187-ФЗ Безопасность КИИ

Максим Прохоров
Специалист по защите критической инфраструктуры

Maxim.Prokhorov@softline.com

Регуляторы

ФСТЭК России

Методологическая функция, надзор выполнения требований

Минкомсвязь России

Банк России (ЦБ РФ)

Отраслевое согласование требований к защите информации

ФСБ России

Техническая функция, надзор за реализацией технических мер, ГосСОПКА

Ответственность

УК РФ
Ст. 274.1. Неправомерное воздействие на КИИ РФ

КоАП РФ
Ст. 19.5.

до 10 лет лишения свободы

Невыполнение требований по безопасности КИИ, в случае наступления инцидента с тяжкими последствиями или их угрозой

до 6 лет лишения свободы

Невыполнение требований по безопасности КИИ, нарушение правил эксплуатации

до 5 лет лишением права занимать определенные должности

ч. 3,4,5 ст. 274.1 УК РФ

до 20 000 административный штраф

Невыполнение предписания регулятора об устранении нарушения законодательства

+ Проект ФЗ «О внесении изменений в КоАП РФ»

Ответственность возлагается на должностных лиц субъекта КИИ:

- Руководитель субъекта КИИ
- Уполномоченное лицо
- Лица, эксплуатирующие значимые объекты
- Лица, обеспечивающие функционирование значимых объектов
- Лица, обеспечивающие безопасность значимых объектов

Субъекты и объекты КИИ

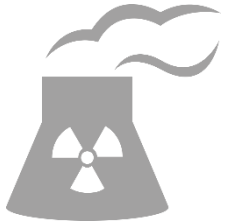
здравоохранение

наука

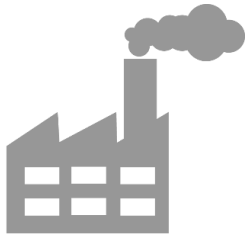
транспорт

связь

финансы и банки



атомная и топливная энергетика



промышленность (горнодобывающая, оборонная, химическая, металлургическая, ракетно-космическая)

Субъекты

- Гос. органы
- Гос. учреждения
- Российские ЮЛ и ИП

Объекты

- информационные системы
- информационно-телекоммуникационные сети
- автоматизированные системы управления

Этапы реализации требований 187-ФЗ

Категорирование объектов КИИ

ПП-127

- Инвентаризация процессов
- Определение критических процессов
- Выделение объектов КИИ
- Оценка возможных последствий (Анализ угроз)
- Сопоставление с показателями (ПП-127)
- Присвоение категории

Включение в Перечень объектов КИИ (ФСТЭК)

Безопасность значимых объектов КИИ

Приказы ФСТЭК 235, 239

- Защита от неправомерного доступа к информации, обрабатываемой объектом КИИ
- Защита от негативных воздействий, в результате которых может быть нарушено и (или) прекращено функционирование объекта КИИ
- Восстановление функционирования объектов КИИ

Создание СОИБ

Взаимодействие с ГосСОПКА

НКЦКИ

- Субъекты КИИ, у которых есть значимые объекты КИИ обязаны подключиться к ГосСОПКА

ГОССОПКА

Подготовительные работы

1. Создание комиссии по категорированию, назначение ответственных
2. Определение процессов в рамках выполнения субъектом функций
3. Выявление из них критичных процессов
4. Определение ОКИИ, связанных с критическими процессами
5. Формирование перечня ОКИИ, подлежащий категорированию

Сроки выполнения требований ФЗ-187

ПП №452
от 13 апреля 19г
О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127

утвердить
до 1 сентября 2019 г.
перечень объектов КИИ, подлежащих категорированию

Создание комиссии по категорированию

Руководитель Безопасности

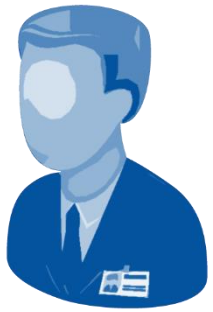
Директор

Уполномоченное лицо

Руководители критичных направлений деятельности

Руководитель подразделения ИТ

Ответственный за контроль опасными веществами

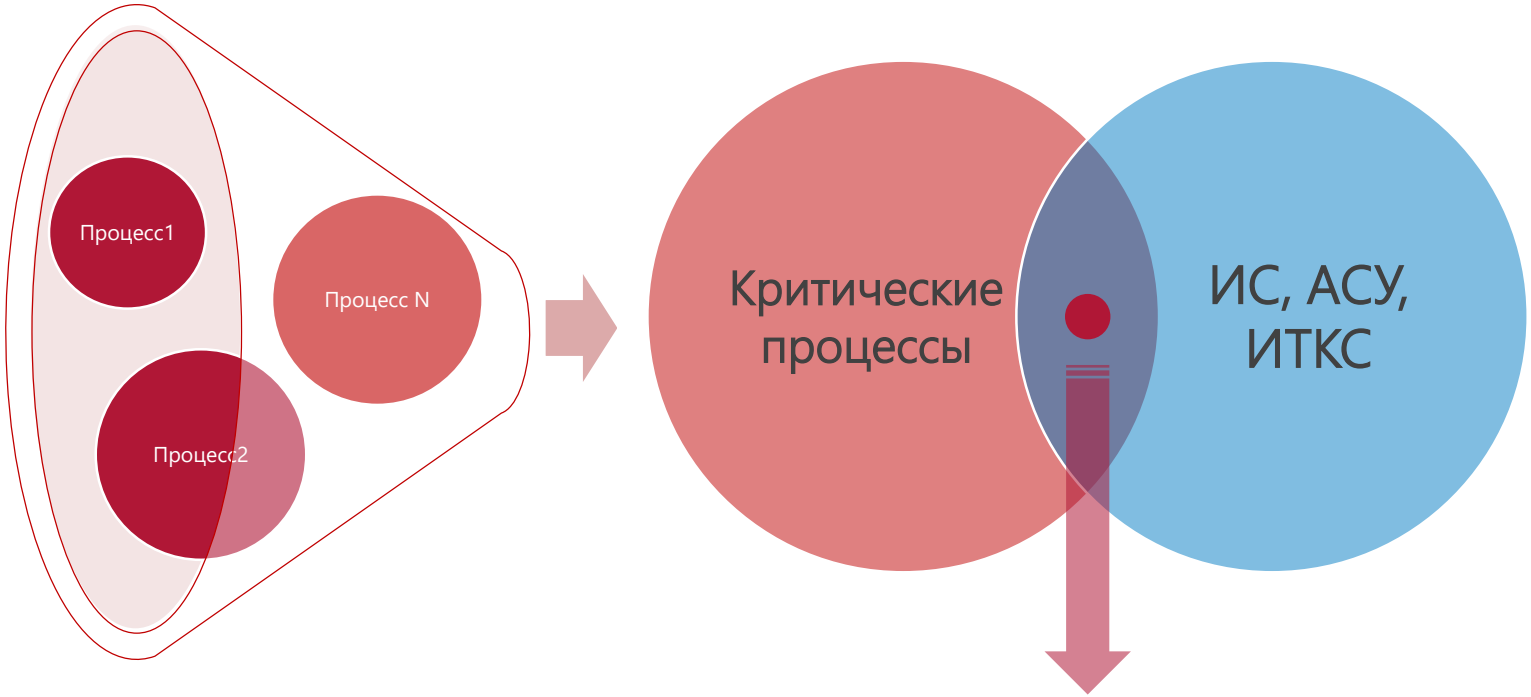


Руководители отдела автоматизации (АСУ)

Руководитель Отдела по ГОиЧС

Руководитель финансов и экономики

Формирование перечня объектов КИИ



Критические процессы

Объекты КИИ

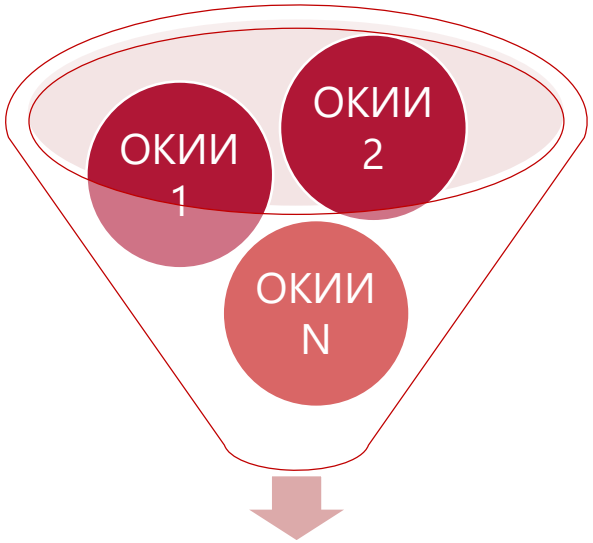
Результат:

Перечень объектов КИИ

5 дней

ФСТЭК

Категорирование объектов КИИ



Значимые объекты

1 2 3 кат.

Показатели критериев ПП-127

- Социальная
- Политическая
- Экономическая
- Экологическая
- Обеспечение обороны

Результат:

Акт категорирования

\+

Модели угроз и нарушителя

Оформление результатов

Отчетная документация

- Акты критических процессов
- Акты категорирования ОКИИ
- Методика обследования;
- Отчет об обследовании ОКИИ
- Частные модели угроз,
- Техническое задание СОИБ
- Частные ТЗ на разработку подсистем безопасности ЗОКИИ

Форма Пр.№236

10 дней на отправку

10 дней на устранение

10 дней

30 дней на проверку сведений

ФСТЭК

Результат:

Решение о внесении в Реестр

Форма:

Бумажный и электронный вид

Комплексный подход к безопасности КИИ

Управление и планирование

- ✓ Построение КСУИБ
- ✓ Ежегодный план
- ✓ Регулярный пересмотр категории (1 раз в 5 лет)

Экспертиза

- ✓ Технический проект СОИБ
- ✓ Программа и методика приемочных испытаний
- ✓ Акт приемки СОИБ
- ✓ Пакет ОРД по обеспечению ИБ

Учебный центр Softline

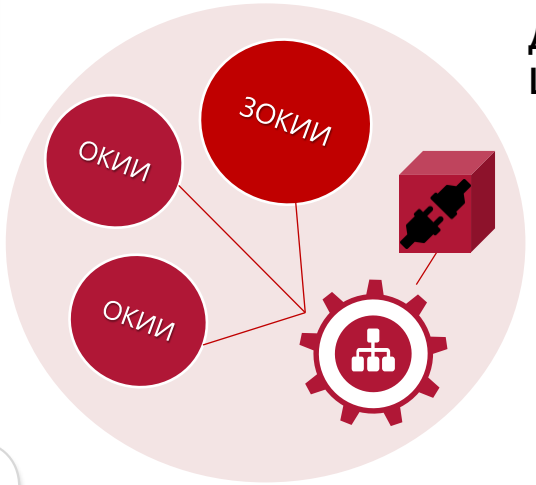
- ✓ Программа повышения квалификации: «Обеспечение безопасности значимых объектов КИИ и АСУ ТП»

Опыт реализации

- ✓ Реализация СОИБ
- ✓ Поддержка решений
- ✓ Поддержка производителей

Взаимодействие с ГосСОПКА

1



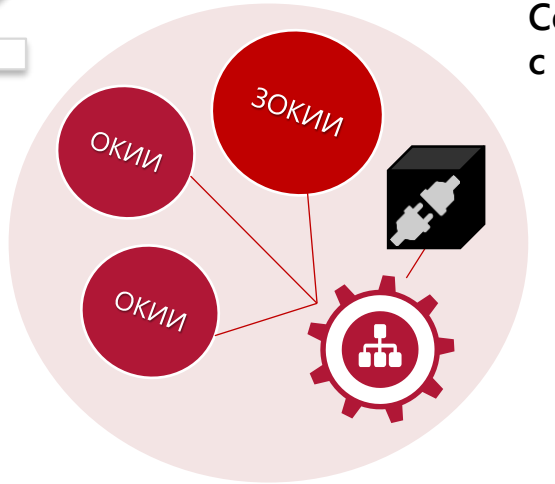
Договор с Центр “А”

Центр ГосСОПКА “А”

Соглашение с 8 ц. ФСБ

НКЦКИ

2



Соглашение с 8 ц. ФСБ

НКЦКИ

ГОССОПКА

- через тех. инфраструктуру НКЦКИ (.json)

  ОБЯЗАТЕЛЬНО!!! для значимых ОКИИ

- через портал НКЦКИ (ЛК субъекта ГосСОПКА)

- E-mail,
- Почта,
- Факс,
- Телефон

«Обеспечение безопасности значимых объектов КИИ и АСУТП»

Программа повышения квалификации

2019

edu.softline.ru
edusales@softline.ru
8 800 505 05 07

Программа повышения квалификации «Обеспечение безопасности значимых объектов КИИ и АСУТП»

- **Продолжительность обучения:** 24 часа (3 дня)
- **Аудитория:** руководители служб и подразделений в сфере информационно-коммуникационных технологий, руководители отделов систем защиты информации, специалисты по защите информации, инженеры автоматизированных систем управления
- **Формат:** очный / дистанционный

- ✓ Программа удовлетворяет требованиям: профессионального стандарта
- ✓ 30% лекций и 70% практики.
- ✓ Удостоверение о повышении квалификации.

Программа курса

Модули:

1. Введение в тему КИИ. Термины и определения. Основная проблематика
2. Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры
3. Классификация АСУ ТП: требования, параметры, сроки. Категорирование объектов критической информационной инфраструктуры
4. Права и обязанности субъектов критической информационной инфраструктуры
5. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры
6. Разработка организационных и технических мер (рекомендации и требования ФСТЭК и ФСБ)
7. Разработка модели угроз
8. Выбор мер защиты объекта информатизации
9. Формирование технического проекта. Разработка эксплуатационной документации

Узнать цены и записаться

edu.softline.ru

8 800 505 05 07

edusales@softline.ru


GO GLOBAL
GO CLOUD
GO INNOVATIVE