

187-ФЗ

Безопасность КИИ

Максим Прохоров

Специалист по защите критической
инфраструктуры

Maxim.Prokhorov@softline.com



История появления 187-ФЗ



Регуляторы



ФСТЭК России

Методологическая функция, надзор выполнения требований



ФСБ России

Техническая функция, надзор за реализацией технических мер, ГосСОПКА



Минкомсвязь России



Банк России (ЦБ РФ)

Отраслевое согласование требований к защите информации

Ответственность



УК РФ

Ст. 274.1. Неправомерное воздействие на КИИ РФ



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

КоАП РФ

Ст. 19.5.



до 20 000
административный
штраф

Невыполнение предписания регулятора об устранении нарушения законодательства

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



СУБЪЕКТЫ КИИ

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

ОБЪЕКТЫ КИИ

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

ОТРАСЛИ КИИ

- здравоохранения;
- науки;
- транспорта;
- связи;
- энергетики;
- банковской сфере и иных сферах финансового рынка;
- топливно-энергетического комплекса;
- атомной энергетики;
- оборонной промышленности;
- ракетно-космической;
- горнодобывающей;
- металлургической промышленности;
- химической промышленности.

Мероприятия по обеспечению требований 187-ФЗ

Провести
категорирование
объекта КИИ

ПП-127

- Инвентаризация всех процессов
- Критические процессы
- Объекты КИИ
- Оценка возможных последствий (Анализ угроз)
- Сопоставление с показателями
- Присвоение категории

3 КАТЕГОРИИ ЗНАЧИМОСТИ

Обеспечить безопасность
значимых объекта КИИ

Приказы ФСТЭК 235, 239

- Защита от неправомерного доступа к информации, обрабатываемой кии
- Защита от негативных воздействий, в результате которых может быть нарушено и (или) прекращено функционирование объекта КИИ
- Восстановление функционирования объекты КИИ
- Непрерывное взаимодействие с ГосСОПКА

Обеспечить взаимодействие
объекта КИИ с ГосСОПКА

НКЦКИ

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



Временные ограничения по выполнению требований ФЗ-187

Решение Коллегии ФСТЭК России от 24.04.18г. №59

Перечень объектов КИИ и их границы определяет сам субъект!

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)

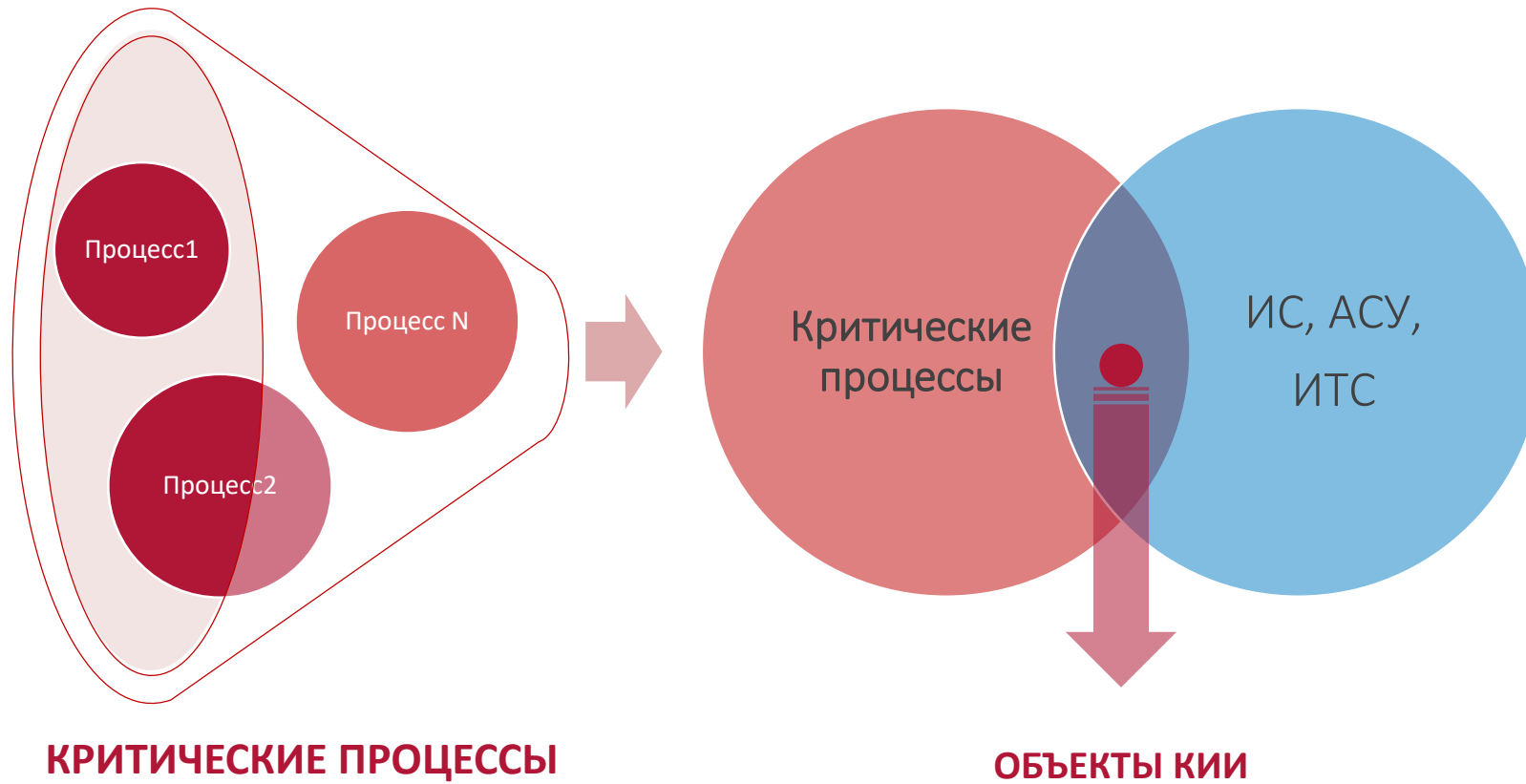


Руководитель Отдела по ГОиЧС



Руководитель финансов и экономики

Формирование перечня объектов КИИ



РЕЗУЛЬТАТ:



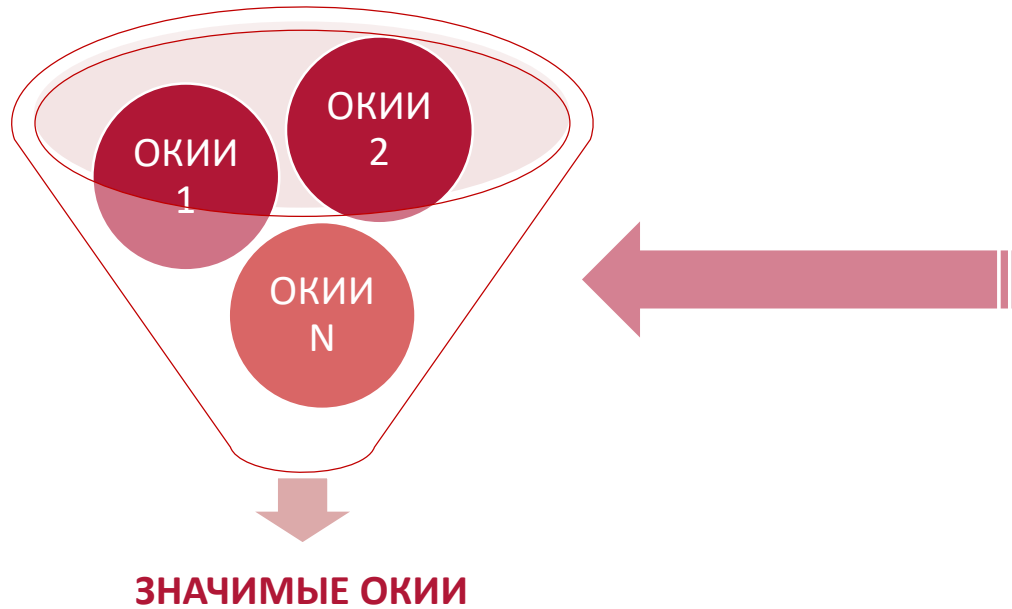
Перечень
объектов
КИИ

5 дней



ФСТЭК

Категорирование объектов КИИ



3 КАТЕГОРИИ ЗНАЧИМОСТИ

Показатели критериев ПП-127

Социальная

Политическая

Экономическая

Экологическая

Обеспечение обороны

РЕЗУЛЬТАТ:



Акт

Категорирования + Форма направления во ФСТЭК

+



Модели угроз и Модели нарушителя/Идентификация ключевых угроз

Требования ФСТЭК приказ №235

Управление

- ✓ Построение КСУИБ
- ✓ Регулярный пересмотр категории

Разработка

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



Учебный центр

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

Опыт

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

ГосСОПКА

Основным назначением ГосСОПКА является обеспечение защищенности информационных ресурсов Российской Федерации от компьютерных атак и штатного функционирования данных ресурсов в условиях возникновения компьютерных инцидентов, вызванных компьютерными атаками.

ВАЖНО ЗНАТЬ

- ГосСОПКА не ограничивается целями и задачами указанными в ФЗ-187
- Нацелена на противодействие целевым атак
- Для функционирования ГосСОПКА необходимо реализовать базовый набор средств защиты объекта КИИ



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

Наш подход

№	Работы	Результат
1.	Составление перечня объектов КИИ	Перечень объектов КИИ
2.	Анализ угроз безопасности	Модель угроз безопасности
3.	Категорирование объектов КИИ	Акт категорирования объектов КИИ
4.	Задание требований к обеспечению безопасности значимых объектов	Техническое задание на создание СОИБ
5.	Разработка организационных и технических мер по обеспечению безопасности значимых объектов	Технический проект на создание СОИБ
6.	Разработка организационно-распорядительных документов по обеспечению безопасности	Пакет организационно-распорядительных документов по обеспечению ИБ
7.	Внедрение организационных и технических мер СОИБ	Реализованная система обеспечения ИБ
8.	Приемочные испытания СОИБ	Программа и методика приемочных испытаний; Акт приемки СОИБ

«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.



Описание программы

Программа направлена на:

- формирование целостного подхода, используемого специалистами в области защиты информации, специалистами в области ИТ, ИТС и АСУ для обеспечения комплексной защищенности объектов критической информационной инфраструктуры РФ в соответствии с актуальными требованиями законов и подзаконных актов;
- подготовку и проведение категорирования объекта критической информационной инфраструктуры;
- подготовку к реализации требований в соответствии с нормативно-методическими документами, публикуемыми ФСТЭК и ФСБ России.



Стоимость и расписание

Актуальное расписание и цены на программу повышения квалификации «Обеспечение безопасности значимых объектов КИИ и АСУТП» вы найдете на сайте Учебного центра **Softline**

Ближайшие даты:

- 01 — 03 апреля 2019, Москва, очно / дистанционно



Узнать цены и
записаться

edu.softline.ru

8 800 505 05 07

edusales@softline.ru

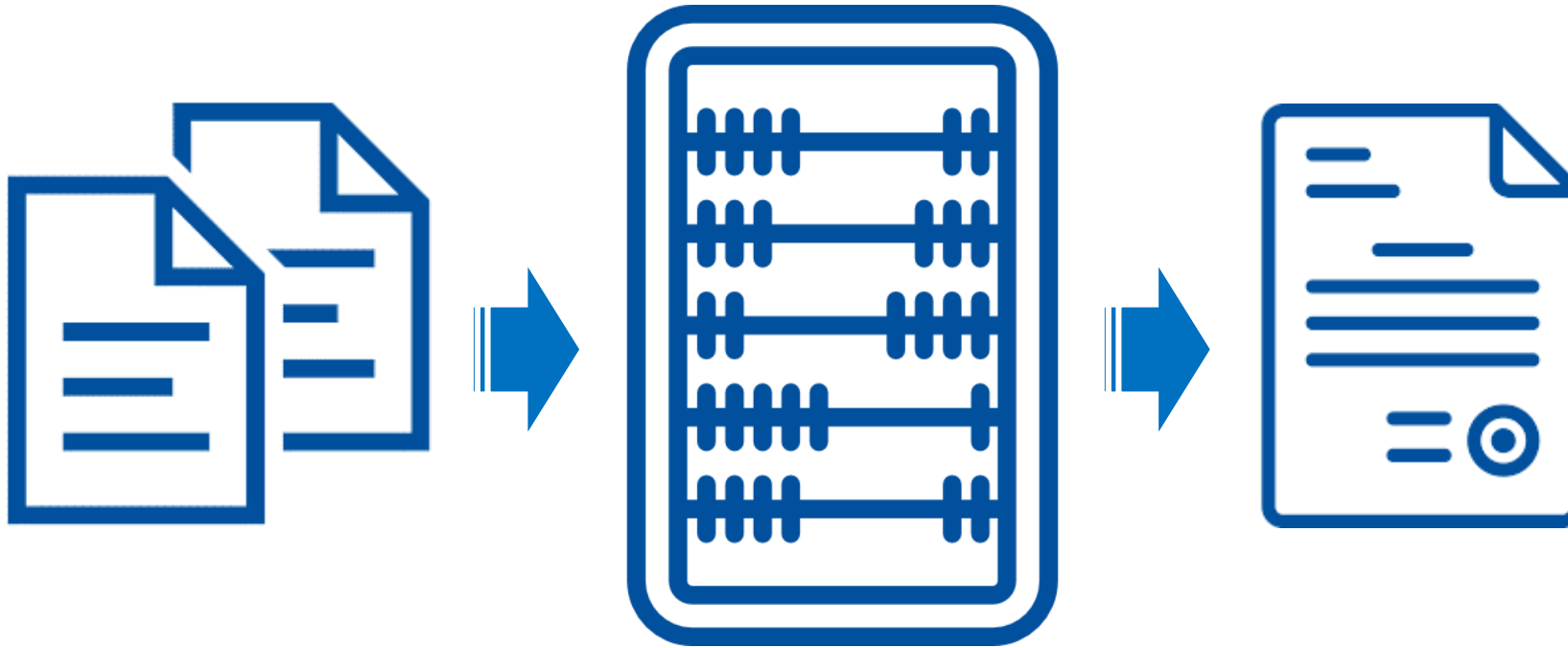
187-ФЗ Безопасность КИИ (Пакетные сервисы)

Максим Прохоров
Специалист по защите критической
инфраструктуры

Maxim.Prokhorov@softline.com



Классический расчет трудозатрат



Опросные Листы

Калькулятор

ТКП

Риски

- Вводные данные
- Реакция на запрос
- Инфраструктура заказчика
- Этапы работ
- Разработка Документов (Успешность проекта)
- Ожидания Заказчика

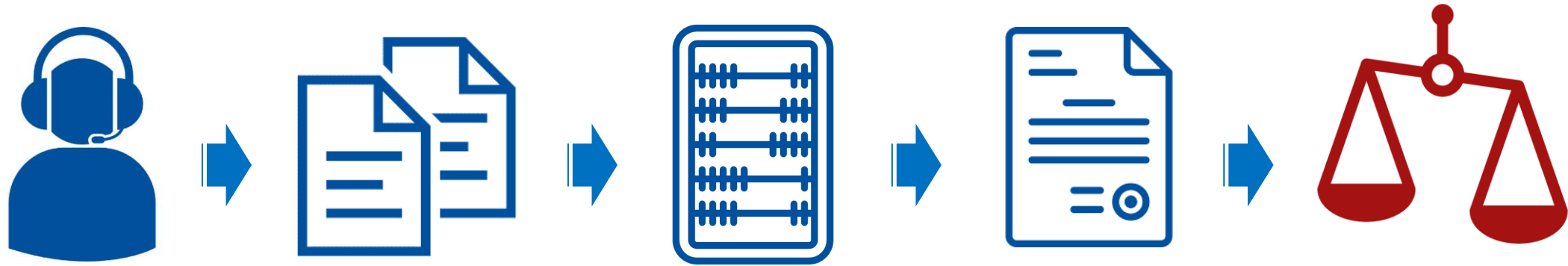
Пакетные Сервисы

	Стартовый	Базовый	Расширенный	Все включено
Объекты обследования				
Обследование информационных систем	v	v	v	v
Обследование телекоммуникационных систем	v	v	v	v
Обследование технологических сетей	-	v	v	v
Количество обследуемых площадок	1	1	1	1
Количество обследуемых ОКИИ	до 10*	11-50*	51-150**	151-300**
Длительность обследования	2-3 недели	3-4 недели	4-6 недель	2-3 месяца
Результат				
Акт о выявлении критических процессов	v	v	v	v
Акт о формировании перечня ОКИИ, подлежащих категорированию	v	v	v	v
Обучение по программе повышения квалификации				
Курс "Обеспечение безопасности значимых ОКИИ"	-	до 5 человек	до 5 человек	до 5 человек
Продолжительность обучения	-	24ч	24ч	24ч
Форма обучения	-	Дистанционная	Очная	Очная
Стоимость				
Стоимость для заказчика	350 000 ₽	700 000 ₽	1 050 000 ₽	2 100 000 ₽
Дополнительные опции:				
Заполнение формы + категорирование (за 1 ОКИИ)	28 000 ₽	23 000 ₽	21 000 ₽	20 000 ₽

* допускается превышение не более чем на 5 ОКИИ если обнаружено в рамках обследования

** допускается превышение не более чем на 10 ОКИИ если обнаружено в рамках обследования

Классический расчет трудозатрат



Пакетные Сервисы



Максим Прохоров
Специалист по защите КИ
+7 (495) 232-0023

Maxim.Prokhorov@softline.com

Учебный Центр Softline
edu.softline.ru
8 800 505 05 07

edusales@softline.ru



GO GLOBAL



GO CLOUD



GO INNOVATIVE