Практический опыт реализации 187-ФЗ.

Алексей Аршинов
Руководитель отдела организации защиты информации

Критическая информационная инфраструктура

СУБЪЕКТЫ

- Гос. Органы
- Рос. Юр. Лица
- ИП

СФЕРА ДЕЯТЕЛЬНОСТИ

- Здравоохранение
- Наука
- Транспорт
- Связь
- Энергетика
- Банковская сфера
- ТЭК
- Атомная энергетика
- Оборонная пром.
- Ракетно-космическая
- Горно-добывающая
- Металлургическая
- Химическая

ОБЪЕКТЫ

- Информационные системы
- Сети связи
- АСУ

ФОРМА ВЛАДЕНИЯ

- Аренда
- Право собственности.
- Иное законное основание

Защита КИИ, 7 непростых шагов

Процессы в организации

Критические процессы

Перечень объектов

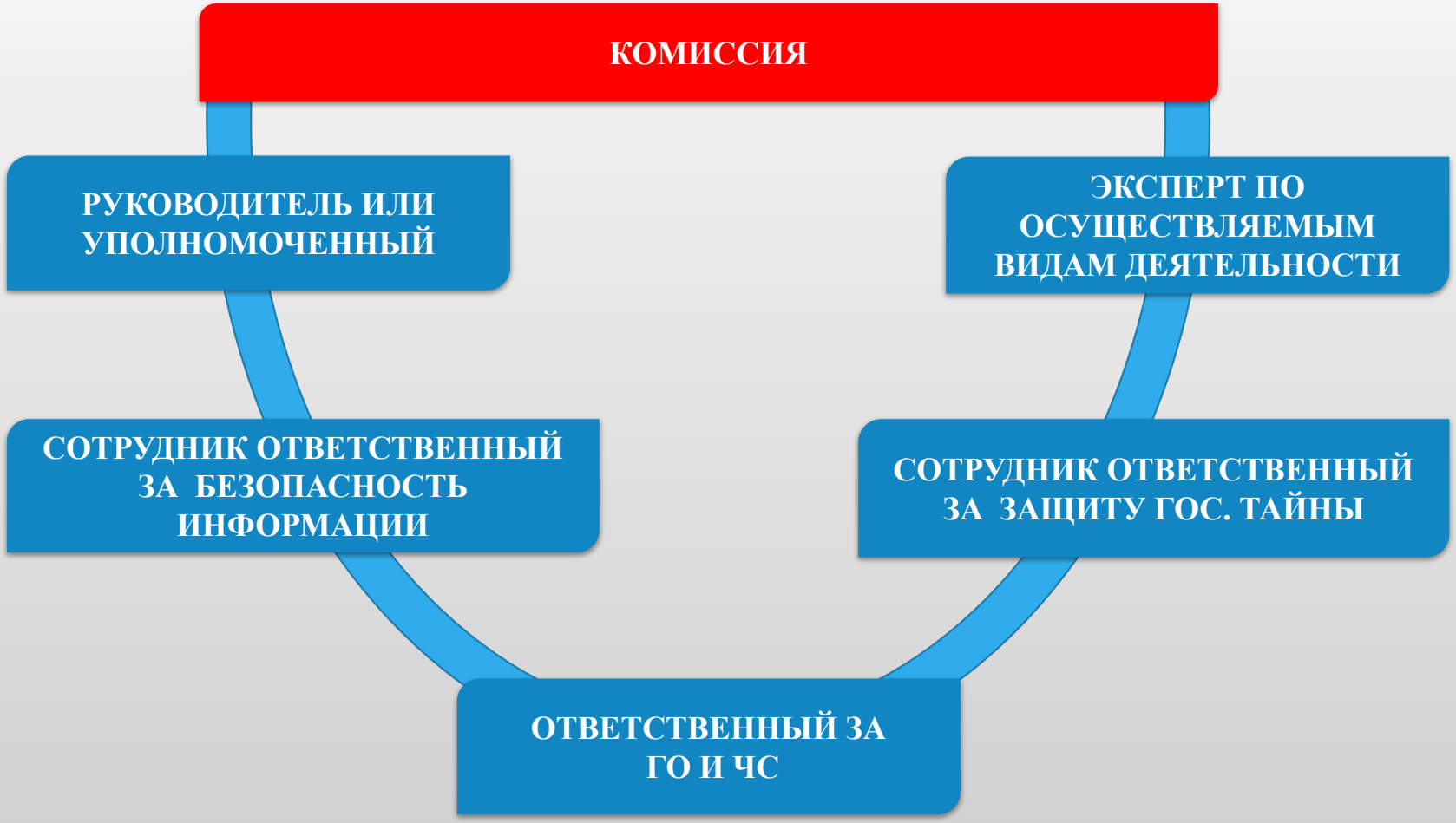
Категорирование объектов

Разработка ТЗ
Разработка ТП

Внедрение СЗИ

Подключение к ГосСОПКА

Шаг 0,5. Комиссия



Шаг 0,5. Комиссия

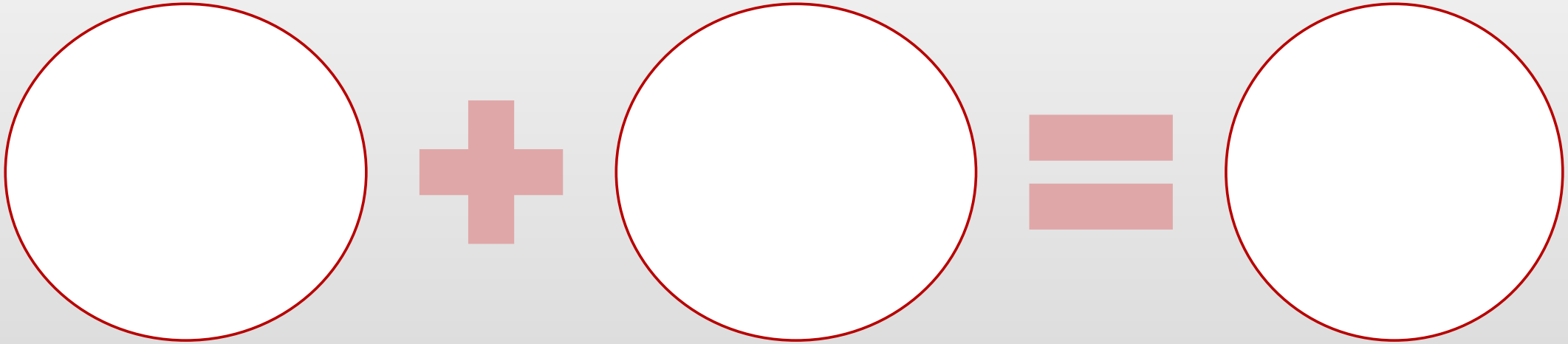
№	Новая статья 274.1 в УК РФ (дела по ней рассматривает ФСБ)	Ответственность
1	Создание, распространение, использование ПО либо иной компьютерной информации для неправомерного воздействия на КИИ	До **5 лет**, со штрафом
2	Неправомерный доступ к охраняемой информации в КИИ, повлекший причинение вреда КИИ	До **6 лет**, со штрафом
3	Нарушение правил эксплуатации и правил доступа, повлекшее причинение вреда КИИ	До **6 лет**, с лишением права занимать должность
4	Все предыдущие деяния по сговору или с использованием служебного положения	До **8 лет**, с лишением права занимать должность
5	Все предыдущие деяния, повлекшие тяжкие последствия	До **10 лет**, с лишением права занимать должность

- Внеплановая проверка ФСТЭК

- Разбор причин произошедшего инцидента

- До 10 лет

Шаг 1. Перечень процессов



- ОКВЭД
- Устав
- Лицензия

- Контракты
- Обязательства

Шаг 2. Перечень критических процессов

- Снабжение столовой
- Управление полетом
- Подбор кадров
- Бухгалтерия

- Управление полетом
- Подбор кадров

Шаг 3. Перечень объектов

Шаг 4. Категорирование объектов

НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ

СОЦИАЛЬНЫЕ	ПОЛИТИЧЕСКИЕ	ЭКОНОМИЧЕСКИЕ	ЭКОЛОГИЧЕСКИЕ
- ущерб жизни и здоровью людей.	- нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора.	- возникновение ущерба бюджетам Российской Федерации более 0,001 от бюджета субъекта РФ или федерального бюджета.	- вредные воздействия на окружающую среду.

ОБОРОНОСПОСОБНОСТЬ СТРАНЫ, БЕЗОПАСНОСТИ ГОСУДАРСТВА И ПРАВОПОРЯДКА

Шаг 4,5. Акты классификации

- сведения о взаимодействии объекта КИИ и сетей электросвязи;
- сведения о программных и программно-аппаратных средствах, используемых на объекте КИИ, в том числе средствах, используемых для обеспечения безопасности;
- возможные последствия в случае возникновения компьютерных инцидентов на объекте КИИ либо сведения об отсутствии таких последствий;
- категорию значимости, которая присвоена объекту КИИ, или сведения об отсутствии необходимости присвоения одной из категорий значимости.

Шаг 4,5. Акты классификации и согласование

- **Максимальное кол-во информации об объектах**
- **Не все объекты являются критическими**
- **Модели угроз только в соответствии с методикой определения угроз в информ. системах**
- **Наличие каналов доступа для разработчиков**
- **Используемое ПО**

Шаг 5. Разработка ТЗ и ТП

Проект по защите КИИ

Обоснование организационных и технических мер защиты

Определенны виды и типы средств защиты

Осуществлен выбор средств защиты информации

Определенны требования по настройке средств защиты

Шаг 6. Внедрение СЗИ

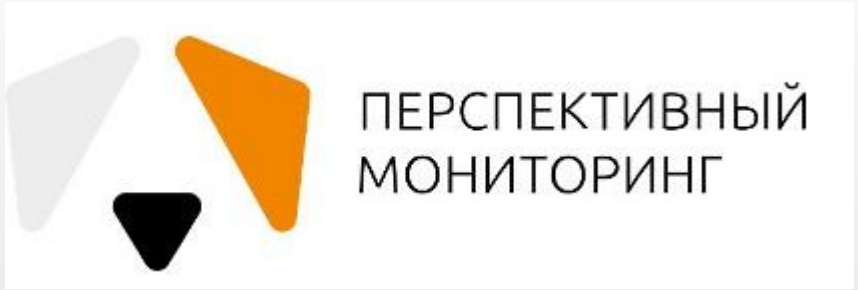
- Разработка организационно-распорядительных документов, регламентирующих правила и процедуры обеспечения безопасности значимого объекта;
- Испытание системы защиты с в соответствии с оформлением акта;
- Анализ системы защиты на возможность нейтрализации угроз из банка данных угроз ФСТЭК России (на данный момент в БДУ 208 угроз);
- Внедрение средств защиты должно выполняться собственными силами либо с привлечением лицензиата ФСТЭК России.

Шаг 7. Подключение к ГосСОПКА

- 6 человек мониторинг
- 1 руководитель

- Комплекс СЗИ в соответствии с Приказом №239
- SIEM система
- Система взаимодействия с НКЦКИ

Шаг 7,5. Подключение к ГосСОПКА
Аутсорсинг.



У меня нет значимых объектов КИИ, меня это не касается?

Отсутствие категории значимости нужно доказать. Если системы используются в сферах деятельности 187-ФЗ, то они подлежат категорированию. Для обоснования отсутствия значимости все равно необходимо провести категорирование.

Если сидеть тихо – можно не выполнять требования?

Для оценки безопасности КИИ регулятор имеет право установить средства, предназначенные для поиска признаков компьютерных атак в сетях электросвязи. Утечки об атаках в СМИ никто не отменял.

Подведомственным и дочерним ждать команду сверху?

Ждать команду сверху не надо. Выполнять требования 187-ФЗ необходимо уже сейчас, так как предусмотрена ответственность независимо от подчиненности той или иной организации

У нас есть черная коробочка от ФСБ, мы уже все сделали?

Нет, черная коробочка – это сенсор, который вам поставили в рамках системы с похожим названием СОПКА для защиты от хакеров. С принятием 187-ФЗ такие сенсоры устанавливают в целях контроля защищенности. Чтобы подключиться к новой системе, надо создать центр ГосСОПКА и заключить соглашение с ФСБ.

Вопросы?

Алексей Аршинов
Тел.: 8-903-300-18-20
Почта: aarshinov@zaschita-it.ru