УЦСБ ИНТЕГРАТОР СИЛЬНЫХ РЕШЕНИЙ

Дорожная карта по проведению мероприятий в рамках 187-ФЗ

Константин Саматов

Руководитель направления в Аналитическом центре Уральского центра систем безопасности

Федеральный закон от 26.07.2017 **N 187-ФЗ**

«О безопасности **критической информационной инфраструктуры** Российской Федерации»

Вступил в силу **1 января 2018 года**.

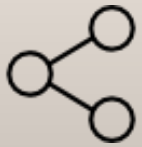
> Критическая информационная инфраструктура **(КИИ)** - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов
>
> ст. 2 187-ФЗ

ОБЪЕКТ КИИ?

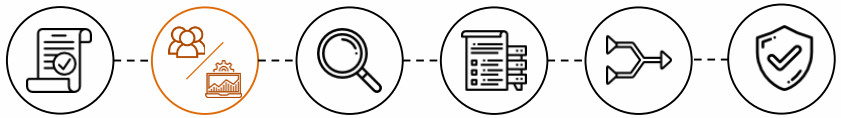
Объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления **субъектов** критической информационной инфраструктуры

ИНФОРМАЦИОННЫЕ СИСТЕМЫ (ИС)

ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ (ИТКС)



АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ (АСУ (ТП))



СУБЪЕКТ КИИ?

Субъекты КИИ – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании **принадлежат** информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, **функционирующие в сферах…** или индивидуальные предприниматели, которые обеспечивают **взаимодействие** указанных систем или сетей.

Здравоохранение	Банковская сфера	Ракетно-космическая промышленность	
Наука	Топливно-энергетический комплекс	Горно-добывающая промышленность	Энергетика
Транспорт	Атомная энергия	Металлургическая промышленность	Финансовые рынки
Связь	Оборонная промышленность	Химическая промышленность	

ШАГ 1: Организация является субъектом КИИ?

Определение функций или видов деятельности → Перечень Видов деятельности

↓

Определение ИС, АСУ, ИТКС принадлежащих организации на праве собственности, аренды, ином законном основании

↓

Определение ИС, АСУ, ИТКС функционирующих в одной из перечисленных в законе сфер → Сведения об объектах КИИ (перечень объектов КИИ)

ШАГ 2: Провести категорирование КИИ

Постановление правительства РФ

от 8 февраля 2018 г. №127

Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации…

- Порядок категорирования
- Сроки категорирования
- Перечень показателей критериев значимости объектов КИИ

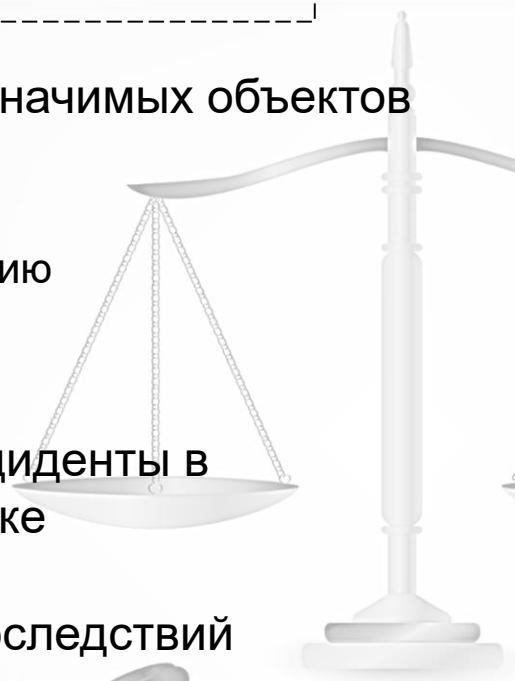
Развилка: Есть ли значимые объекты?

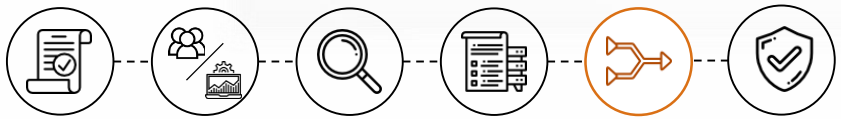
ЗНАЧИМЫЕ ОБЪЕКТЫ ЕСТЬ

- Создание системы безопасности значимых объектов КИИ
- Выполнение требований по обеспечению безопасности значимых объектов КИИ
- Реагировать на компьютерные инциденты в установленном ФСБ России порядке
- Принимать меры по ликвидации последствий компьютерных атак
- Обеспечивать беспрепятственный доступ должностным лицам ФСТЭК России к значимым объектам КИИ

ЗНАЧИМЫХ ОБЪЕКТОВ НЕТ

- Информировать о компьютерных инцидентах ФСБ России
- Оказывать содействие должностным лицам ФСБ России
- Выполнять порядок и тхенические условия в случае взаимодействия с ГосСОПКА





ШАГ 3: Безопасность значимых объектов

Приказ ФСТЭК России №235

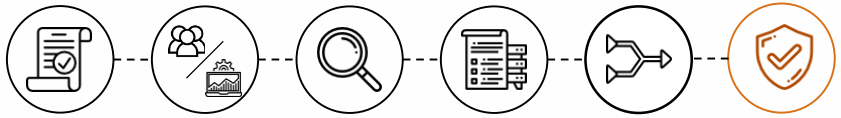
от 21 декабря 2017 г.

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

Приказ ФСТЭК России N239

от 25 декабря 2017 г.

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



Шаг 3.1: Силы обеспечения безопасности значимых объектов

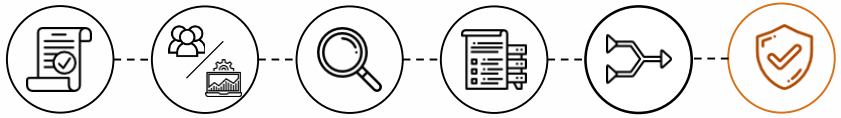
Подразделения (работники), ответственные за обеспечение безопасности значимых объектов КИИ (структурное подразделение по безопасности, специалисты по безопасности)

Подразделения (работники), эксплуатирующие значимые объекты КИИ

Подразделения (работники), обеспечивающие функционирование (сопровождение, обслуживание, ремонт) значимых объектов КИИ

Подразделения (работники), участвующие в обеспечении безопасности значимых объектов КИИ

До 1 сентября 2019 года создание (совершенствование) систем безопасности и назначение **ответственного** за **организацию и контроль** обеспечения безопасности значимых объектов КИИ, создание (назначение) **структурного подразделения**, ответственного за **обеспечение безопасности** значимых объектов КИИ, а также **разработку** организационно – распорядительных документов по вопросам обеспечения безопасности КИИ



Шаг 3.2: Моделирование угроз

- Выявление источников угроз безопасности информации и оценка возможностей (потенциала) внешних и внутренних нарушителей
- Анализ возможных уязвимостей значимого объекта и его программных, программно-аппаратных средств
- Определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации
- **Оценка возможных последствий** от реализации (возникновения) угроз безопасности информации.

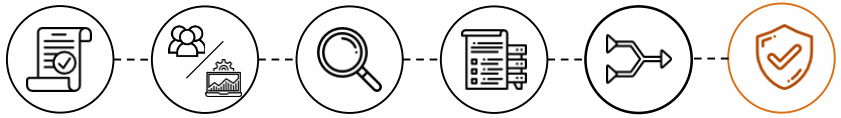
ШАГ 3.3: Требования и подсистемам безопасности

ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КИИ

- Определение требований осуществляется в соответствии с категорией значимости
- Задание требований осуществляется субъектом критической информационной инфраструктуры и (или) лицом, устанавливающим требования к обеспечению безопасности объектов
- Требования включаются в **Техническое задание** на создание подсистемы безопасности значимых объектов КИИ

ПОДСИСТЕМА БЕЗОПАСНОСТИ

- **Технический проект** по созданию подсистемы безопасности значимых объектов КИИ



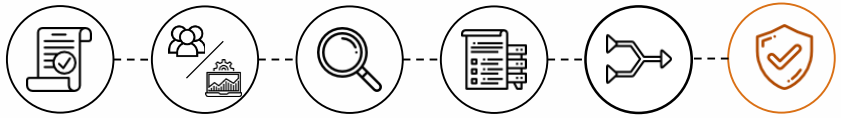
ШАГ 3.4: Организационные меры и подсистемам безопасности

ОРГАНИЗАЦИОННЫЕ МЕРЫ

- Внедрение организационных мер по обеспечению безопасности значимых объектов КИИ
- Организационно-распорядительные **документы**

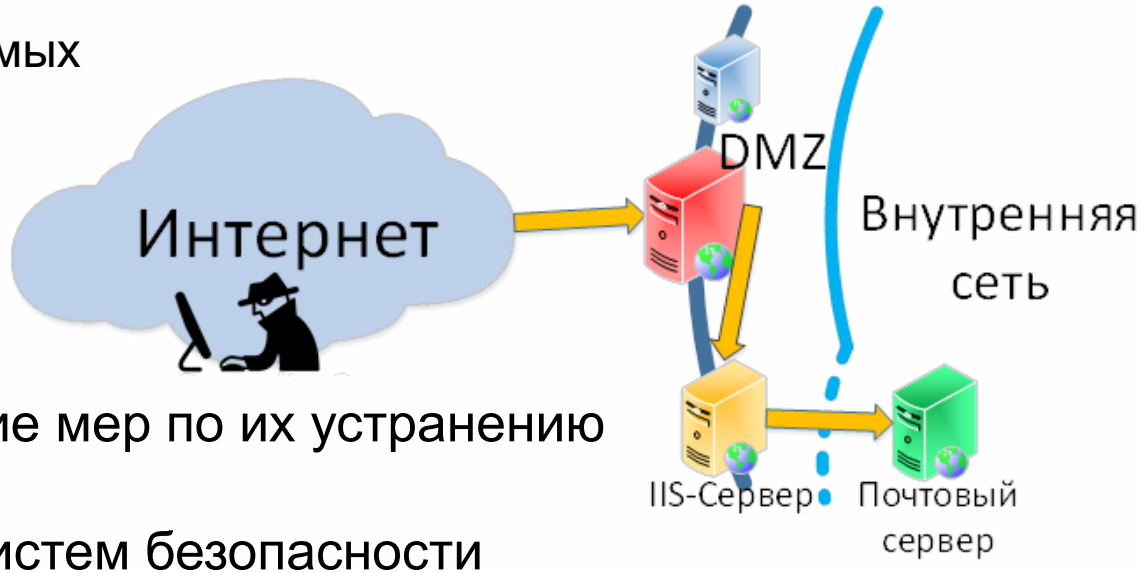
ПОДСИСТЕМА БЕЗОПАСНОСТИ

- Разработать Рабочую (эксплуатационную) **документацию** на подсистему безопасности значимых объектов КИИ



ШАГ 3.5: Подсистема безопасности

Ввод **в действие** подсистемы безопасности значимых объектов КИИ



- установка и настройка СрЗИ
- предварительные испытания
- опытная эксплуатация
- выявление уязвимостей объектов и принятие мер по их устранению (Penetration Test)
- приемочные испытания объектов и их подсистем безопасности

Акты установки СрЗИ, программы и методики испытаний, протокол испытаний, акты по результатам испытаний, отчет по результатам сканирования значимых объектов КИИ на наличие уязвимостей

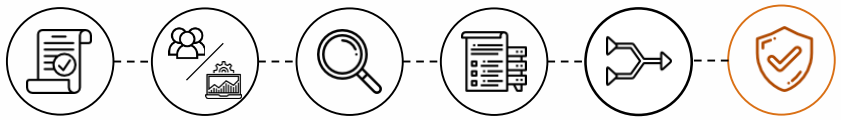
ШАГ 4 (?): КСУИБ

Рекомендуется создать Корпоративную систему управления ИБ (КСУИБ)

ШАГ 5: Эксплуатация и вывод из неё объектов КИИ

- Обеспечение **безопасности в ходе эксплуатации** значимого объекта осуществляется субъектом КИИ в соответствии с эксплуатационной документацией и документами по безопасности значимого объекта

- Обеспечение **безопасности** значимого объекта **при выводе** его из эксплуатации осуществляется в соответствии с эксплуатационной документацией на значимый объект и документами по безопасности значимого объекта

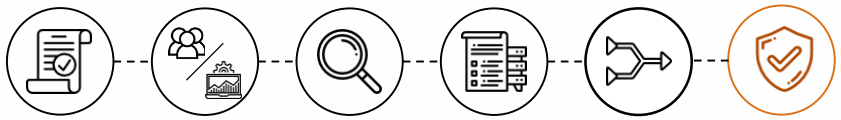


ШАГ (6?): ГосСОПКА

- В случае использования средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, **обеспечивается** их **интеграция** с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (**ГосСОПКА**)

↑ Для объектов КИИ **2 и 1 категории** значимости использование таких средств ОБЯЗАТЕЛЬНО

- Интеграция с ГосСОПКА возможна:
— в виде иерархической системы с централизованным подключением к ГосСОПКА;
— в виде отдельного подключения к ГосСОПКА.



ДОРОЖНАЯ КАРТА

ПЛАН ДЕЙСТВИЙ

- Категорирование объектов КИИ
- Значимые объекты ЕСТЬ
- Безопасность в ходе эксплуатации
- Безопасность при выводе из эксплуатации

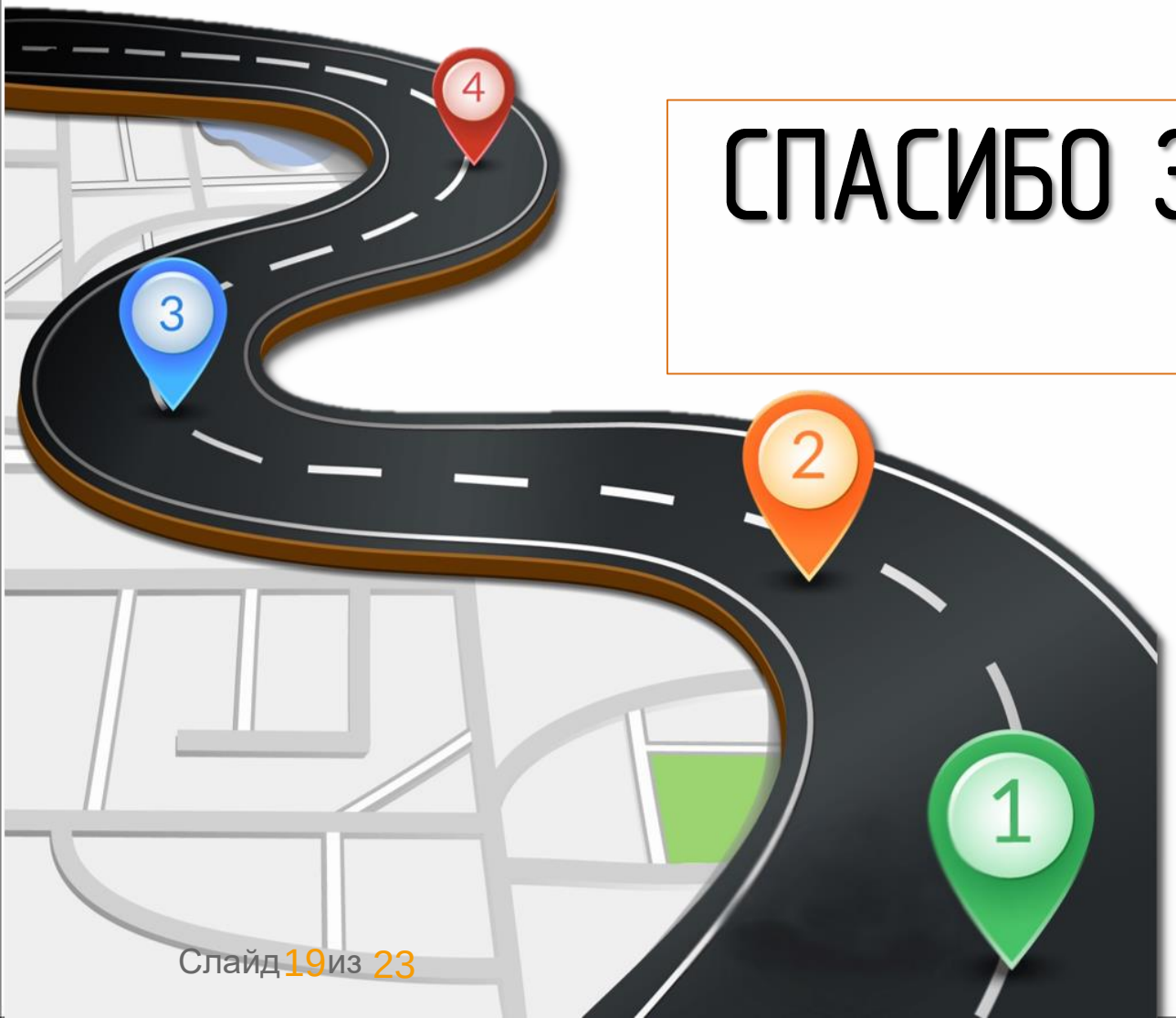
Комиссия → Перечень объектов КИИ → Категорирование → Ответственные за безопасность

Моделирование угроз

Формулировка требований к обеспечению безопасности → Принятие организационных мер (Организационно-распорядительные документы) → Корпоративная система управления ИБ

Проектирование подсистемы безопасности → Формирование рабочей документации → Ввод в действие подсистемы безопасности

ГосСОПКА



СПАСИБО ЗА ВНИМАНИЕ!