

КИИ - от категорирования до защиты

вебинар



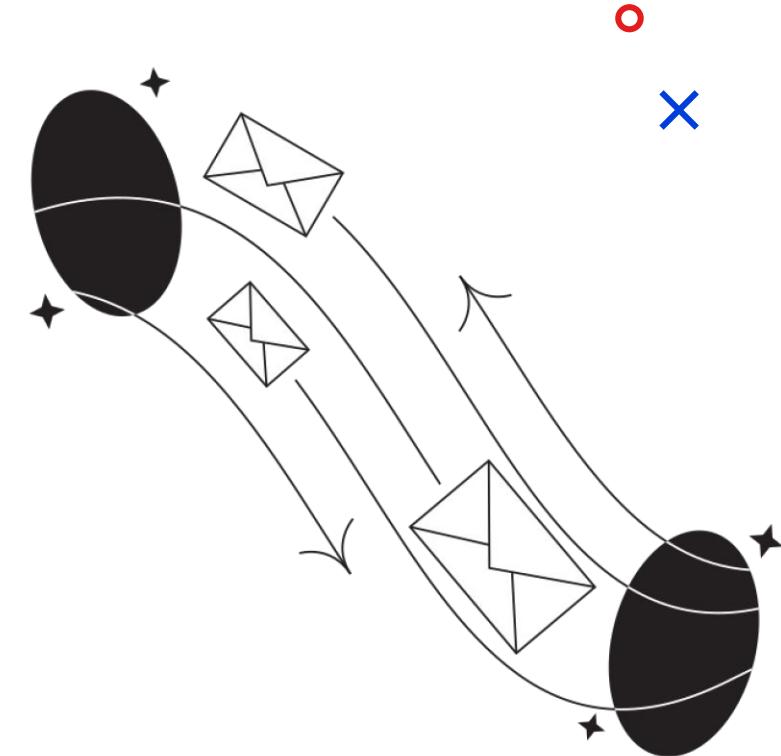


t.me/margoshater

 tmv@astral.ru

Маргарита Терехова

Специалист Астрал. Безопасность



АО «Калуга Астрал»

15 лет

на рынке информационной
безопасности

100%

успешное прохождение проверок
контролирующими органами

80+

лицензий и сертификатов на
осуществление деятельности

70+

компаний-вендоров
в нашем brand-листе

32 000+

реализованных проектов

ТОП-30

CNews и Tadviser. Крупнейшие компании
России в сфере ИБ

ТОП-3

Magic People IT Channel Awards 2020. В
номинации «Антикризисная команда»

Направления «Астрал. Безопасность»

1. Защита персональных данных
2. Защита конфиденциальной информации
3. Защита государственной тайны
4. Защита коммерческой тайны
5. Защита объектов КИИ
6. Поставка средств защиты информации
7. Проведение пентестов
8. Импортозамещение
9. Аудит информационной безопасности
10. Разработка информационных систем
11. Внедрение системы видеонаблюдения
12. Обучение в области информационной безопасности
13. Организация защищенного удаленного рабочего места
14. Подключение к корпоративному центру мониторинга ГосСОПКА
15. Аттестация государственных информационных систем (ГИС)

Будьте в курсе последних новостей



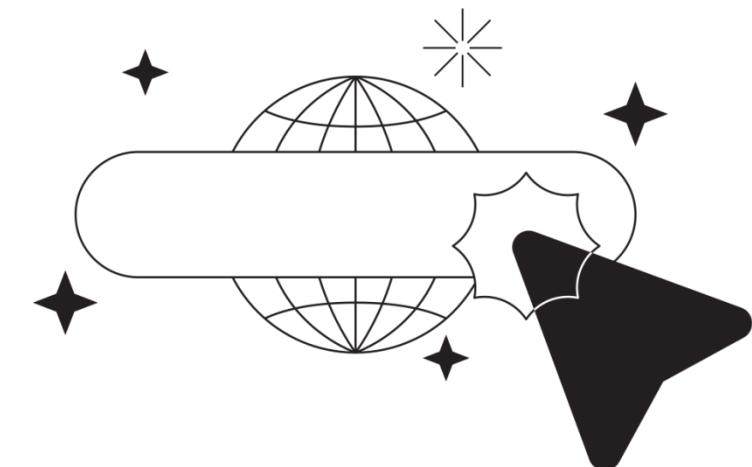
is.astral.ru



vk.com/is.astral

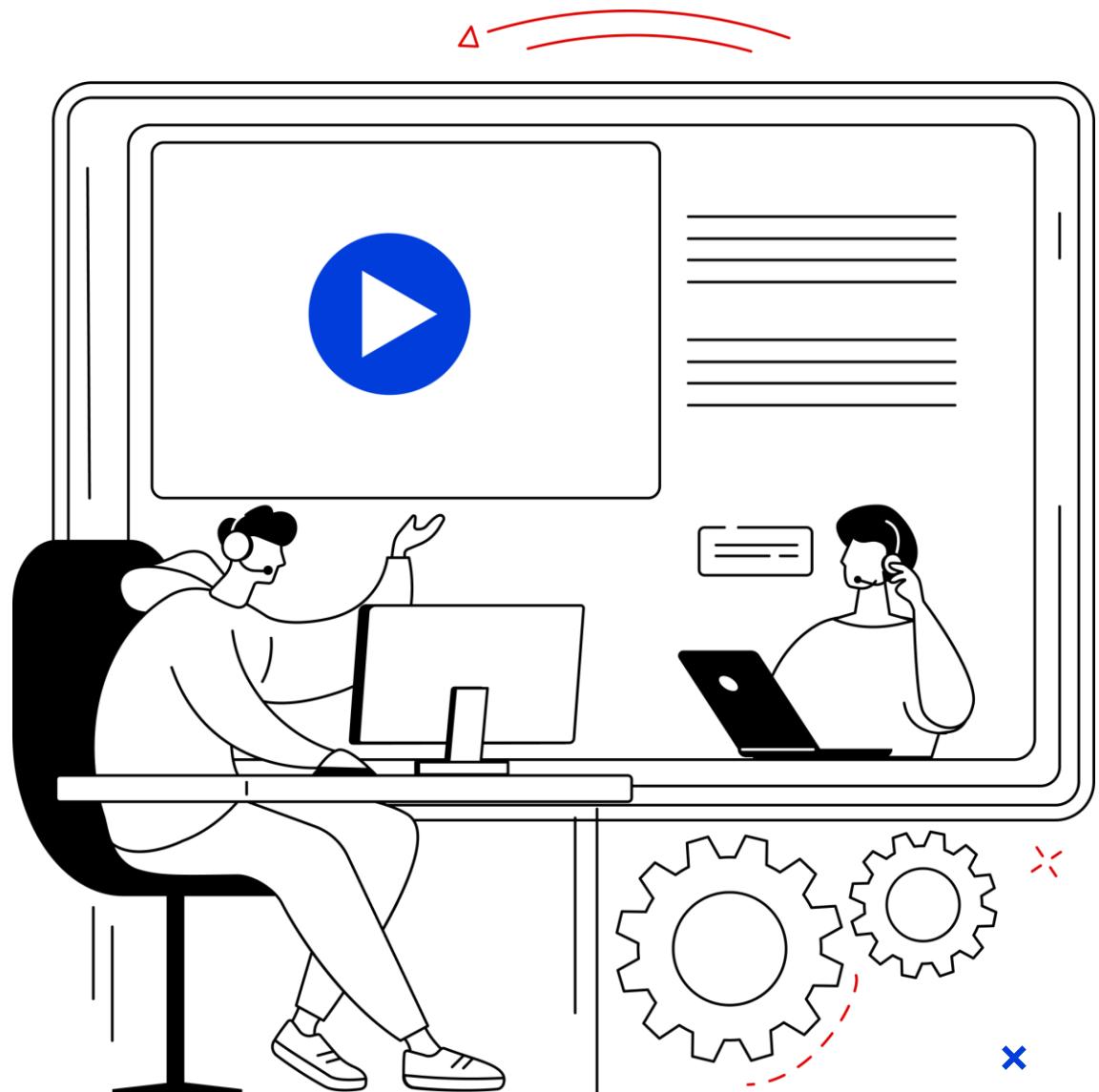


t.me/is_astral



План вебинара

1. Перечислим нормативные документы
2. Разберем процесс категорирования
3. Поговорим куда и как отправлять сведения по объектам КИИ
4. Проговорим как обеспечить защиту ЗО КИИ



Нормативные документы

1

Федеральный закон от 26.07.2017 № 187

«О безопасности критической информационной инфраструктуры РФ»

2

Приказ ФСТЭК России от 06.12.2017 № 236

«Об утверждении формы направления сведений о результатах присвоений объекту КИИ одной из категорий значимости»

3

Постановление правительства РФ от 08.02.2018 № 127

«Об утверждении правил категорирования объектов критической информационной инфраструктуры РФ, а так же перечня показателей критериев значимости объектов КИИ РФ и их значений»

4

Приказ ФСТЭК России от 25.12.2017 № 239

«Об утверждении требований по обеспечению безопасности ЗО объектов КИИ РФ»

5

Приказ ФСТЭК России от 25.12.2017 № 235

«Об утверждении требований к созданию системы безопасности значимых объектов критической информационной инфраструктуры РФ и обеспечению их функционирования»

6

Указ Президента РФ от 30.03.2022 №166

«О мерах по обеспечению технической независимости и безопасности КИИ РФ»

7

Указ Президента РФ от 01.05.2022 №250

«О дополнительных мерах по обеспечению информационной безопасности РФ»

Кто может прийти с проверкой

ФСТЭК

Прокуратору

ФСБ

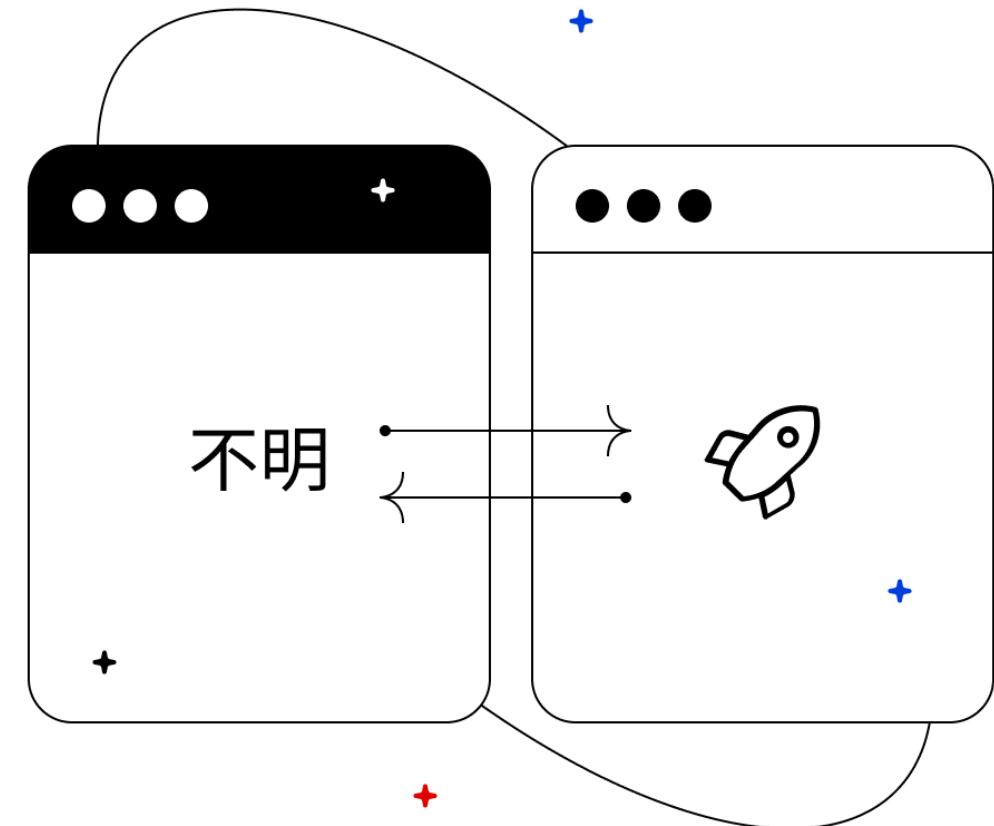
Представители
министерства



Основные понятия

1. **Субъекты критической информационной инфраструктуры** – это организации подпадающие под сферу действия закона

2. **Объекты критической информационной инфраструктуры** – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры



+ в чат, кто знает, что
является субъектом КИИ





Сфера действия ФЗ 187



Здравоохранение

больничные и амбулаторно-поликлинические учреждения, диспансеры, учреждения скорой медицинской помощи



Наука

институты ядерной физики и научно-исследовательские, медицинские университеты и др., где ведется научная деятельность



Транспорт

железные дороги, метро, аэропорты, канатные дороги, организации городского общественного транспорта



Финансы

банки, страховые компании, кредитные организации



Оборона

организации в области разработки и производства оборонной продукции



Связь

операторы связи, провайдеры

Сфера действия ФЗ 187



Химическая

производство аммиака, содовые производства, силикатная промышленность, удобрения, пестициды, полиэтилен, бакелит



Горнодобывающая

рудодобывающие организации,, промышленность неметаллических ископаемых и местных стройматериалов, гидроминеральные



Металлургическая

черная металлургия (нерудное сырье, трубное производство) и цветная металлургия (медь, свинец-цинк, никель-cobальт)



ТЭК

добыча и переработка нефти, природного газа, угля, урана



Атомная и энергетика

разработка и производство атомной энергии, объекты электроэнергетики



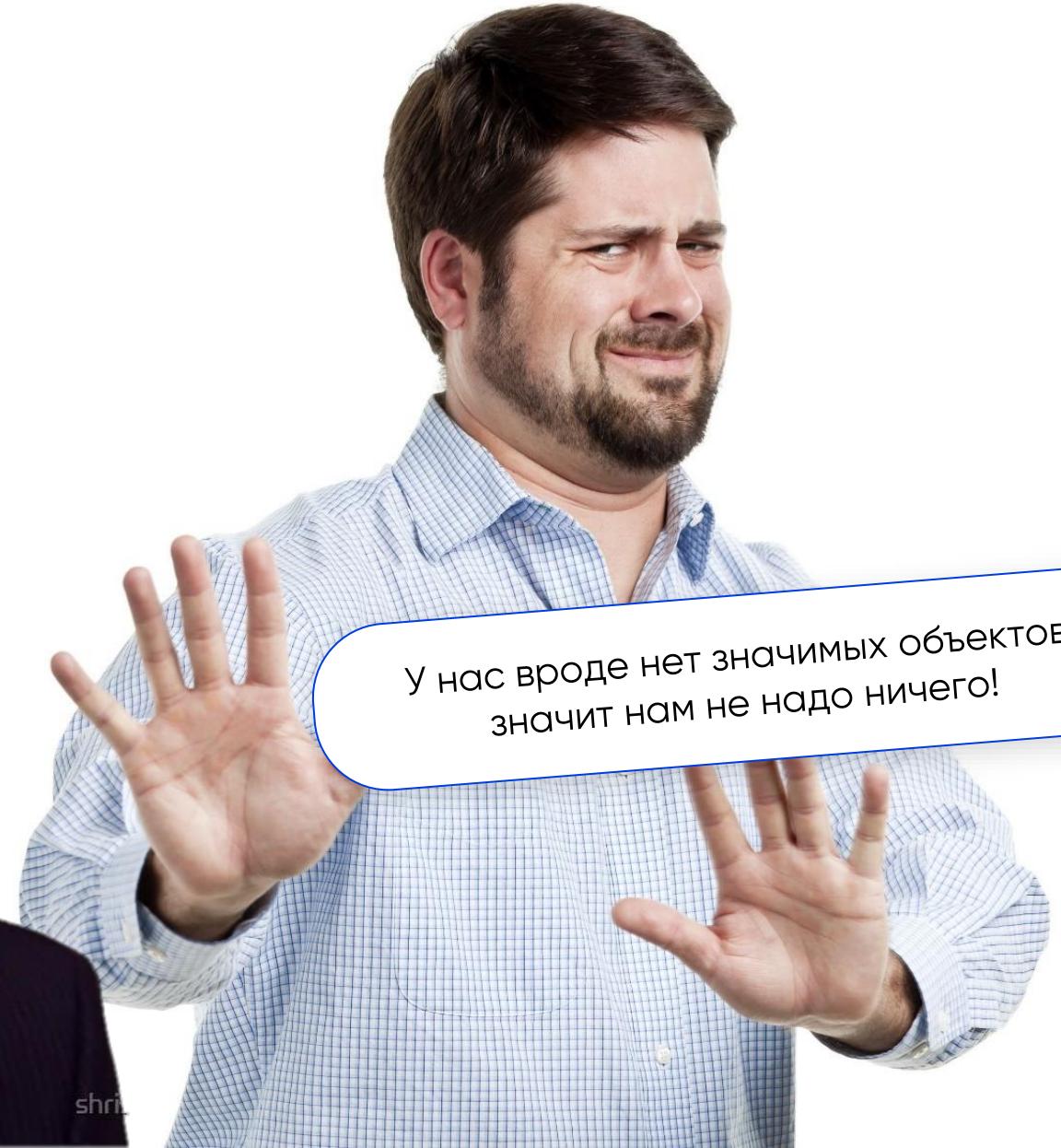
Ракетно-космическая

производство космической техники, создание ракетных двигателей

3 этапа соблюдения ФЗ

1. Категорирование объектов критической информационной инфраструктуры
2. Обеспечение безопасности значимых объектов КИИ
3. Подключение значимых объектов КИИ к государственной системе обнаружения и ликвидации последствий компьютерных атак





Обязанности субъекта КИИ

1. Провести категорирование объектов КИИ

в соответствии с требованиями 187-ФЗ и Постановления Правительства РФ от 08.02.2018 № 127

2. Информировать об инцидентах

Незамедлительно информировать о компьютерных инцидентах ГосСОПКА

3. Возложить полномочия

на заместителя руководителя организации по обеспечению информационной безопасности , в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты

4. Создать структурное подразделение

осуществляющее функции по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, либо возложить данные функции на существующее структурное подразделение;

3 этапа соблюдения ФЗ

1. Категорирование объектов критической информационной инфраструктуры
2. Обеспечение безопасности значимых объектов КИИ
3. Подключение значимых объектов КИИ к государственной системе обнаружения и ликвидации последствий компьютерных атак



1

Формирование комиссии

2

Определение процессов

3

Определение критических процессов

4

Определение объектов КИИ, подготовка перечня, отправка во ФСТЭК

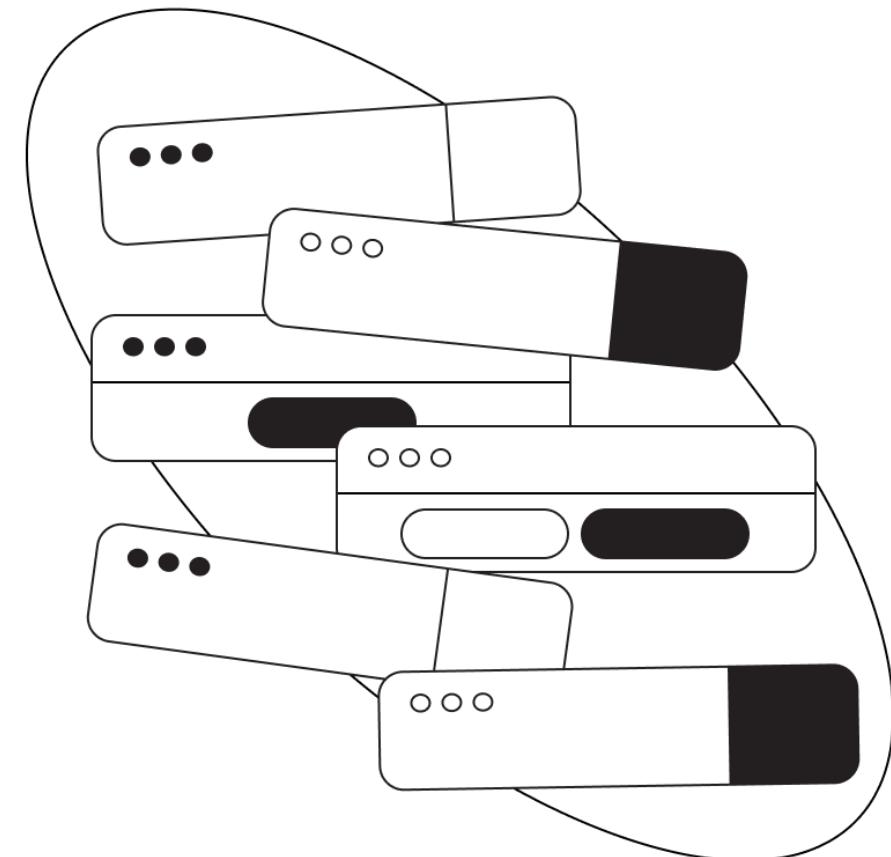
5

Подготовка форм сведений №236 для каждого объекта КИИ и Акта категорирования

6

Отправка форм сведений во ФСТЭК

6 этапов категорирования объектов КИИ



1

Формирование комиссии

2

Определение процессов

3

Определение критических процессов

4

Определение объектов КИИ, подготовка перечня, отправка во ФСТЭК

5

Подготовка форм сведений №236 для каждого объекта КИИ и Акта категорирования

6

Отправка форм сведений во ФСТЭК

Кто входит в комиссию

1. Руководитель субъекта КИИ
2. Руководитель ИБ подразделения
3. Руководитель ИТ подразделения
4. Руководитель подразделения АСУ
5. Ответственный за систему управления промышленной безопасности
6. Руководитель подразделения комплексной безопасности
7. Ответственный за ГО и ЧС
8. Другие руководители бизнес-подразделений, ответственные за управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ.

1
Формирование комиссии

2
Определение процессов

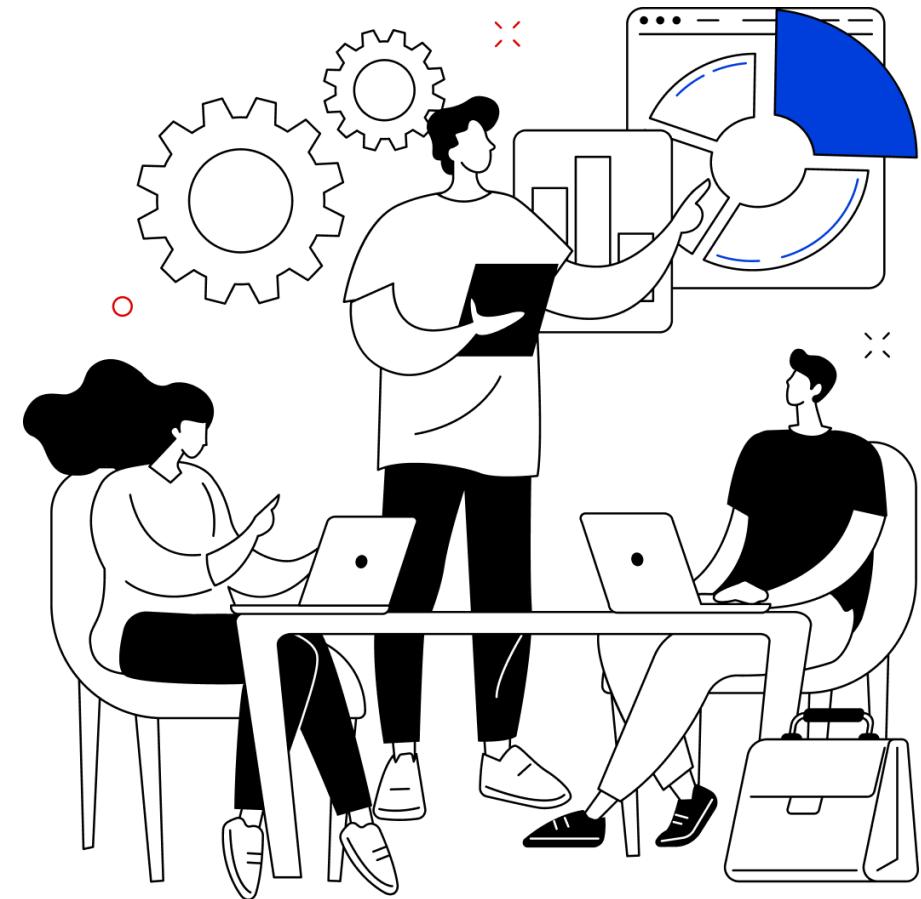
3
Определение критических процессов

4
Определение объектов КИИ, подготовка перечня, отправка во ФСТЭК

5
Подготовка форм сведений №236 для каждого объекта КИИ и Акта категорирования

6
Отправка форм сведений во ФСТЭК

Выписываем все процессы, происходящие в организации, и раскладываем на более мелкие



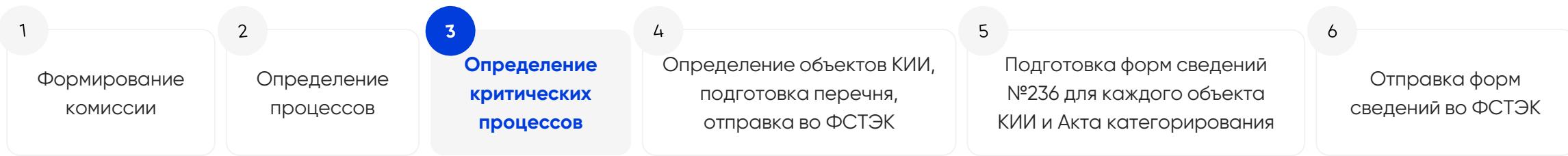


Таблица критических процессов

№	Процесс	Последствия нарушения или прекращения процесса	Критичный
1	Подача горячей воды		
1.1.	Подача горячей воды на тепловые узлы	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения	
1.2.	Подача горячей воды от теплового узла до квартиры		

1

Формирование комиссии

2

Определение процессов

3

Определение критических процессов

4

Определение объектов КИИ, подготовка перечня, отправка во ФСТЭК

5

Подготовка форм сведений №236 для каждого объекта КИИ и Акта категорирования

6

Отправка форм сведений во ФСТЭК

Рассмотрим экологическую значимость

Показатели критериев значимости	Значение показателя		
	III категория	II категория	I категория
Вредные воздействия на окружающую среду, оцениваемые: а) на территории, на которой окружающая среда может подвергнуться вредным воздействиям	в пределах территории одного муниципального образования (числ. от 2 тыс. чел.) или одной внутригородской территории города федерального значения, с выходом вредных воздействий за пределы территории субъекта критической информационной инфраструктуры	выход за пределы территории одного муниципального образования (числ. от 2 тыс. чел.) или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта Российской Федерации или территории города федерального значения, с выходом вредных воздействий за пределы территории субъекта критической информационной инфраструктуры	выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения, с выходом вредных воздействий за пределы территории субъекта критической информационной инфраструктуры
б) по количеству людей, которые могут быть подвержены вредным воздействиям (тыс. человек)	≥ 2, но < 1 000	≥ 1 000, но < 5 000	≥ 5 000

1
 Формирование комиссии

 2
 Определение процессов

 3
Определение критических процессов

 4
 Определение объектов КИИ, подготовка перечня, отправка во ФСТЭК

 5
 Подготовка форм сведений №236 для каждого объекта КИИ и Акта категорирования

 6
 Отправка форм сведений во ФСТЭК

Рассмотрим социальную значимость

Показатели критериев значимости	Значение показателя		
	III категория	II категория	I категория
Прчинение ущерба жизни и здоровью людей (человек)	более или равно 1, но менее или равно 50	более 50, но менее или равно 500	более 500
Прекращение ¹⁾ или нарушение функционирования ²⁾ объектов обеспечения жизнедеятельности населения ³⁾ , оцениваемые:			
а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения;	в пределах территории одного муниципального образования (численностью от 2 тыс. чел.) или одной внутригородской территории города федерального значения < 1000	выход за пределы территории одного муниципального образования (численностью от 2 тыс. чел.) 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 2, но менее 1000	более или равно 1000, но менее 5 000	более или равно 5 000

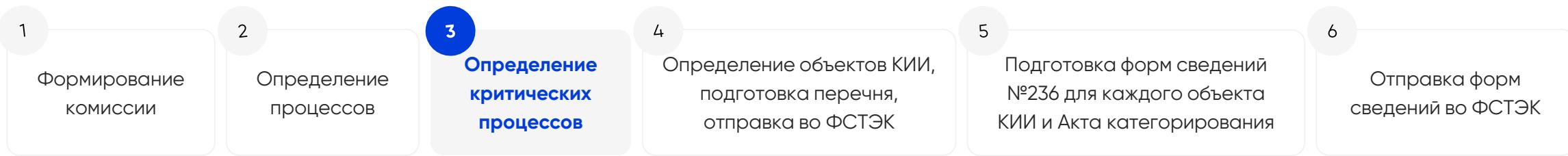


Таблица критических процессов

№	Процесс	Последствия нарушения или прекращения процесса	Критический
1	Подача горячей воды		Да
1.1.	Подача горячей воды на тепловые узлы	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения	Да
1.2.	Подача горячей воды от теплового узла до квартиры		Да

1

Формирование комиссии

2

Определение процессов

3

Определение критических процессов

4

Определение объектов КИИ, подготовка перечня, отправка во ФСТЭК

5

Подготовка форм сведений №236 для каждого объекта КИИ и Акта категорирования

6

Отправка форм сведений во ФСТЭК

Примеры критических процессов

Здравоохранение

- Оказания медицинской помощи
- Оказания психиатрической помощи
- Фармацевтическая деятельность
- Деятельность, связанная с оборотом наркотических средств и психотропных веществ
- Деятельность в области использования источников ионизирующего излучения

Транспорт

- Наземное обслуживание воздушных судов
- Обеспечение обслуживания пассажиров
- Аэродромное обеспечение
- Электросветотехническое обеспечение
- Штурманское обеспечение
- Авиатопливообеспечение
- Авиационная безопасность
- Обеспечение безопасности полетов

Энергетика

- Передача электроэнергетики и технологическое присоединение к распределительным электросетям
- Реализация электрической энергии потребителям
- Обеспечение работоспособности котельных, энергетических и тепловых сетей
- Обеспечение безопасности учреждения

1
Формирование комиссии

2
Определение процессов

3
Определение критических процессов

4
Определение объектов КИИ, подготовка перечня, отправка во ФСТЭК

5
Подготовка форм сведений №236 для каждого объекта КИИ и Акта категорирования

6
Отправка форм сведений во ФСТЭК

ФУНКЦИИ ОБЪЕКТОВ ПО 127 ПОСТАНОВЛЕНИЮ

1. Обрабатывают информацию, необходимую для обеспечения КП
2. Осуществляют управление КП
3. Осуществляют контроль КП
4. Осуществляют мониторинг КП

КП – критические процессы

1
 Формирование комиссии

 2
 Определение процессов

 3
 Определение критических процессов

 4
Определение объектов КИИ, подготовка перечня, отправка во ФСТЭК

 5
 Подготовка форм сведений №236 для каждого объекта КИИ и Акта категорирования

 6
 Отправка форм сведений во ФСТЭК

Таблица объектов КИИ

№	Наименование объекта	Тип объекта	Сфера (область) деятельности, в которой функционирует объект	Планируемый срок категорирования объекта	Должность, фамилия, имя, отчество (при наличии) представителя, его телефон, адрес электронной почты (при наличии)
1	АСУ управления компьютерным томографом	АСУ	Здравоохранение	До июня 2025	Инженер-программист И.И. Иванов Номер телефона Эл. почта
2					

1. Согласовываем с **головным учреждением**
 2. Отправляем **руководителю регионального управления ФСТЭК**

1
Формирование комиссии

2
Определение процессов

3
Определение критических процессов

4
Определение объектов КИИ, подготовка перечня, отправка во ФСТЭК

5
Подготовка форм сведений №236 для каждого объекта КИИ и Акта категорирования

6
Отправка форм сведений во ФСТЭК

Информация по объекту

1. Расположение объекта и его сегментов
2. Назначение объекта
3. Архитектура объекта
4. Состав объекта (сервера, АРМ, СХД, сетевые устройства, контроллеры, специализированное оборудование, оборудование с ЧПУ и т.д.)
5. Используемые информационные технологии
6. Используемые СЗИ
7. Карта информационных потоков
8. Взаимодействие с другими ИТ, ИТС, АСУ
9. Сведения о подключении к сетям электросвязи, операторе связи
10. Сведения о лицах эксплуатирующих элементы (компоненты) объектов КИИ
11. Сведения о имеющихся уязвимостях
12. Сведения о обеспечении физической и промышленной безопасности
13. Применяемые организационные меры защиты

1
Формирование комиссии

2
Определение процессов

3
Определение критических процессов

4
Определение объектов КИИ, подготовка перечня, отправка во ФСТЭК

5
Подготовка форм сведений №236 для каждого объекта КИИ и Акта категорирования

6
Отправка форм сведений во ФСТЭК

Определяем категорию объекта КИИ

Таблица объектов + информация по объекту

Объект КИИ

Смотрим на угрозы и анализируем возможные инциденты и их последствия

Показатели критерии значимости	Значение показателя		
	III категория	II категория	I категория
Вредные воздействия на окружающую среду, оцениваемые:			
а) на территории, на которой окружающая среда может подвернуться вредным воздействиям	в пределах территории одного муниципального образования (числ. от 2 тыс. чел.) или одной внутригородской территории города федерального значения, с выходом за пределы территорий субъекта критической информационной инфраструктуры	выход за пределы территории одного муниципального образования (числ. от 2 тыс. чел.) или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта Российской Федерации или территории города федерального значения, с выходом за пределы территории субъекта критической информационной инфраструктуры	выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения, с выходом за пределы территории субъекта критической информационной инфраструктуры
б) по количеству людей, которые могут быть подвергены вредным воздействиям (тыс. человек)	$\geq 2, < 1000$	$\geq 1000, < 5000$	≥ 5000

Сравниваем с таблицей критериев значимости

Присваиваем категорию значимости по каждому критерию

значимый / незначимый

Объект КИИ + категория значимости

1

Формирование комиссии

2

Определение процессов

3

Определение критических процессов

4

Определение объектов КИИ, подготовка перечня, отправка во ФСТЭК

5

Подготовка форм сведений №236 для каждого объекта КИИ и Акта категорирования

6

Отправка форм сведений во ФСТЭК

По итогу



Составляем **акт категорирования** – один на все объекты КИИ

На каждый объект КИИ заполняем **форму 236**

1
Формирование комиссии

 2
Определение процессов

 3
Определение критических процессов

 4
Определение объектов КИИ, подготовка перечня, отправка во ФСТЭК

 5
Подготовка форм сведений №236 для каждого объекта КИИ и Акта категорирования

 6
Отправка форм сведений во ФСТЭК

Акт категорирования

1. Один на **все** объекты КИИ
2. Хранится у вас в организации
3. Указывается: комиссия, информация об объекте КИИ, программно-аппаратные связи, взаимосвязи инфраструктуры и сетей электросвязи, угрозы безопасности информации и т.д.

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: _____ (пол., должность, фамилия, инициалы)

члены комиссии:
 _____ (пол., должность, фамилия, инициалы)
 _____ (пол., должность, фамилия, инициалы)
 _____ (пол., должность, фамилия, инициалы)

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

Ходе работы комиссии по категорированию определена:

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

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

(наименование объекта) присвоена категория _____.

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: _____ (ФИО, подпись)

Члены комиссии:
 _____ (ФИО, подпись)
 _____ (ФИО, подпись)
 _____ (ФИО, подпись)

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. Техническое исполнительное оборудование - шт.
Обеспечение программное обеспечение	Средства беспроводного доступа - шт. Производственное оборудование - шт. Иные программно-аппаратные средства - шт.
Прикладное программное обеспечение	Наименование операционных систем: Средства виртуализации:
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
Возможные последствия от компьютерных инцидентов	

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

Организационные меры	
Технические меры	

Перечень показателей критерии значимости и их значения:

№	Показатель	Социальная значимость		Категория
		Значение показателя		
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, теплоснабжения, газоснабжения, электроснабжения, коммунальных сооружений, оцениваемые:			
	а) на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг;			
	б) по количеству людей, для которых могут быть нарушены 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 (тыс. человек);			
	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 пользователей 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 с субъектом Российской Федерации и подписание планируемого в дальнейшем международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации			
	Экономическая значимость			
8.	Возникновение ущерба субъектам критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, муниципальным унитарным предприятием, государственной компанией, организацией с участием государства и (или) стратегическими акционерными обществами, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акций 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);			

1
Формирование комиссии

 2
Определение процессов

 3
Определение критических процессов

 4
Определение объектов КИИ, подготовка перечня, отправка во ФСТЭК

 5
Подготовка форм сведений №236 для каждого объекта КИИ и Акта категорирования

 6
Отправка форм сведений во ФСТЭК

Форма 236

1. Заполняется на **каждый** объект КИИ, даже если он незначимый
2. Содержит сведения о результатах присвоения объекту КИИ одной из категорий значимости
3. Отправляется во ФСТЭК
4. Если есть замечания от ФСТЭКа, то есть 10 дней на внесение правок

1. Сведения об объекте критической информационной инфраструктуры

1.1. Наименование объекта(наименование информационной системы, автоматизированной системы управления информационно-телекоммуникационной сетью)	
1.2. Адреса размещения объекта в том числе адреса обособленных подразделений (филиалов представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта	
1.3. Сфера (область) деятельности в которой функционирует объект, в соответствии с пунктом 2 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	
1.4. Назначение объекта	
1.5. Тип объекта (информационная система, автоматизированная система управления информационно-телекоммуникационная сеть)	
1.6. Архитектура объекта одноранговая сеть, клиент-серверная система, технология "тонкий клиент", сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура)	

2. Сведения о субъекте критической информационной инфраструктуры

2.1. Наименование субъекта	
2.2. Адрес местонахождения субъекта	
2.3. Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	
2.4. Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов, или в случае отсутствия такого должностного лица, наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта	
2.5. Структурное	

подразделение ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	
2.6. ИНН субъекта и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	

3. Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи

3.1. Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при помощи электромагнитных систем) или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	
3.2. Наименование оператора связи (или) провайдера хостинга	
3.3. Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	
3.4. Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), протоколов взаимодействия	

4. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

4.1. Наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя, эксплуатирующего объект	
4.2. Адрес местонахождения юридического лица или адрес места жительства индивидуального предпринимателя, эксплуатирующего объект	
4.3. Элемент (компонент) объекта, который эксплуатируется лицом (центр обработки данных, серверное оборудование, телекоммуникационное оборудование, технологическое производственное оборудование (исполнительные устройства), иные элементы (компоненты))	
4.4. ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	
4.5. Наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя, эксплуатирующего объект	
4.6. Адрес местонахождения юридического лица или адрес места жительства индивидуального предпринимателя, эксплуатирующего объект	
4.7. Элемент (компонент) объекта, который эксплуатируется лицом (центр обработки данных, серверное оборудование, телекоммуникационное оборудование, технологическое производственное оборудование (исполнительные устройства), иные элементы (компоненты))	
4.8. ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	

5. Сведения о программных и программно-аппаратных средствах, используемых

1
Формирование комиссии

2
Определение процессов

3
Определение критических процессов

4
Определение объектов КИИ, подготовка перечня, отправка во ФСТЭК

5
Подготовка форм сведений №236 для каждого объекта КИИ и Акта категорирования

6
Отправка форм сведений во ФСТЭК

Форма 236 содержит

1. Сведения об объекте КИИ
2. Сведения о субъекте КИИ
3. Сведения о взаимодействии объекта КИИ и сетей электросвязи
4. Сведения о лице, эксплуатирующем объект КИИ
5. Сведения о программных и программно-аппаратных средствах, используемых на объекте КИИ
6. Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта КИИ
7. Возможные последствия в случае возникновения компьютерных инцидентов
8. Категория значимости, которая присвоена объекту КИИ, или сведения об отсутствии необходимости присвоения одной из категорий значимости, а также сведения о результатах оценки показателей критериев значимости
9. Организационные и технические меры, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры

1
Формирование комиссии

2
Определение процессов

3
Определение критических процессов

4
Определение объектов КИИ, подготовка перечня, отправка во ФСТЭК

5
Подготовка форм сведений №236 для каждого объекта КИИ и Акта категорирования

6
Отправка форм сведений во ФСТЭК

Ответ от ФСТЭКа



Значимый объект



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ
КОНТРОЛЮ
(ФСТЭК России)
Старая Басманная, 17, Москва, 105066
Тел./факс: (495) 699-04-04
E-mail: post@fss.ru
13_08_20_09_№ 240/
На №_____

О рассмотрении сведений о
результатах категорирования

Уважаемый [Имя получателя]

Сведения о результатах присвоения объекту критической информационной инфраструктуры Российской Федерации одной из категорий значимости, представленные ФСТЭКом «Банкоматы, кассы, скайп интернет» в виде вложений в письме № 187-ФЗ, ФСТЭК России рассмотрены.

В соответствии с частью 7 статьи 7 Федерального закона от 26 июня 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» уведомляем о внесении указанных сведений в Реестр значимых объектов критической информационной инфраструктуры Российской Федерации:

№ п/з	Регистрационный номер	Наименование объекта	Дата внесения в Реестр
1	1300012 2 15	ИС «МЕРКУРИЙ»	23.01.2019

с уважением,
[Signature]

Исполняющий обязанности
начальника 2 управления

Е.Торбенко



Незначимый объект



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ
КОНТРОЛЮ
(ФСТЭК России)
Старая Басманная, 17, Москва, 105066
Тел./факс: (495) 699-04-04
E-mail: post@fss.ru
13_08_20_09_№ 240/25/115
На №_____

О направлении сведений в ГосСОПКА

В соответствии с частью 10 статьи 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» уведомляем о том, что сведения об отсутствии необходимости присвоения объектам критической информационной инфраструктуры Российской Федерации категории значимости, представленные ФСТЭКом «Банкоматы, кассы, скайп интернет» проверены и направлены в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Начальник 2 управления

[Signature]

Д.Шевцов

1

Формирование комиссии

2

Определение процессов

3

Определение критических процессов

4

Определение объектов КИИ, подготовка перечня, отправка во ФСТЭК

5

Подготовка форм сведений №236 для каждого объекта КИИ и Акта категорирования

6

Отправка форм сведений во ФСТЭК

Незначимые объекты

1. ФСТЭК передает данные об объектах в ГосСОПКу
2. Вы должны:
 1. Информировать о компьютерных инцидентах ГосСОПКА
 2. Оказывать содействие должностным лицам ФСБ РФ, в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов

1

Формирование комиссии

2

Определение процессов

3

Определение критических процессов

4

Определение объектов КИИ, подготовка перечня, отправка во ФСТЭК

5

Подготовка форм сведений №236 для каждого объекта КИИ и Акта категорирования

6

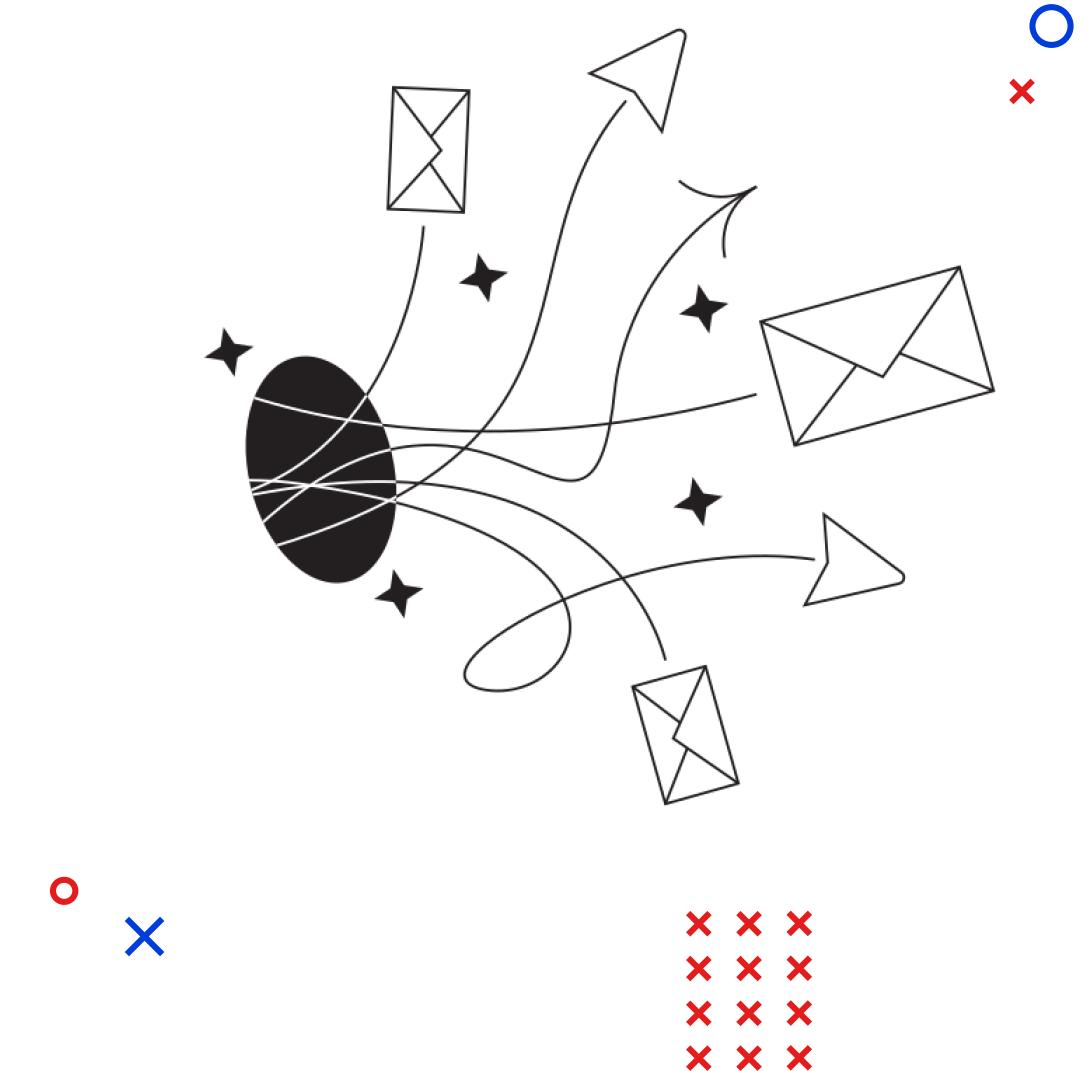
Отправка форм сведений во ФСТЭК

Значимые объекты

Согласно приказам ФСТЭК №235 и №239 от 25.12.2017 необходимо обеспечить безопасность данных объектов

1. Установление 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 ввод его в действие
4. Обеспечение безопасности значимого объекта в ходе его эксплуатации
5. Обеспечение безопасности значимого объекта при выводе его из эксплуатации

В каких случаях в данные документы нужно вносить изменения?



1. По решению, принятому по результатам проверки, проведенной в рамках осуществления гос. контроля в области обеспечения безопасности значимых объектов КИИ

2. В случае изменения значимого объекта КИИ, в результате которого такой объект перестал соответствовать критериям значимости и показателям их значений, на основании которых ему была присвоена определенная категория значимости, **в течение 2 недель**

3. В связи с ликвидацией, реорганизацией субъекта КИИ и (или) изменениями его организационно-правовой формы, в результате которых были изменены либо утрачены признаки субъекта КИИ

4. Так же в случае появления новых объектов КИИ, или модернизации существующих **в течение 2 недель**

5. По прошествии 5 лет после согласования со ФСТЭК

3 этапа соблюдения ФЗ

1. Категорирование объектов критической информационной инфраструктуры
2. **Обеспечение безопасности значимых объектов КИИ**
3. Подключение значимых объектов КИИ к государственной системе обнаружения и ликвидации последствий компьютерных атак



Обеспечение безопасности значимых объектов

1

**Приказ ФСТЭК России
от 21 декабря 2017 г. №235**

«Об утверждении Требований к созданию систем
безопасности значимых объектов критической
информационной инфраструктуры Российской
Федерации и обеспечению их функционирования»

2

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

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

Требования к работникам по безопасности



Руководитель подразделения по безопасности

- высшее проф. образование по специальности в области ИБ
- ИЛИ иное высшее проф. образование и документ о проф. переподготовке по направлению ИБ (срок обучения не менее 360 часов)
- наличие стажа работы в сфере ИБ не менее 3-х лет



Штатные работники подразделения безопасности

- высшее проф. образование по специальности в области ИБ
- ИЛИ иное высшее проф. образование и документ о повышении квалификации по направлению ИБ (срок обучения не менее 72 часов)
- прохождение не реже 1 раза в 5 лет обучения по программам повышения квалификации по направлению ИБ

5 шагов к обеспечению безопасности значимых объектов КИИ

- 1 Установление требований к обеспечению безопасности значимого объекта (ЗО)
- 2 Разработка организационных и технических мер по обеспечению безопасности ЗОКИИ
- 3 Внедрение организационных и технических мер по обеспечению безопасности ЗО и ввод его в действие
- 4 Обеспечение безопасности значимого объекта в ходе его эксплуатации
- 5 Обеспечение безопасности значимого объекта при выводе его из эксплуатации



1

Установление требований к обеспечению безопасности значимого объекта (ЗО)

Разработка технического задания

1. Цель и задачи обеспечения безопасности ЗОКИИ
2. Категория значимости ЗОКИИ
3. Перечень НПА
4. Перечень типов объектов защиты ЗОКИИ
5. Требования к организационным и техническим мерам
6. Стадии (этапы работ) создания подсистемы безопасности ЗОКИИ
7. Требования к программным и программно-аппаратным средствам и СЗИ
8. Требования к защите средств и систем, обеспечивающих функционирование ЗОКИИ (обеспечивающей инфраструктуре)
9. Требования к информационному взаимодействию ЗОКИИ с иными объектами КИИ, а также иными ИС, АСУ, ИТКС
10. Требования к составу и содержанию документации, разрабатываемой в ходе создания ЗОКИИ

1

Установление требований к обеспечению безопасности значимого объекта (ЗО)

Что нужно учитывать, при разработке ТЗ

ГОСТ Р 59853-2021

Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения

ГОСТ 34.201-2020

Информационные технологии (ИТ). Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем

ГОСТ 34.602-89

Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы

ГОСТ Р 50922-2006

Защита информации. Основные термины и определения

ГОСТ Р 51583-2014

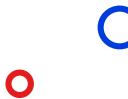
Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения

ГОСТ Р 51624-2000

Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования

5 шагов к обеспечению безопасности значимых объектов КИИ

- 1 Установление требований к обеспечению безопасности значимого объекта (ЗО)
- 2 **Разработка организационных и технических мер по обеспечению безопасности ЗОКИИ**
- 3 Внедрение организационных и технических мер по обеспечению безопасности ЗО и ввод его в действие
- 4 Обеспечение безопасности значимого объекта в ходе его эксплуатации
- 5 Обеспечение безопасности значимого объекта при выводе его из эксплуатации



2

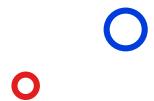
Разработка организационных и технических мер по обеспечению безопасности ЗОКИИ

Происходит в 3 этапа

1. Моделирование угроз

2. Проектирование системы защиты

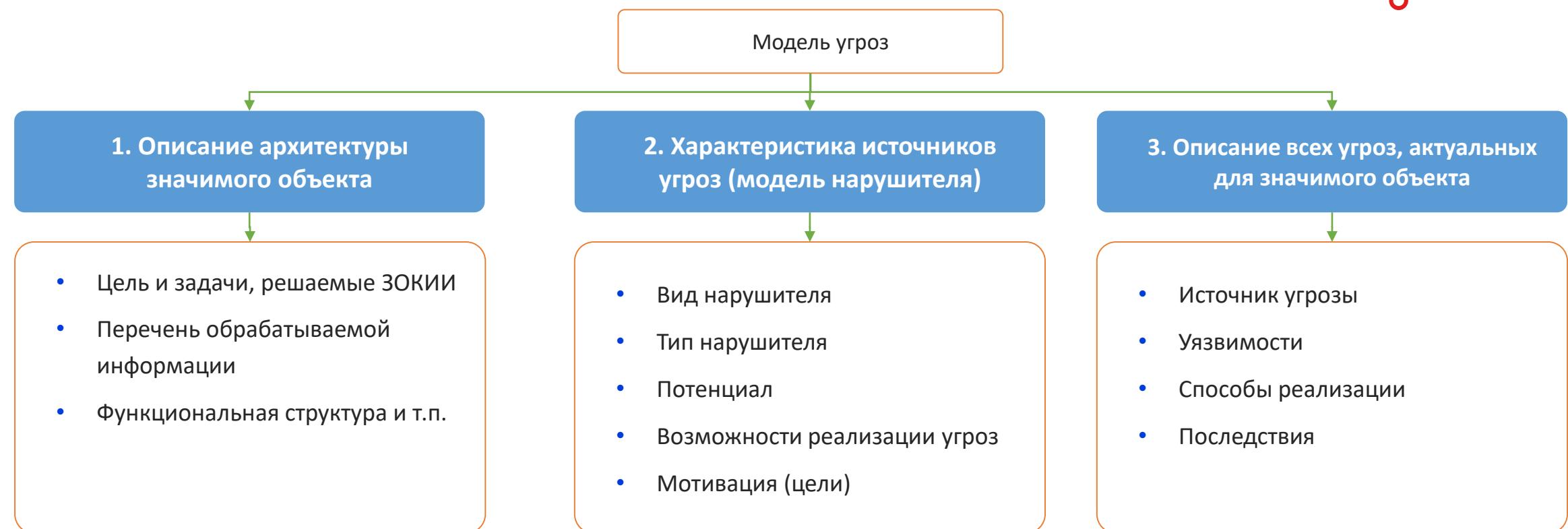
3. Разработка рабочей (эксплуатационной) документации



2

Разработка организационных и технических мер по обеспечению безопасности ЗОКИИ

1. Моделирование угроз



2

Разработка организационных и технических мер по обеспечению безопасности ЗОКИИ

1. Моделирование угроз



Модель угроз разрабатывается с учетом [методического документа](#), разработанного ФСТЭК России от 5 февраля 2021 г.

Актуальность возможных угроз безопасности информации определяется наличием сценариев их реализации, возможностью нарушителя к осуществлению сценария и наличием интерфейса с объектом воздействия.

При наличии хотя бы одного сценария угрозы безопасности информации такая угроза признается актуальной для системы и включается в Модель угроз безопасности для обоснования выбора организационных и технических мер по защите информации (обеспечению безопасности).

2

Разработка организационных и технических мер по обеспечению безопасности ЗОКИИ

2. Проектирование системы защиты

1. Определение субъектов и объектов доступа
2. Определение политик управления доступом
3. Определение и обоснование организационных и технических мер
4. Определение видов и типов средств защиты информации
5. Выбор средств защиты информации
6. Разработка архитектуры подсистемы безопасности значимого объекта
7. Определение требований к параметрам настройки программных и программно-аппаратных средств
8. Определение мер по обеспечению безопасности при взаимодействии значимого объекта с иными объектами

2

Разработка организационных и технических мер по обеспечению безопасности ЗОКИИ

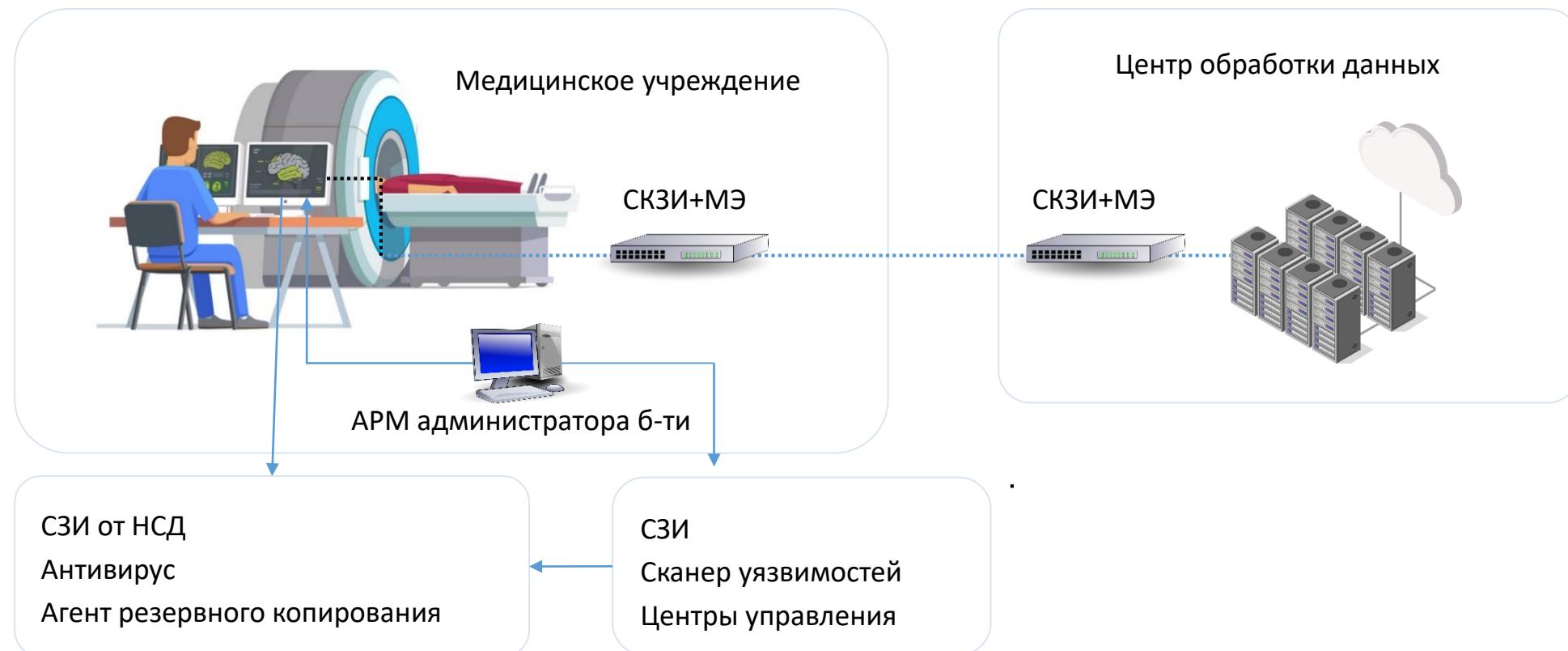
2. Проектирование системы защиты. Состав технического проекта

- 1. Ведомость ТП
- 2. Ведомость покупных изделий
- 3. Спецификация
- 4. Схема функциональной структуры
- 5. Схема структурная
- 6. Программы и методики испытаний
- 7. Перечень кабельных соединений
- 8. Описание информационного обеспечения
- 9. Описание комплекса программных средств
- 10. Описание комплекса технических средств
- 11. Описание алгоритма
- 12. Описание автоматизируемых функций
- 13. Пояснительная записка

2

Разработка организационных и технических мер по обеспечению безопасности ЗОКИИ

2. Проектирование системы защиты. Крупная медицинская техника



2

Разработка организационных и технических мер по обеспечению безопасности ЗОКИИ

2. Проектирование системы защиты. Выбор СЗИ 1



2

Разработка организационных и технических мер по обеспечению безопасности ЗОКИИ

2. Проектирование системы защиты. Выбор СЗИ 2

4. Система резервного копирования

ОДТ.4 Резервное копирование информации

ОДТ.5 Обеспечение возможности восстановления информации

ОДТ.6 Обеспечение возможности восстановления ПО

5. Сканер уязвимостей

АУД.2 Анализ уязвимостей и их устранение

АУД.1 Инвентаризация информационных ресурсов

АУД.10 Проведение внутренних аудитов

СЗИ от НСД

Secret Net

Dallas Lock

Антивирус

Касперский антивирус

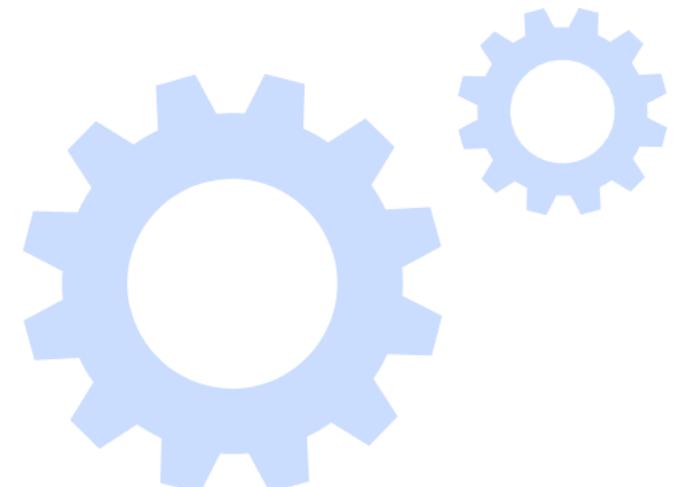
Dr Web

ПАК МЭ + СКЗИ

АПКШ Континент 3.9.

ViPNet Coordinator HW

С-Терра



Система резервного копирования

Кибер бекап

RuBackup

Сканер уязвимостей

Сканер-ВС

MaxPatrol 8

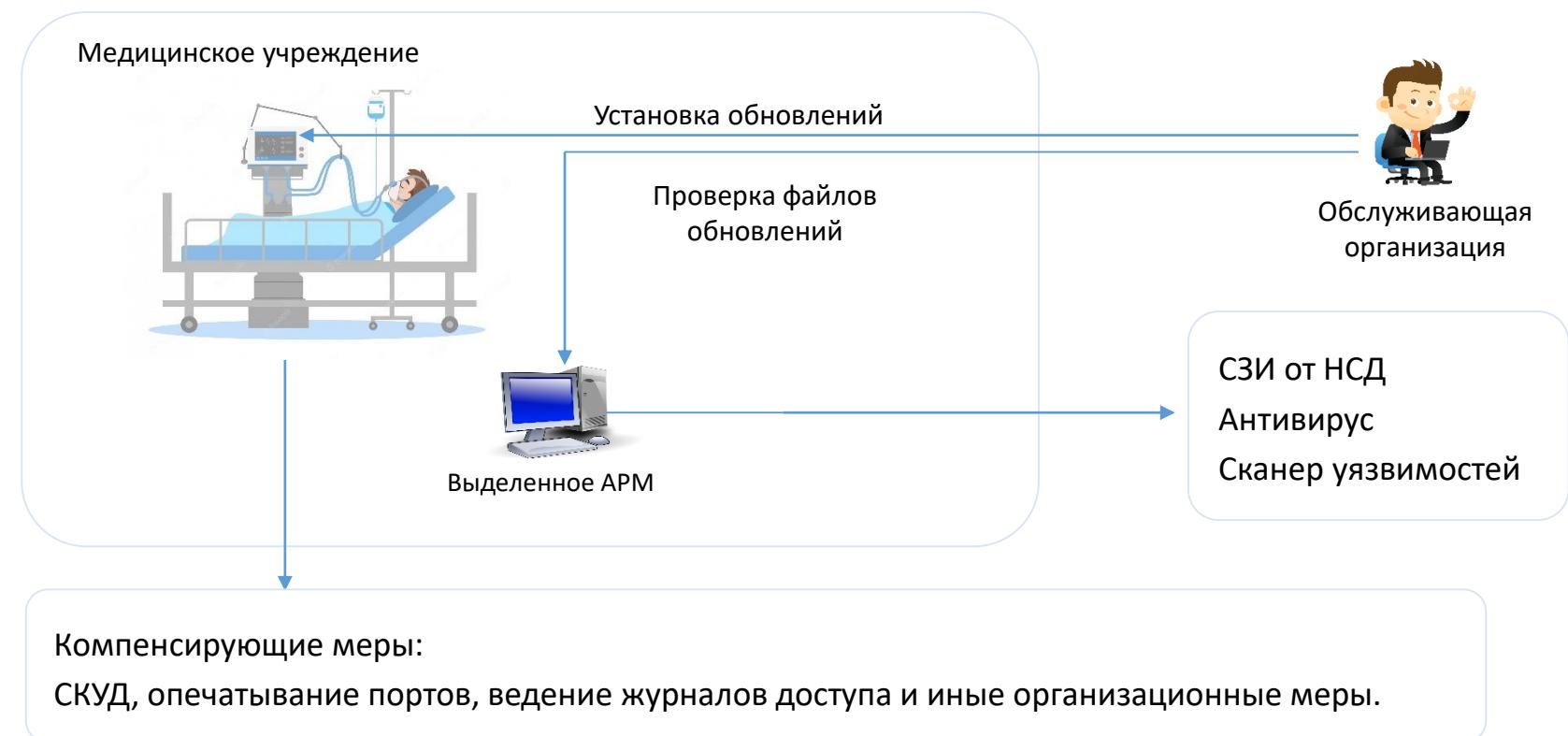
RedCheck

PT VM

2

Разработка организационных и технических мер по обеспечению безопасности ЗОКИИ

2. Проектирование системы защиты. Медицинская техника без возможности установки СЗИ



2

Разработка организационных и технических мер по обеспечению безопасности ЗОКИИ

3. Разработка рабочей (эксплуатационной) документации

1. описание архитектуры подсистемы безопасности значимого объекта
2. порядок и параметры настройки программных и программно-аппаратных средств, в том числе средств защиты информации
3. правила эксплуатации программных и программно-аппаратных средств, в том числе средств защиты информации (правила безопасной эксплуатации)



Контрольные примеры настройки СЗИ

Эксплуатационная документация СЗИ

Описание архитектуры

Ведомость ЭД



5 шагов к обеспечению безопасности значимых объектов КИИ

- 1 Установление требований к обеспечению безопасности значимого объекта (ЗО)
- 2 Разработка организационных и технических мер по обеспечению безопасности ЗОКИИ
- 3 Внедрение организационных и технических мер по обеспечению безопасности ЗО и ввод его в действие
- 4 Обеспечение безопасности значимого объекта в ходе его эксплуатации
- 5 Обеспечение безопасности значимого объекта при выводе его из эксплуатации



3

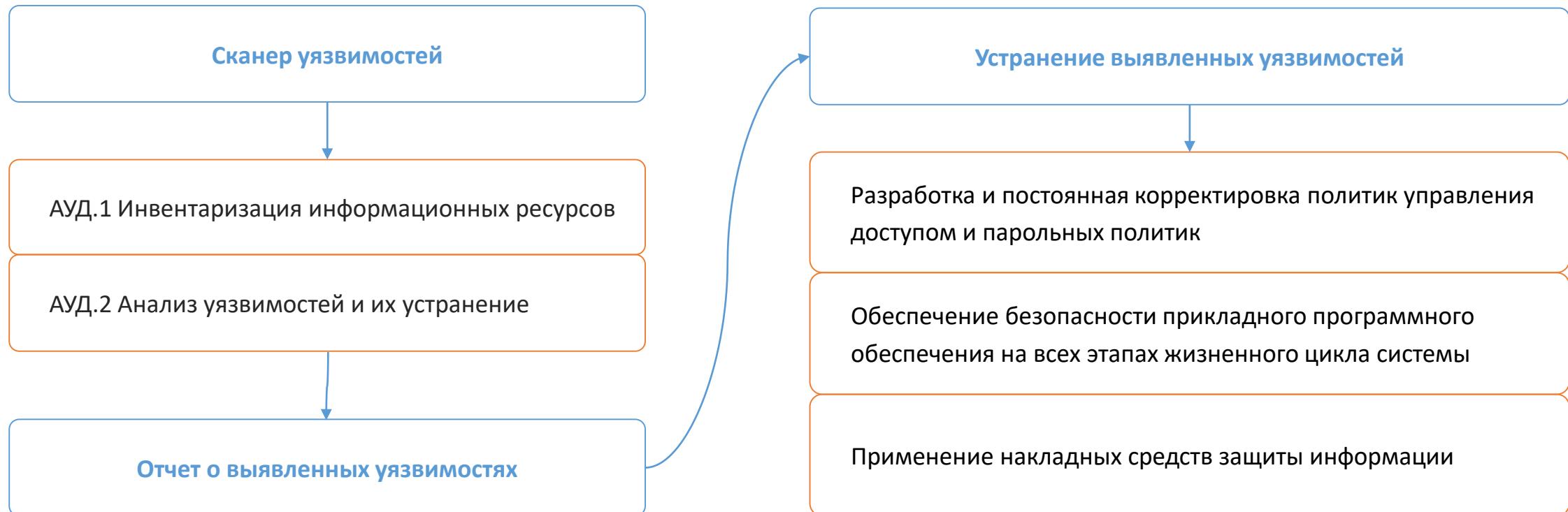
Внедрение организационных и технических мер по обеспечению безопасности ЗО и ввод его в действие

1. Установка и настройка средств защиты информации, настройка программных и программно-аппаратных средств
2. Разработка организационно-распорядительных документов, регламентирующих правила и процедуры обеспечения безопасности значимого объекта
3. Внедрение организационных мер по обеспечению безопасности значимого объекта
4. Предварительные испытания значимого объекта и его подсистемы безопасности
5. Опытная эксплуатация значимого объекта и его подсистемы безопасности
6. Анализ уязвимостей значимого объекта и принятие мер по их устранению
7. Приемочные испытания значимого объекта и его подсистемы безопасности

3

Внедрение организационных и технических мер по обеспечению безопасности ЗО и ввод его в действие

Анализ уязвимостей и их устранение



3

Внедрение организационных и технических мер по обеспечению безопасности ЗО и ввод его в действие

Ввод в эксплуатацию



Ввод в эксплуатацию значимого объекта и его подсистемы безопасности осуществляется при положительном заключении (выводе) в акте приемки (или в аттестате соответствия) о соответствии значимого объекта установленным требованиям по обеспечению безопасности.

! Форма оценки - аттестация **по желанию**

5 шагов к обеспечению безопасности значимых объектов КИИ

- 1 Установление требований к обеспечению безопасности значимого объекта (ЗО)
- 2 Разработка организационных и технических мер по обеспечению безопасности ЗОКИИ
- 3 Внедрение организационных и технических мер по обеспечению безопасности ЗО и ввод его в действие
- 4 Обеспечение безопасности значимого объекта в ходе его эксплуатации
- 5 Обеспечение безопасности значимого объекта при выводе его из эксплуатации



4

Обеспечение безопасности значимого объекта в ходе его эксплуатации

1. Планирование мероприятий по обеспечению безопасности значимого объекта
2. Анализ угроз безопасности информации в значимом объекте и последствий от их реализации
3. Управление (администрирование) подсистемой безопасности значимого объекта
4. Управление конфигурацией значимого объекта и его подсистемой безопасности
5. Реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта
6. Обеспечение действий в нештатных ситуациях в ходе эксплуатации значимого объекта
7. Информирование и обучение персонала значимого объекта
8. Контроль за обеспечением безопасности значимого объекта

4

Обеспечение безопасности значимого объекта в ходе его эксплуатации

! Ежегодно составляется план мероприятий по обеспечению безопасности и обеспечивается его реализация

В план мероприятий включаются мероприятия по обеспечению функционирования системы безопасности, а также организационные и технические мероприятия по обеспечению безопасности ЗОКИИ

! Осуществляется внутренний или внешний контроль эффективности реализованных мер

Контроль проводится комиссией или организацией, имеющей соответствующую лицензию на деятельность по защите информации. Контроль проводится не реже, чем раз в 3 года

! Осуществляется совершенствование системы безопасности

По результатам анализа функционирования системы безопасности и ЗОКИИ разрабатываются предложения по совершенствованию системы безопасности. Мероприятия включаются в ежегодный план мероприятий по обеспечению безопасности ЗОКИИ.

5 шагов к обеспечению безопасности значимых объектов КИИ

- 1 Установление требований к обеспечению безопасности значимого объекта (ЗО)
- 2 Разработка организационных и технических мер по обеспечению безопасности ЗОКИИ
- 3 Внедрение организационных и технических мер по обеспечению безопасности ЗО и ввод его в действие
- 4 Обеспечение безопасности значимого объекта в ходе его эксплуатации
- 5 Обеспечение безопасности значимого объекта при выводе его из эксплуатации



5

Обеспечение безопасности значимого объекта при выводе его из эксплуатации

1. Архивирование информации, содержащейся в значимом объекте
2. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации
3. Уничтожение или архивирование данных об архитектуре и конфигурации значимого объекта
4. Архивирование или уничтожение эксплуатационной документации на значимый объект и его подсистему безопасности и организационно-распорядительных документов по безопасности значимого объекта

3 этапа соблюдения ФЗ



1. Категорирование объектов критической информационной инфраструктуры



2. Обеспечение безопасности значимых объектов КИИ

3. Подключение значимых объектов КИИ к государственной системе обнаружения и ликвидации последствий компьютерных атак



Что такое ЦМ и для чего он нужен?

Основная задача ЦМ - это обеспечение реагирования на инциденты

информационной безопасности

Что дает заказчику подключение к ЦМ?

1. Обеспечение реагирования на инциденты ИБ
2. Непрерывный контроль за безопасностью организации
3. Сведения о вторжениях и киберугрозах хранят и обрабатывают централизованно
4. Одновременно подразделения организации совместно решают вопросы безопасности
5. Сокращаются риски для организации
6. Снижаются затраты на кибербезопасность



Задачи центра мониторинга

- 1 Выполнять мониторинг, искать и анализировать вторжения в режиме реального времени
- 2 Предотвращать киберугрозы
- 3 Быстро реагировать на подтвержденные инциденты и исключать ложные срабатывания
- 4 Анализировать большие объемы данных



Виды центров мониторинга



Внутренний
(ведомственный) SOC



Внешний
(корпоративный) SOC



Гибридная модель

Режимы работы

1

24 часа в сутки

7 дней в неделю

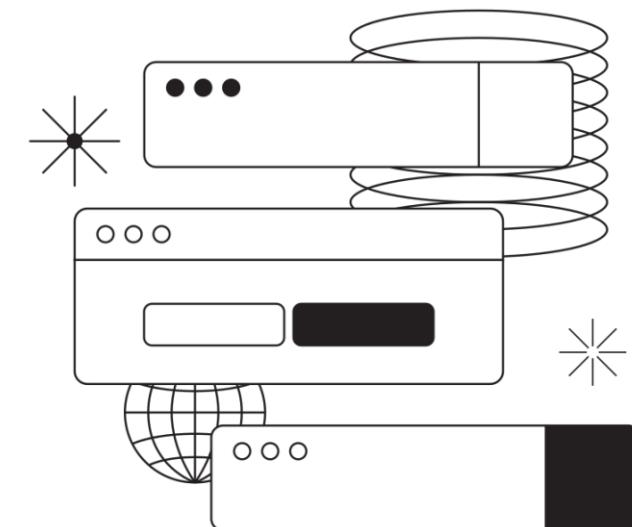
365 дней в году

2

8 часов в сутки

5 дней в неделю

247 дней в году



Подключение к ЦМ Калуга Астрал

1. Заключить договор с АО «Калуга Астрал»
2. Уведомить НКЦКИ о включении своих информационных ресурсов в зону ответственности корпоративного центра мониторинга информационной безопасности АО «Калуга Астрал»
3. Все требуемые лицензии, соглашение с НКЦКИ и штат сотрудников имеются в наличии у АО «Калуга Астрал»

Преимущества

- + Нехватка, отсутствие или загруженность собственного персонала для сбора и анализа данных
- + Быстрый старт
- + Выполнение организационных и технических требований
- + Понятные и прогнозируемые затраты

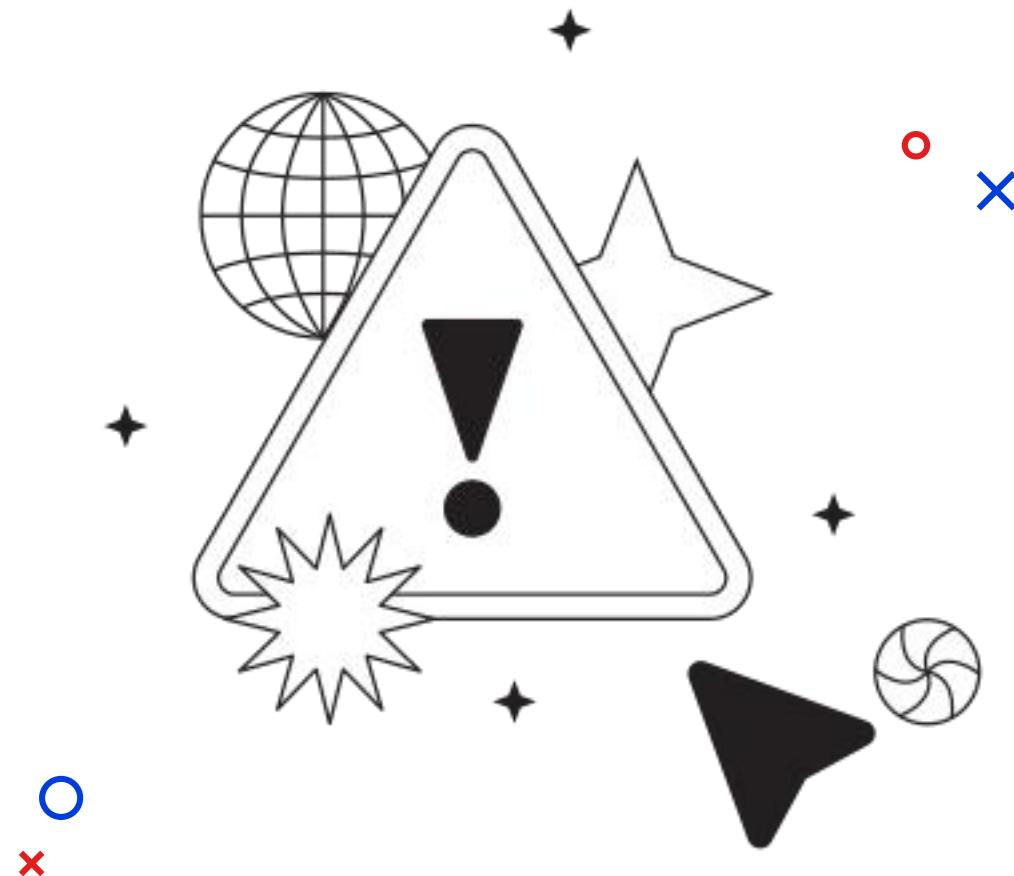
1

Административная ответственность

2

Уголовная ответственность

Ответственность



1

Административная ответственность

2

Уголовная ответственность

№	Нарушение	Штраф для должностных лиц, руб.	Штраф для юридических лиц, руб.
1	Непредставление или нарушение сроков предоставления в ФСТЭК России сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий	10 000 - 50 000	50 000 - 100 000
2	Нарушение требований к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования либо требований по обеспечению безопасности значимых объектов КИИ	10 000 - 50 000	50 000 - 100 000
3	Штраф за непредставление или нарушение сроков предоставления в ФСТЭК России сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий	10 000 - 50 000	50 000 - 100 000
4	Штраф за нарушение требований к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования либо требований по обеспечению безопасности значимых объектов КИИ	10 000 - 50 000	50 000 - 100 000
5	Штраф за нарушение порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ	10 000 - 50 000	100 000 - 500 000
6	Штраф за нарушение порядка обмена информацией о компьютерных инцидентах между субъектами КИИ, между субъектами КИИ и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты	20 000 - 50 000	100 000 - 500 000

1

Административная ответственность

2

Уголовная ответственность

Статья	Содержание	Наказание	Срок давности	Тип объектов КИИ
УК РФ ст. 274.1 ч. 1	Создание, распространение и (или) использование ПО или иной компьютерной информации для неправомерного воздействия на КИИ	Принудительные работы до 5 лет / лишение свободы до 5 лет / штраф до 1 миллиона рублей	10 лет	Все
УК РФ ст. 274.1 ч. 2	Неправомерный доступ к информации КИИ, если он повлёк вред	Принудительные работы до 5 лет / лишение свободы до 6 лет / штраф до 1 миллиона рублей	10 лет	Все
УК РФ ст. 274.1 ч. 3	Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой законом информации КИИ либо правил доступа, если оно повлекло причинение вреда для КИИ	Принудительные работы до 5 лет / лишение свободы до 6 лет / запрет занимать должности до 3 лет	10 лет	Все
УК РФ ст. 274.1 ч. 4	Деяния, предусмотренные частью 1, 2 или 3, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения	Лишение свободы на срок до 8 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового.	10 лет	Все
УК РФ ст. 274.1 ч. 5	Деяния, предусмотренные частью 1, 2, 3 или 4, если они повлекли тяжкие последствия	Лишение свободы на срок до 10 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет или без такового	10 лет	Все

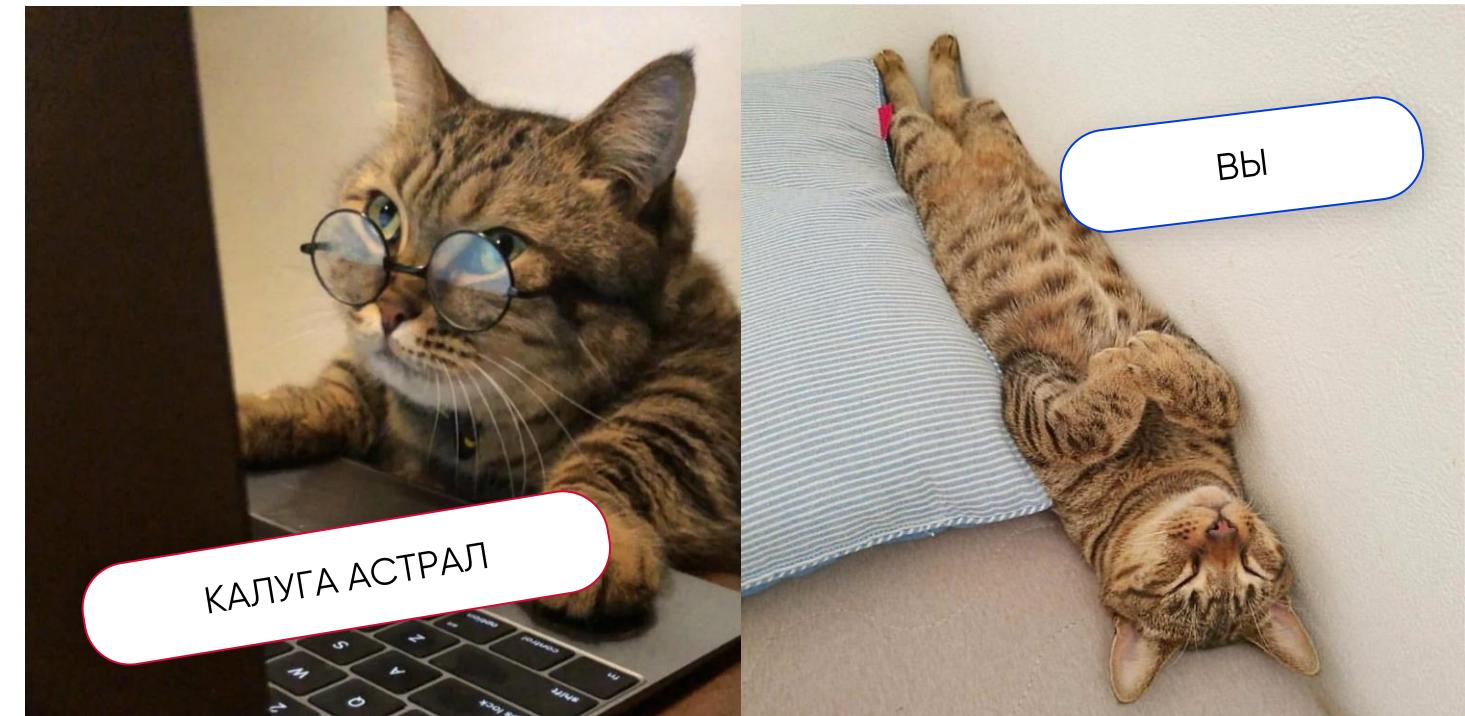
Наши контакты:

is@astral.ru

[+7 \(4842\) 788-999, доб. 60](tel:+74842788999)

is.astral.ru

**Будем рады ответить
на все Ваши вопросы!**



Будьте в курсе последних новостей



is.astral.ru



vk.com/is.astral



t.me/is_astral

