Практический опыт реализации 187-ФЗ.

Алексей Аршинов
Руководитель отдела организации защиты информации

Критическая информационная инфраструктура

КИИ 7 этапов реализации требований 187-ФЗ

Процессы в организации

Критические процессы

Перечень объектов

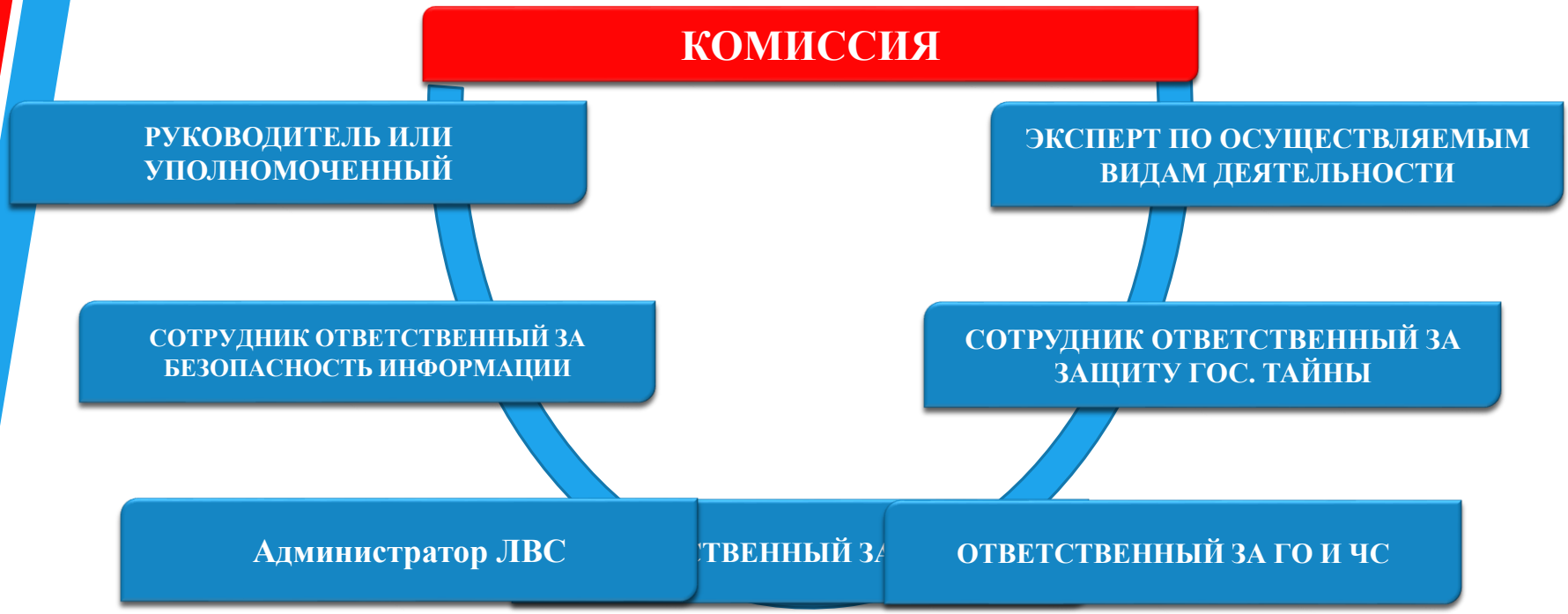
Категорирование объектов

Разработка ТЗ
Разработка ТП

Внедрение СЗИ

Подключение к ГосСОПКА

Комиссия


КОМИССИЯ
РУКОВОДИТЕЛЬ ИЛИ УПОЛНОМОЧЕННЫЙ
ЭКСПЕРТ ПО ОСУЩЕСТВЛЯЕМЫМ ВИДАМ ДЕЯТЕЛЬНОСТИ
СОТРУДНИК ОТВЕТСТВЕННЫЙ ЗА БЕЗОПАСНОСТЬ ИНФОРМАЦИИ
СОТРУДНИК ОТВЕТСТВЕННЫЙ ЗА ЗАЩИТУ ГОС. ТАЙНЫ
Администратор ЛВС
ОТВЕТСТВЕННЫЙ ЗА ГО И ЧС

Мотивация

№	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

Определение перечня процессов

- ОКВЭД
- Устав
- Полученные лицензии
- Декларации промышленной безопасности

Стоит обратить внимание на:

- Контракты
- Обязательства

Выделение критических процессов

Снабжение столовой

Критический процесс

Подбор кадров

Бухгалтерия

Постановление № 127

Критический процесс

Определение Перечень объектов КИИ

Разработка актов 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;
- Модель угроз и модель нарушителя объекта КИИ.

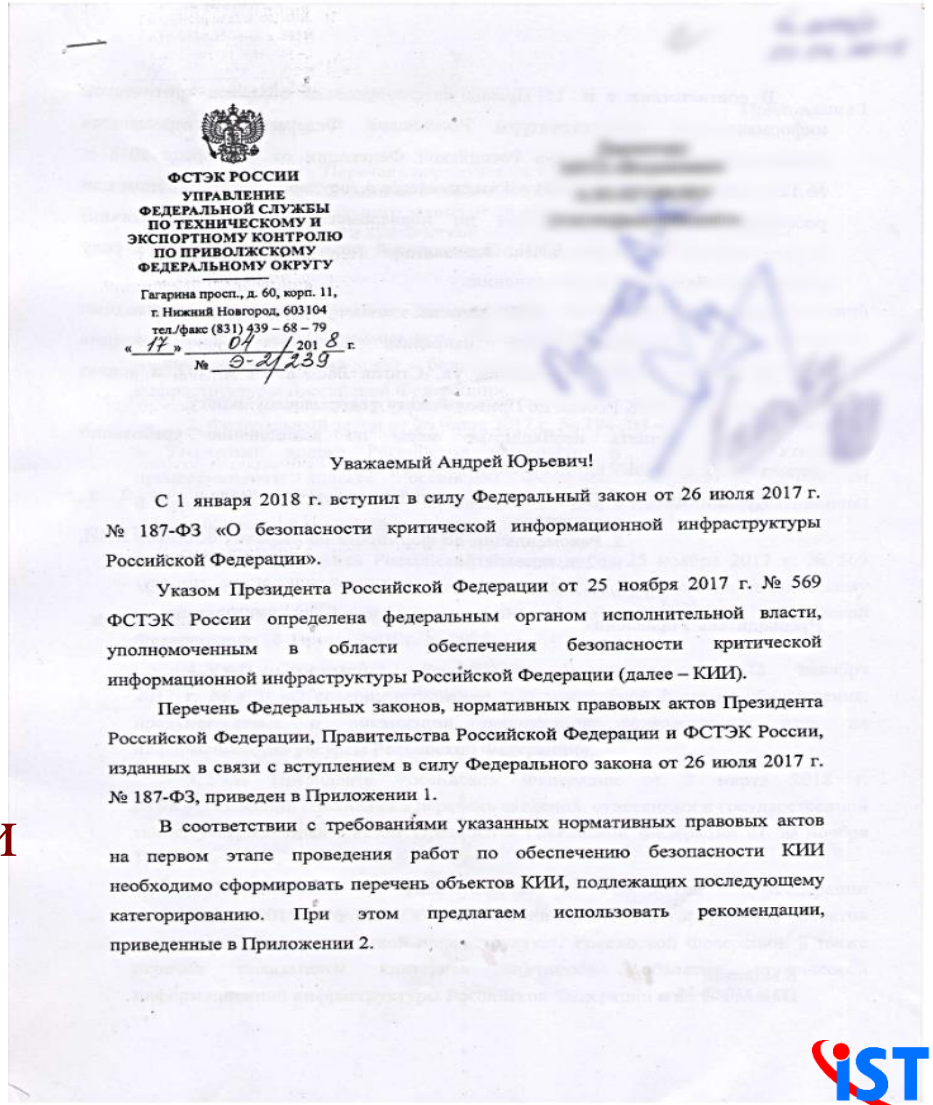
Разработка модели угроз

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.

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



ФСТЭК РОССИИ
УПРАВЛЕНИЕ
ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И
ЭКСПОРТНОМУ КОНТРОЛЮ
ПО ПРИВОЛЖСКОМУ
ФЕДЕРАЛЬНОМУ ОКРУГУ

Гагарина просп., д. 60, корп. 11,
г. Нижний Новгород, 603104
тел./факс (831) 439 – 68 – 79
«17» 04 2018 г.
№ 9-2/239

Уважаемый Андрей Юрьевич!

С 1 января 2018 г. вступил в силу Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Указом Президента Российской Федерации от 25 ноября 2017 г. № 569 ФСТЭК России определена федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее – КИИ).

Перечень Федеральных законов, нормативных правовых актов Президента Российской Федерации, Правительства Российской Федерации и ФСТЭК России, изданных в связи с вступлением в силу Федерального закона от 26 июля 2017 г. № 187-ФЗ, приведен в Приложении 1.

В соответствии с требованиями указанных нормативных правовых актов на первом этапе проведения работ по обеспечению безопасности КИИ необходимо сформировать перечень объектов КИИ, подлежащих последующему категорированию. При этом предлагаем использовать рекомендации, приведенные в Приложении 2.

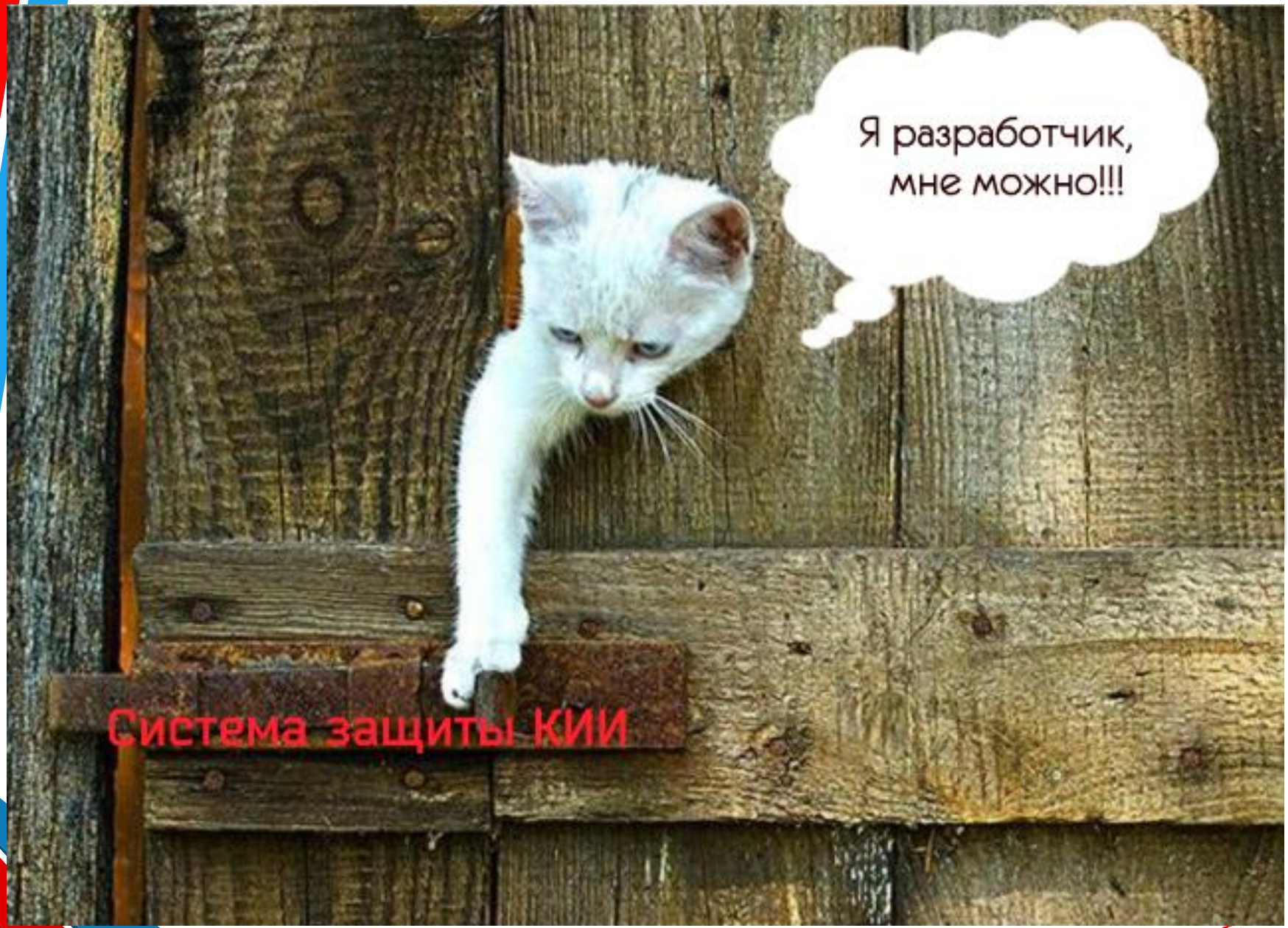
Категорирование объектов КИИ

НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ

СОЦИАЛЬНЫЕ	ПОЛИТИЧЕСКИЕ	ЭКОНОМИЧЕСКИЕ	ЭКОЛОГИЧЕСКИЕ
Причинение ущерба жизни и здоровью людей (даже одного человека)	Прекращение или нарушение функционирования органа государственной власти субъекта Российской Федерации или города федерального значения	Возникновение ущерба бюджетам Российской Федерации более 0,001 от бюджета субъекта РФ или федерального бюджета.	Вредные воздействия на окружающую среду в рамках одного муниципального образования или Одной внутригородской территории города федерального значения

ОБОРОНОСПОСОБНОСТЬ СТРАНЫ, БЕЗОПАСНОСТИ ГОСУДАРСТВА И ПРАВОПОРЯДКА

Прекращение или нарушение функционирования пункта управления или ситуационного центра органа государственной власти субъекта Российской Федерации или города федерального значения


Я разработчик,
мне можно!!!
Система защиты КИИ

Внедрение СЗИ

- Разработка организационно-распорядительных документов, регламентирующих правила и процедуры обеспечения безопасности значимого объекта;
- Тестирование на проникновение в условиях, соответствующих возможностям нарушителей, определенных в модели угроз безопасности информации выявление известных уязвимостей программных и программно-аппаратных средств **(лицензируемый вид деятельности)**
- Тестирование в соответствии с программой и методикой приемочных испытаний. Результаты приемочных испытаний значимого объекта и его подсистемы безопасности с выводом о ее соответствии установленным требованиям включаются в акт приемки значимого объекта в эксплуатацию

Подключение к ГосСОПКА

Подключение к ГосСОПКА
Аутсорсинг?

POSITIVE TECHNOLOGIES

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

SOLAR SECURITY
software&services

Вопросы?

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