187-ФЗ: От теории к практике

Алексей Липатов
Эксперт по информационной безопасности в СЗФО

Alexey.Lipatov@softline.com

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 юр. лица

Объекты

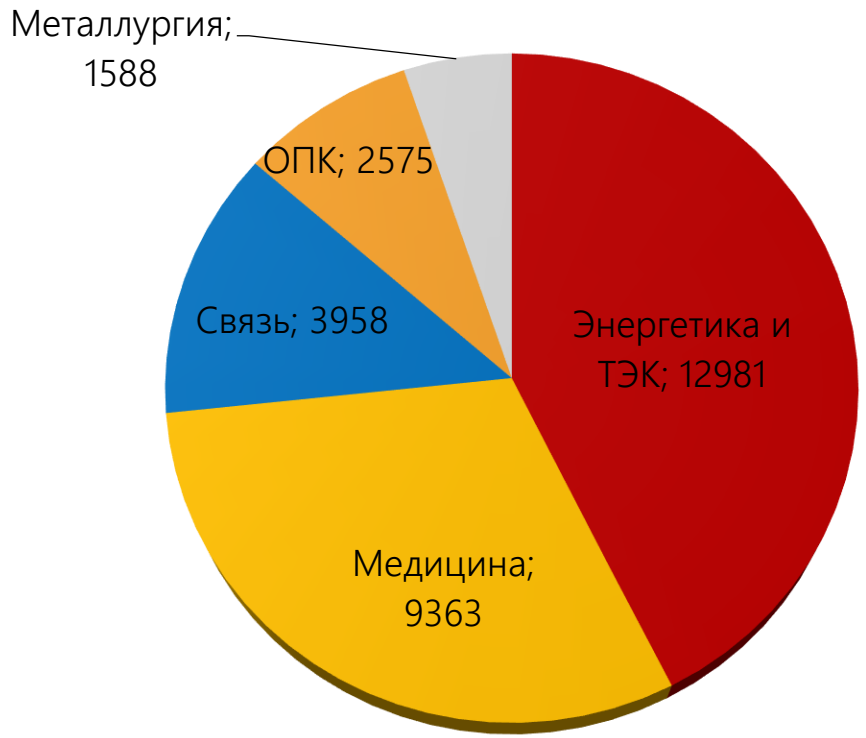
- информационные системы
- информационно-телекоммуникационные сети
- автоматизированные системы управления

Текущие результаты категорирования объектов КИИ

Во ФСТЭК России по состоянию на август 2019 г. предоставлены сведения:

1. От 3 500+ субъектов
2. По 36 000+ ОКИИ
3. О категорировании ≈ 4000 ОКИИ

ТОП-5 сфер с ОКИИ для категорирования:



Этапы реализации требований 187-ФЗ

Категорирование объектов КИИ

ПП-127

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

Включение в Перечень объектов КИИ (ФСТЭК)

Безопасность значимых объектов КИИ

Приказы ФСТЭК № 235, 239

- Силы обеспечения безопасности ОКИИ
- Средства обеспечения безопасности ОКИИ
- Документы по безопасности ОКИИ
- Процессы обеспечения безопасности ОКИИ

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 ОКИИ, связанных с критическими процессами
3. Формирование перечня ОКИИ, подлежащий категорированию

Сроки выполнения требований ФЗ-187

ПП № 452
от 13.04.2019
«О внесении изменений в постановление Правительства Российской Федерации от 8.02.2018 № 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

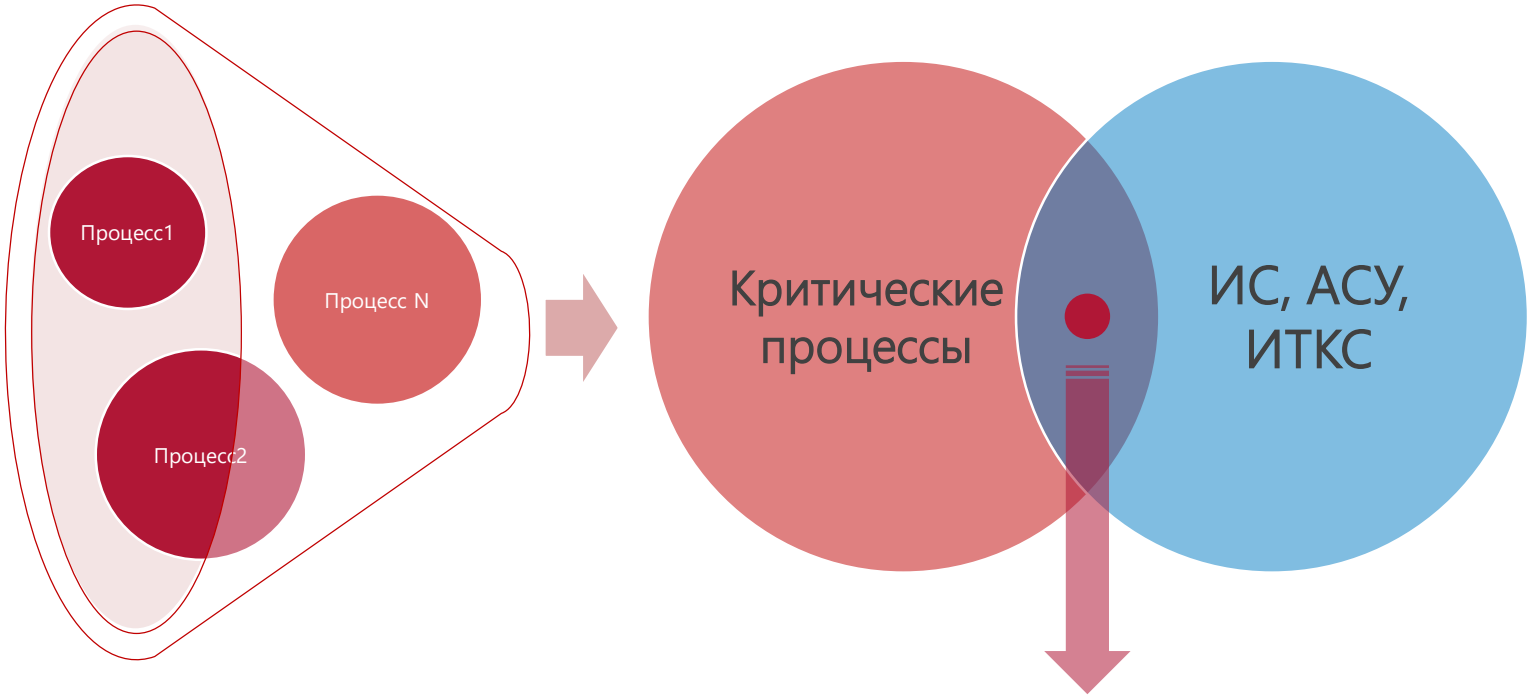
Ответственный за контроль опасными веществами

Руководители отдела автоматизации (АСУ)

Руководитель Отдела по ГОиЧС

Руководитель финансов и экономики

Формирование перечня объектов КИИ



Критические процессы

Объекты КИИ

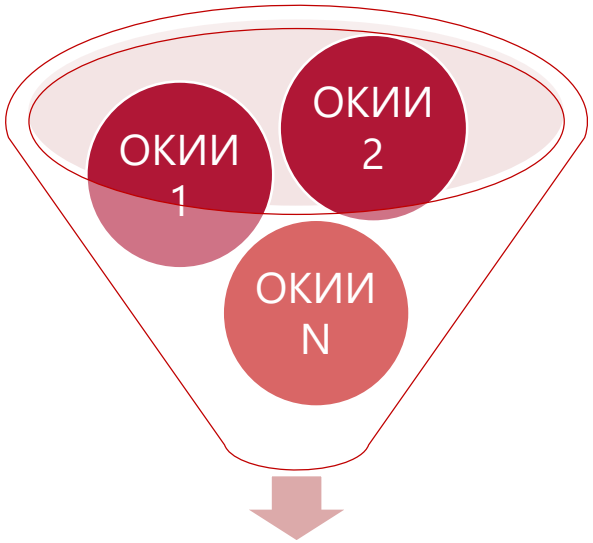
Результат:

Перечень объектов КИИ

10 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

Автоматизация категорирования объектов КИИ

Задачи систем автоматизации (GRC):

1. Формирование комиссии по категорированию ОКИИ
2. Определение критических процессов
3. Определение перечня ОКИИ
4. Анализ угроз
5. Категорирование объектов КИИ
6. Консолидация данных с дочерних обществ и контроль работ
7. Формирование отчетности

eplatform RVision At the root of your security Security Vision

ICL СИСТЕМНЫЕ ТЕХНОЛОГИИ alfadoc DOCSHELL

Комплексный подход к безопасности ОКИИ

Управление и планирование

- ✓ Ежегодный план по ИБ
- ✓ Регулярный пересмотр категории (1 раз в 5 лет)

Проектирование

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

Обучение

- ✓ Программа УЦ Softline: «Обеспечение безопасности значимых объектов КИИ и АСУ ТП»
- ✓ Security Awareness

Реализация

- ✓ Реализация СОИБ
- ✓ Акт приемки СОИБ
- ✓ Техническая поддержка СОИБ

Пример технической реализации СОИБ ОКИИ

Основные средства защиты ОКИИ:

1. Защита от несанкционированного доступа: Secret Net Studio 8
2. Антивирусная защита: Kaspersky Endpoint Security 11
3. Межсетевое экранирование, предотвращение вторжений: FortiGate
4. Шифрование: ViPNet
5. SIEM: MaxPatrol SIEM
6. Сканер уязвимостей: MaxPatrol 8
7. ГосСОПКА: ПТ Ведомственный центр

ГосСОПКА

ГосСОПКА предназначена для обеспечения защищенности информационных ресурсов РФ от компьютерных атак и их штатного функционирования при возникновении компьютерных инцидентов

ВАЖНО ЗНАТЬ

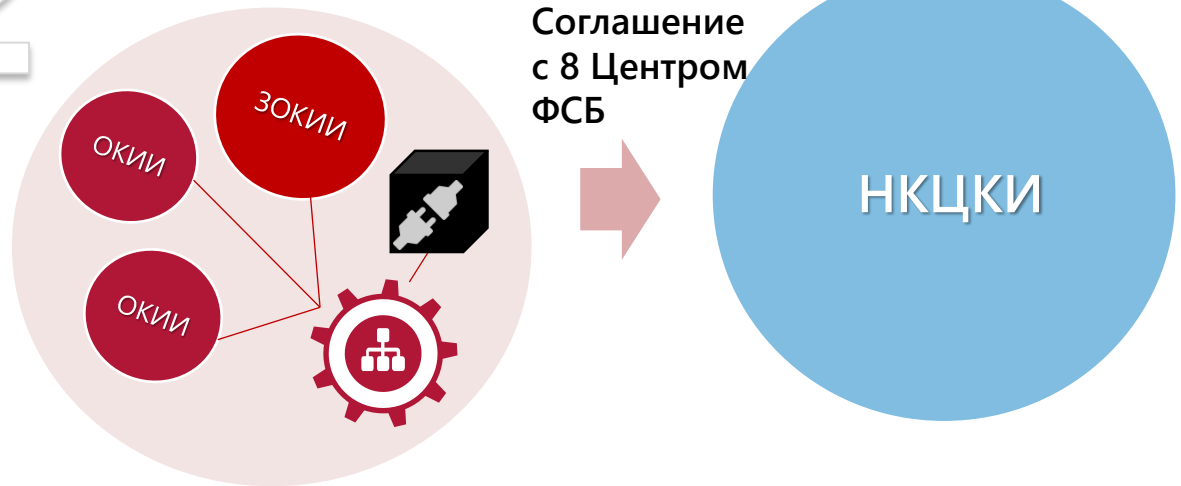
- ГосСОПКА не ограничивается целями и задачами, указанными в ФЗ-187
- Нацелена на противодействие целевым атакам (APT)
- Для функционирования ГосСОПКА необходимо реализовать базовый набор средств и мер защиты ОКИИ

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

Взаимодействие с ГосСОПКА

1

2



ГОССОПКА

- через тех. инфраструктуру НКЦКИ (.json)

  ОБЯЗАТЕЛЬНО!!! для значимых ОКИИ

- через портал НКЦКИ (ЛК субъекта ГосСОПКА)

- E-mail,
- Почта,
- Факс,
- Телефон

Функции Центра ГосСОПКА

«Обеспечение безопасности значимых объектов КИИ и АСУ ТП»

Программа повышения квалификации

2019

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

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

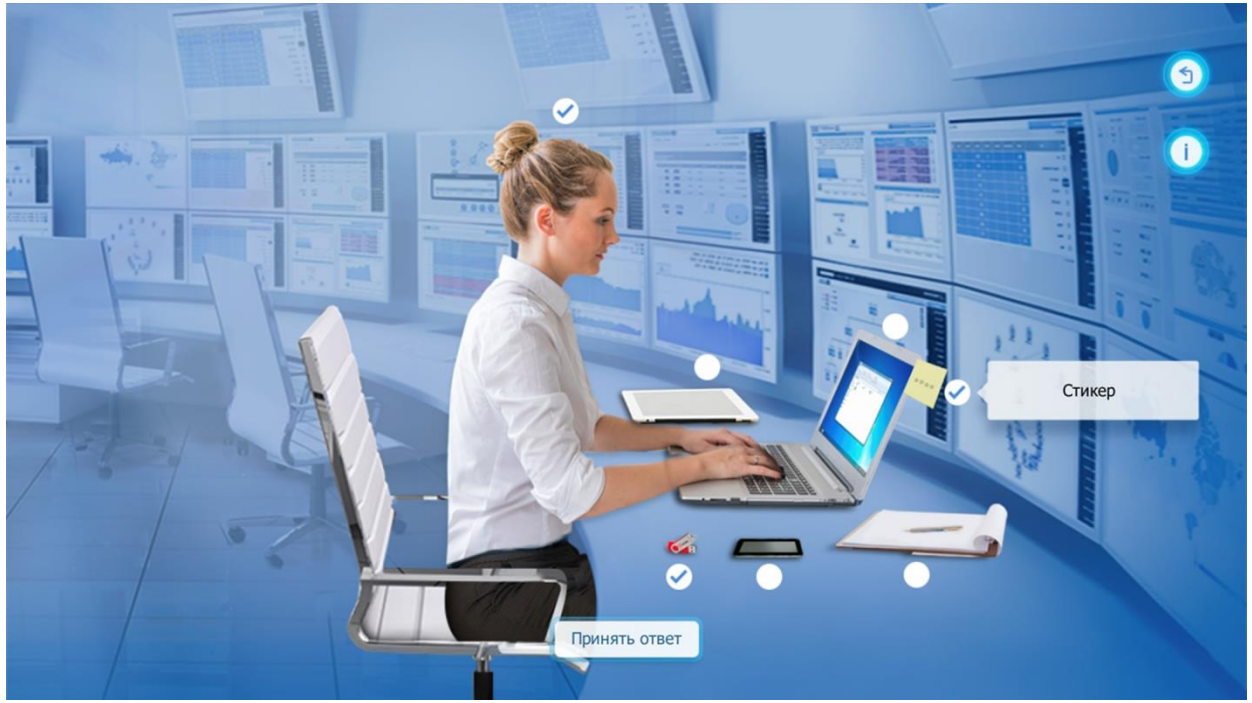
- Продолжительность обучения: 24 часа (3 дня)
- Аудитория: руководители служб и подразделений в сфере информационно-коммуникационных технологий, руководители отделов систем защиты информации, специалисты по защите информации, инженеры автоматизированных систем управления
- Формат: очный / дистанционный

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

Системы дистанционного обучения по ИБ

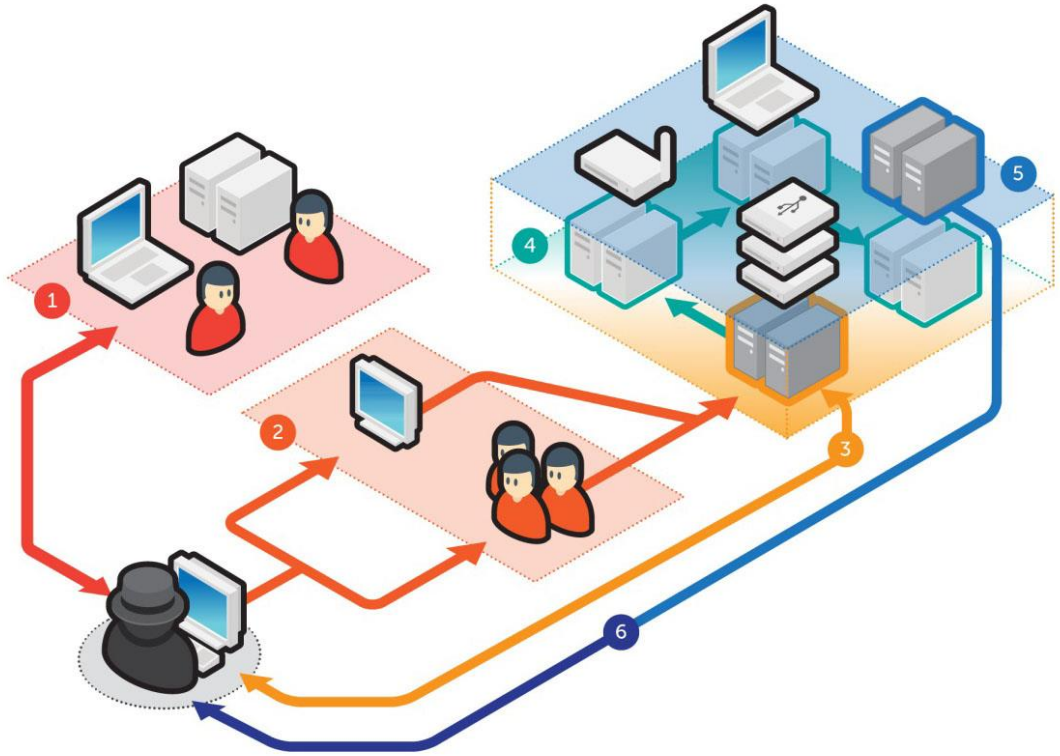
Системы Security Awareness: Антифишинг, Левел, Kaspersky Security Awareness, Phishman:

1. Обучение
2. Геймификация
3. Аттестация
4. Статистика



Киберполигон для обучения по ИБ и киберучений

1. Создание типовой ИТ-инфраструктуры субъекта на Windows/Cisco
2. Эмуляция компьютерных атак
3. Запись действий операторов SOC по реагированию на компьютерные атаки
4. Оценка действий операторов SOC
5. Аналитика готовности и успешности операторов SOC
6. Диджитализация процесса тренировки и контроля готовности операторов SOC



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

Опыт реализации проектов по защите ОКИИ

1. Один из крупнейших российских энергетических холдингов
2. Российская энергетическая компания, (11 областей)
3. Региональные водоканалы
4. Оператор магистральных нефтепроводов России
5. Одна из крупнейших в мире урановая компания
6. Российская двигателестроительная компания
7. Нефтехимический холдинг России
8. Государственные учреждения

- Более 20+ проектов за последние 3 года
- Опыт внедрения СОИБ
- Наличие компетенций по безопасности ОКИИ в СЗФО
- Наличие статусов и опыт внедрения специализированных средств защиты АСУ (Kaspersky CICS и др.)


GO GLOBAL
GO CLOUD
GO INNOVATIVE