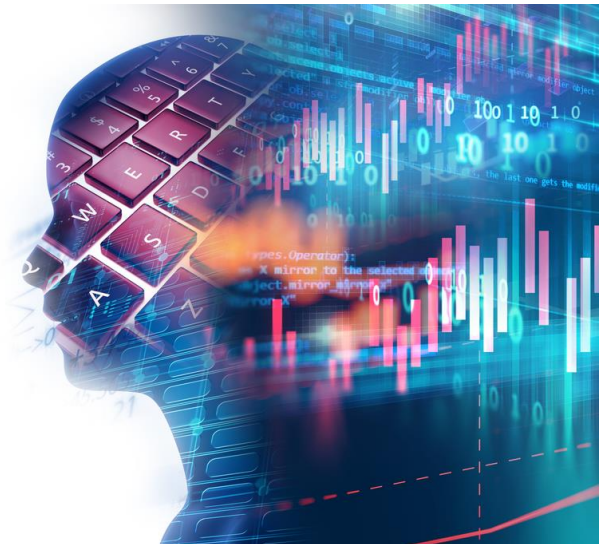
3. Выделить **управленческие, технологические, производственные, финансово-экономические** и (или) иные **процессы** в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ.

4. Выделить **ИС, ИТКС, АСУ**, исходя из цели обработки информации.

Как выделить Объекты КИИ?

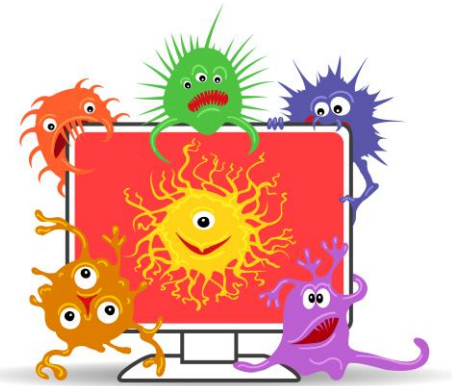
5. Выделить **перечень критических процессов*** предприятия.

***Критические процессы** – это процессы, нарушение и(или) прекращение которых может привести к **негативным социальным, политическим, экономическим, экологическим последствиям, а также последствиям для обеспечения обороны страны, безопасности государства и правопорядка**

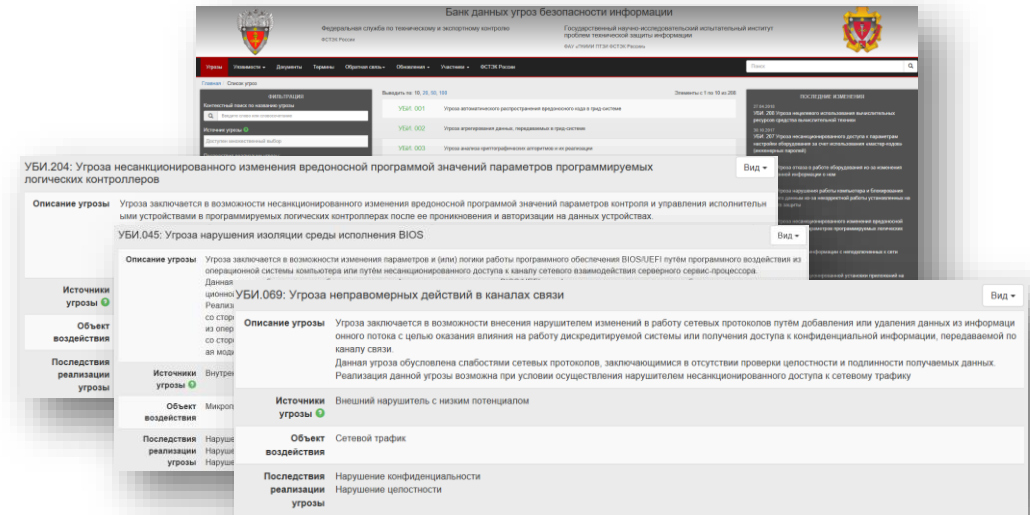


Как выявить критические процессы?

- Провести **анализ угроз безопасности** информации и **уязвимостей**, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ
- Рассмотреть возможные **действия нарушителей** в отношении объектов КИИ, а также **иные источники угроз** безопасности информации



Разработать **модель угроз и нарушителя** безопасности информации



Перечень объектов КИИ

6. 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**

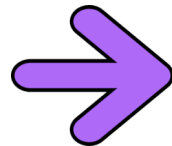


7. Составить **перечень объектов КИИ**.

Перечень объектов КИИ

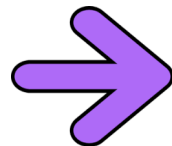


Утверждает



Субъект КИИ

Согласует



Ведомство
(при наличии
подведомственности)

СОГЛАСОВАНО



Перечень объектов КИИ **в течение 5 рабочих дней** после утверждения и согласования направляется в **ФСТЭК России**

Перечень объектов КИИ

Примерная форма

ПЕРЕЧЕНЬ объектов критической информационной инфраструктуры

№ п/п	Наименование организации	Сфера деятельности	Наименование объекта КИИ	Планируемый срок категорирования	Реквизиты субъекта КИИ	Примечание
1	2	3	4	5	6	7
1.	АО «Металлургический комбинат «Руда»	Металлургическая промышленность	<u>Информационные системы:</u> 1. Корпоративные сервисы и информационные системы семейства 1С (...). <u>АСУ ТП:</u> 2. Системы автоматизации производством ... на базе программного обеспечения ... 3. ...	До апреля 2019 г.	Юридический адрес. Электронная почта (при наличии). Должность, Ф.И.О. руководителя организации (ответственного за ОБ КИИ). Телефон, факс (при наличии)	

Наименование должности
руководителя субъекта КИИ или
уполномоченного им лица

«___» _____ 20___ г.

(подпись)

М.П.
(при наличии)

(инициалы, фамилия)

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»



Сроки проведения категорирования



Максимальный срок категорирования **не должен превышать одного года** со дня утверждения субъектом КИИ перечня объектов КИИ

Создаем 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



Проект приказа о создании комиссии

ПРИКАЗ

О назначении комиссии по категорированию объектов критической информационной инфраструктуры в <Наименование организации>

В целях исполнения требований Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Постановления 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»,

ПРИКАЗЫВАЮ:

1. Создать комиссию по категорированию объектов критической информационной инфраструктуры (далее – КИИ) <Наименование организации>, в составе:

Председателя комиссии	<ФИО Руководителя субъекта КИИ/уполномоченного им лица>
Членов комиссии:	<ФИО специалистов, участвующих в процессах в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ>
	<ФИО специалистов по информационной безопасности>
	<ФИО специалистов по защите государственной тайны>
	<ФИО специалистов по ГО и ЧС>

2. В своей работе комиссии строго руководствоваться требованиями нормативных документов в сфере обеспечения безопасности КИИ.
3. Комиссии в срок до «__» _____ 201_ года разработать перечень объектов КИИ, подлежащих категорированию и направить его в <Наименование организации (при наличии подведомственности)> по адресу: _____ для согласования.
4. Комиссии в срок до «__» _____ 201_ года провести категорирование объектов КИИ в соответствии с утвержденным перечнем (п. 3 настоящего

Приказа) согласно требованиям Постановления 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».

5. Комиссии направить результаты проведенного категорирования во ФСТЭК России согласно требованиям Приказа ФСТЭК России от 22.12.2017 №236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»).
6. Контроль над исполнением настоящего приказа оставляю за собой.
7. Приказ вступает в силу со дня его регистрации.

Процедура категорирования

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

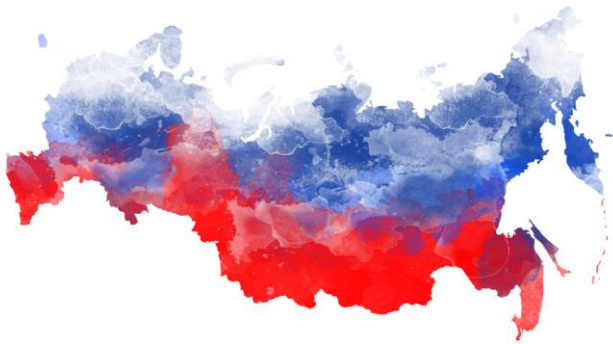
В соответствии с **перечнем показателей критериев значимости**



Критерии значимости:



- Социальная значимость (5 показателей)
- 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.



Форма Акта категорирования

УТВЕРЖДАЮ

(руководитель организации)

(подпись, инициалы, фамилия)

«___» _____ 20__ г.

А К Т категорирования объекта критической информационной инфраструктуры

(наименование объекта)

На основании приказа от «___» _____ 20__ г. № _____ комиссия в составе:

председатель комиссии: _____

(полн., должность, фамилия, инициалы)

члены комиссии: _____

(полн., должность, фамилия, инициалы)

(полн., должность, фамилия, инициалы)

(полн., должность, фамилия, инициалы)

в соответствии с требованиями Федерального закона от 26.07.2017 №187, постановления Правительства РФ от 08.02.2018г. №127 проведена категорирование объекта критической информационной инфраструктуры _____

(наименование объекта)

В ходе работы комиссия по категорированию определила:

1. Сведения об объекте критической информационной инфраструктуры (далее – КИИ), представленные в Приложении 1.
2. Сведения об угрозах безопасности информации объекта КИИ, представленные в Приложении 2.
3. Реализованные на объекте КИИ меры по обеспечению безопасности, представленные в Приложении 3.
4. Масштаб возможных последствий в случае возникновения компьютерных инцидентов в соответствии с перечнем показателей критериев значимости, представленный в Приложении 4.

На основании результата анализа значений показателей критериев значимости объекта КИИ в соответствии с постановлением Правительства РФ от 08.02.2018г. №127 объекту

присвоена категория _____

(наименование объекта)

Состав необходимых мер по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов КИИ, утвержденными приказом ФСТЭК от 25.12.2017 № 239, представлен в Приложении 5.

Председатель комиссии:

(ИО, подпись)

Члены комиссии:

(ИО, подпись)

(ИО, подпись)

(ИО, подпись)

Приложение 1

Сведения об объекте КИИ:

Наименование объекта	
Адреса размещения объекта	
Сфера (область) деятельности, в которой функционирует объект	
Назначение объекта	
Критические процессы, которые обеспечиваются объектом	
Архитектура объекта	

Сведения о программных и программно-аппаратных средствах, используемых на объекте КИИ:

Программно-аппаратные средства	Пользовательские компьютеры - шт. Серверы - шт. Телекоммуникационное оборудование - шт. Средства беспроводного доступа - шт. Производственное оборудование - шт. Иные программно-аппаратные средства - шт.
Общесистемное программное обеспечение	Наименования операционных систем: Средства виртуализации.
Прикладное программное обеспечение	
Средства защиты информации	

Сведения о взаимодействии объекта КИИ и сетей электросвязи.

Категория сети электросвязи	
Наименование оператора связи	
Цель взаимодействия с сетью электросвязи	
Способ взаимодействия с сетью электросвязи	

Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта КИИ:

Категория нарушителя	
Угрозы безопасности информации	

Возможные последствия в случае возникновения компьютерных инцидентов:

Типы компьютерных инцидентов	
Возможные последствия от компьютерных инцидентов	

Реализованные организационные и технические меры, применяемые для обеспечения безопасности объекта критической информационной инфраструктуры:

Организационные меры	
Технические меры	

Перечень показателей критериев значимости и их значения:

№	Показатель	Значение показателя	Категория
Социальная значимость			
1.	Причинение ущерба жизни и здоровью людей (человек)		
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; б) по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек)		
3.	Прекращение или нарушение функционирования объектов транспортной инфраструктуры, оцениваемые: а) на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг; б) по количеству людей, для которых могут быть недоступны транспортные услуги (тыс. человек)		
4.	Прекращение или нарушение функционирования сети связи, оцениваемые: а) на территории, на которой возможно прекращение или нарушение функционирования сети связи; б) по количеству людей, для которых могут быть недоступны услуги связи (тыс. человек)		
5.	Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)		
Политическая значимость			
6.	Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)		
7.	Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации		
Экономическая значимость			
8.	Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, муниципальным унитарным предприятием, государственной компанией, организацией с участием государства и (или) стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов прогнозируемого объема годового дохода по всем видам деятельности)		
9.	Возникновение ущерба бюджетам Российской Федерации, оцениваемого: а) в снижении доходов федерального бюджета, (процентов прогнозируемого годового дохода бюджета); б) в снижении доходов бюджета субъекта Российской Федерации (процентов прогнозируемого годового дохода бюджета);		

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>

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**.

Реестр объектов КИИ



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

Реестр объектов КИИ

Приказ ФСТЭК России от 21 декабря 2017г.
№235

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



Приказ ФСТЭК России от 25 декабря 2017г.
№239

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

The background of the slide is a photograph of a landscape at sunset. In the foreground, several wind turbines are silhouetted against the bright orange and yellow sky. In the middle ground, a series of high-voltage power lines with pylons stretch across the horizon. The sun is low on the horizon, creating a strong glow and casting long shadows.

Спасибо!