Дмитрий Кузнецов
Директор по методологии и стандартизации
dkuznetsov@ptsecurity.com

Практика построения центров ГосСОПКА

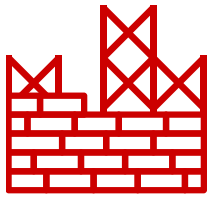
Часть 1: Структура и функции центров

Нормативные требования и рекомендации

Нормативная база ГосСОПКА

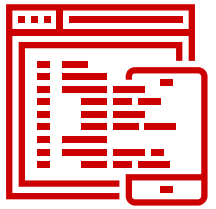
POSITIVE TECHNOLOGIES

ФЗ «О безопасности критической информационной инфраструктуры» (пока в проекте)



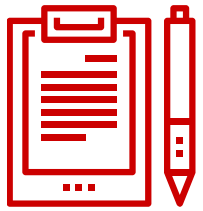
Указ Президента №31с

Основные направления государственной политики в области безопасности КВО



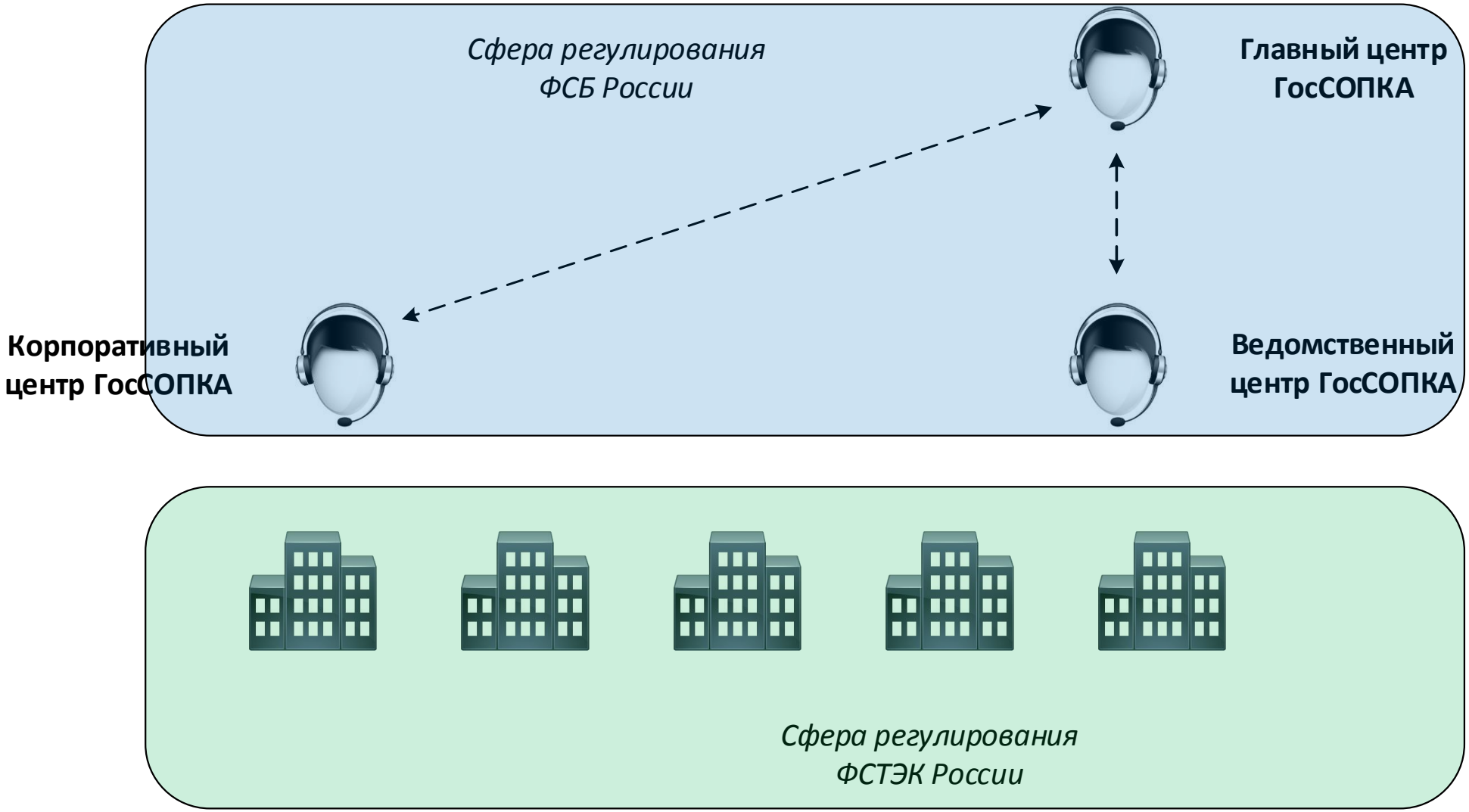
Концепция ГосСОПКА

Методические рекомендации по созданию центров ГосСОПКА



Меры защиты информации в государственных информационных системах

Сферы регулирования

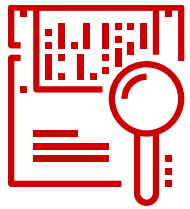


В чем разница

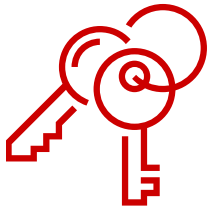
POSITIVE TECHNOLOGIES

ФСТЭК

Защита от атак отдельных ИС



Надзор за выполнением требований

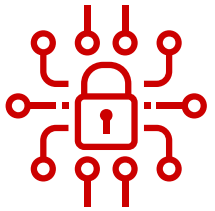


Средства защиты в составе ИС

ФСБ

Реагирование на атаки в целом для объекта

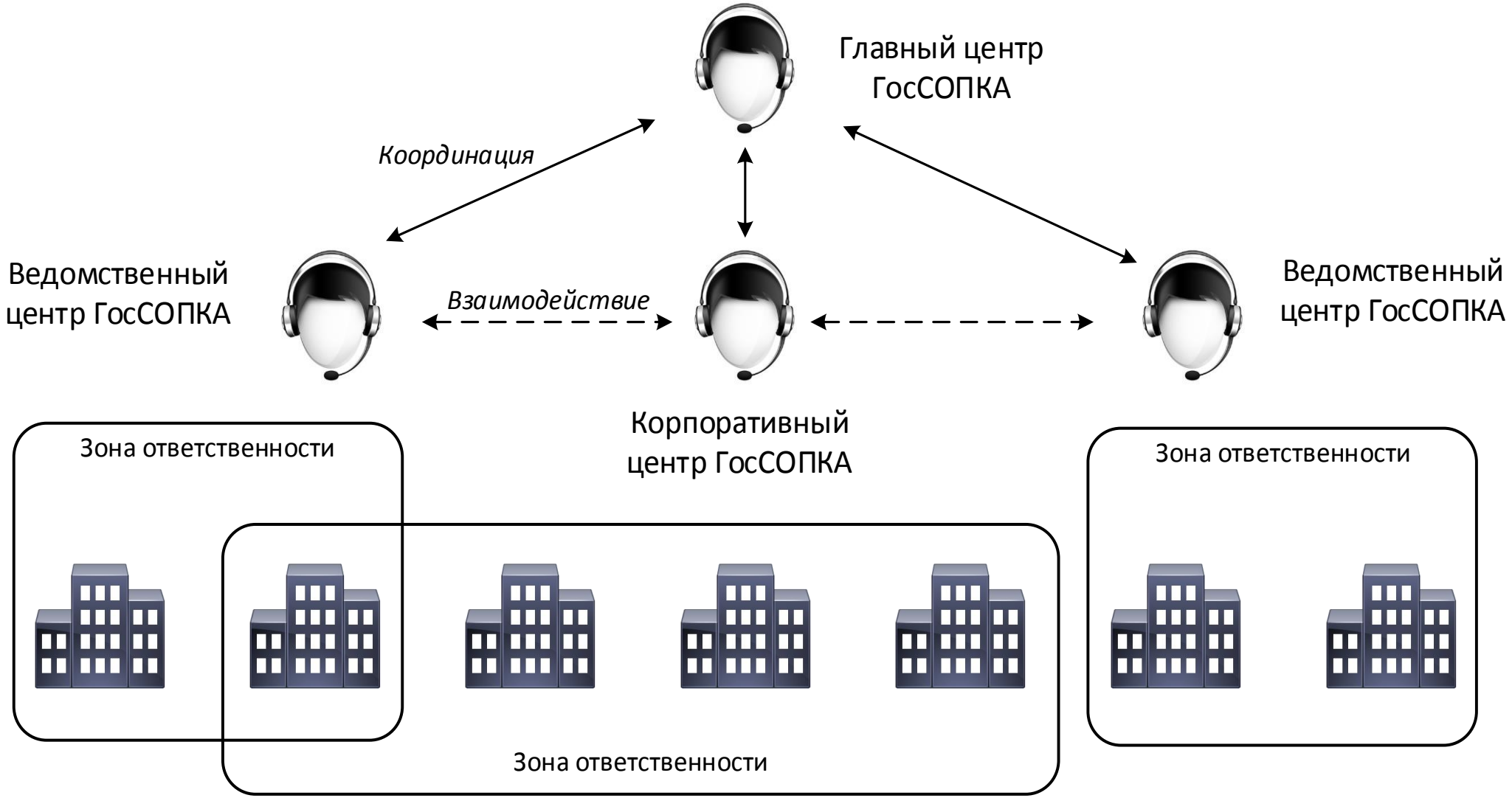
Оценка состояния защищенности



Дополнительные средства защиты

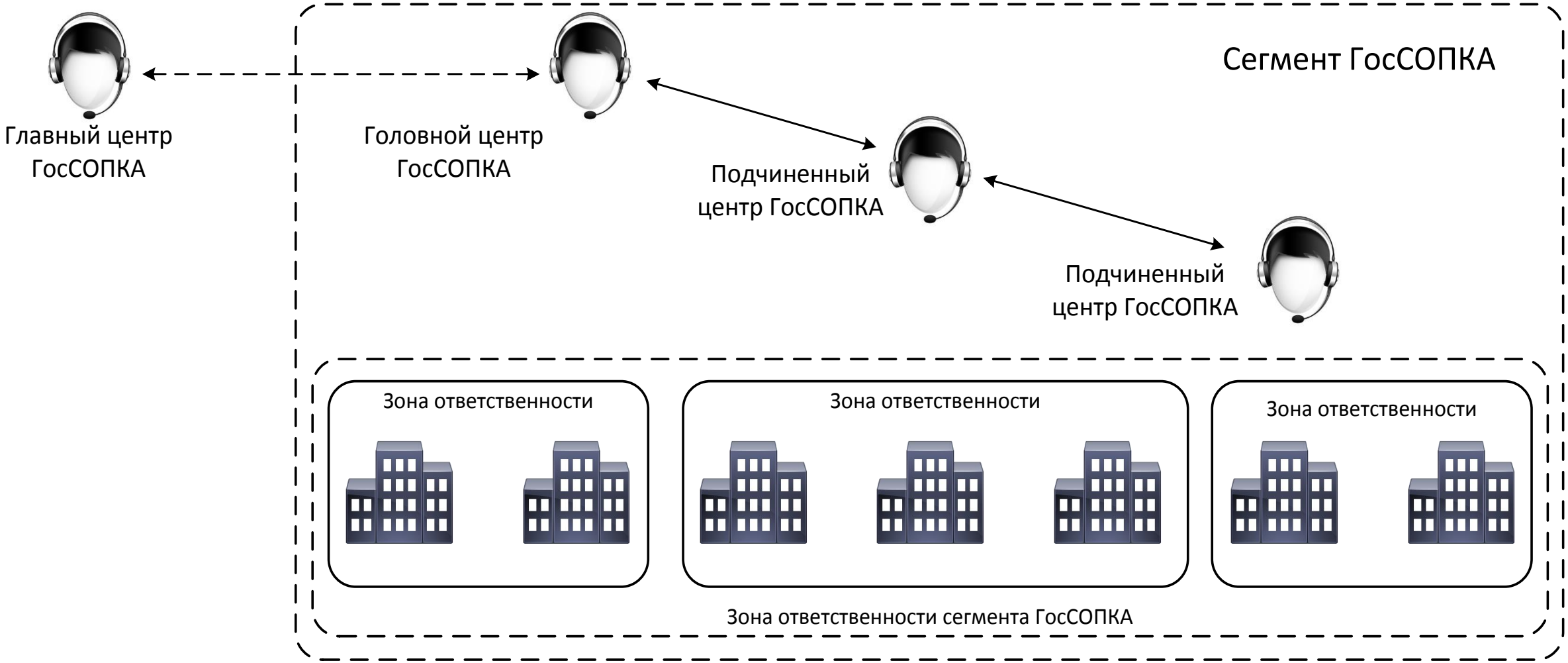
Общая структура ГосСОПКА

POSITIVE TECHNOLOGIES



Центры и сегменты ГосСОПКА

POSITIVE TECHNOLOGIES



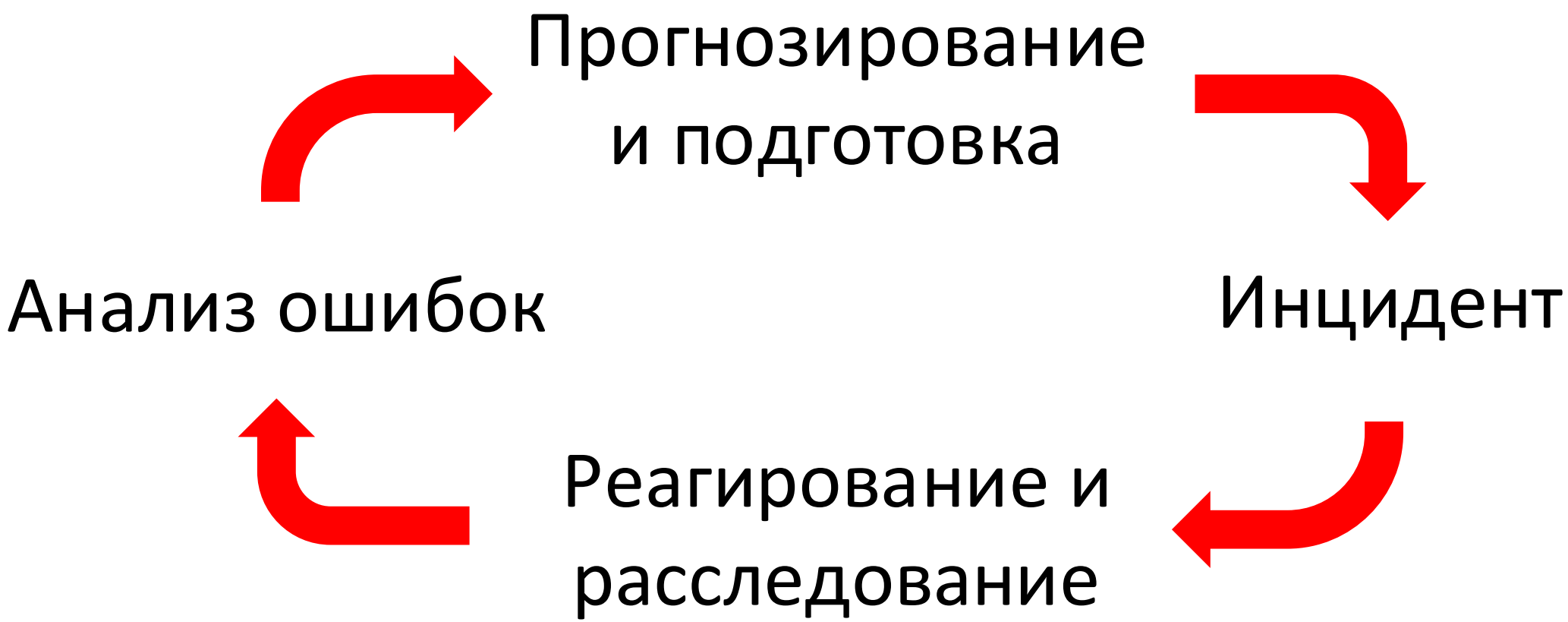
Функции центра ГосСОПКА

POSITIVE TECHNOLOGIES

- Инвентаризация информационных ресурсов
- Выявление уязвимостей
- Анализ угроз
- Повышение осведомленности персонала и пользователей
- Прием сообщений о возможных инцидентах
- Обнаружение компьютерных атак
- Анализ данных о событиях безопасности
- Регистрация инцидентов
- Реагирование на инциденты и ликвидация их последствий
- Расследование инцидентов
- Анализ результатов устранения последствий инцидентов

«PDCA для инцидентов»

POSITIVE TECHNOLOGIES



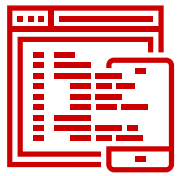
Вопросы?

От теории к практике

Инвентаризация

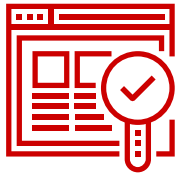
POSITIVE TECHNOLOGIES

Определение сетевого периметра



Идентификация ИС

Идентификация вычислительной техники

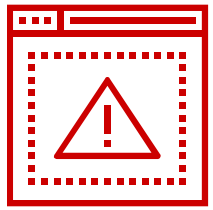


Определение состава программного обеспечения

Идентификация контактных лиц

Выявление уязвимостей

POSITIVE TECHNOLOGIES

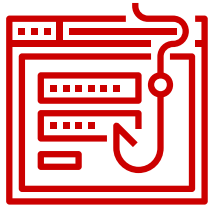


Поиск известных уязвимостей ПО и сетевых служб

Анализ проектной документации

Анализ настроек ПО

Контроль мер защиты и оценка соответствия требованиям

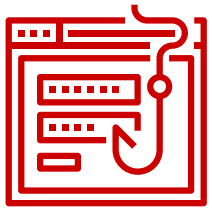


Тестирование на проникновение и устойчивости к DoS

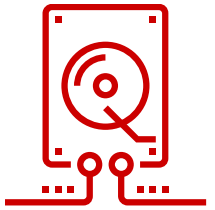
Контроль устранения недостатков

Анализ угроз: делаем выводы из уязвимостей

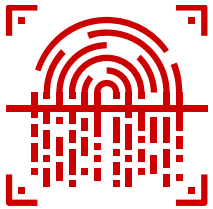
POSITIVE TECHNOLOGIES



Что может сделать нарушитель?

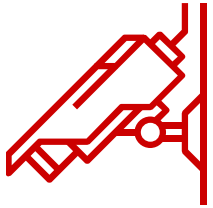


Что делать, если обнаружили?

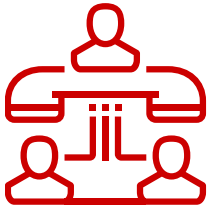


Какие следы он может оставить?

Чем можем пожертвовать?



Как эти следы обнаружить?



Кто может помочь?

Повышение осведомленности

POSITIVE TECHNOLOGIES

Регламенты, процедуры, инструкции

Наглядная агитация

Очное и дистанционное обучение

“Киберучения”

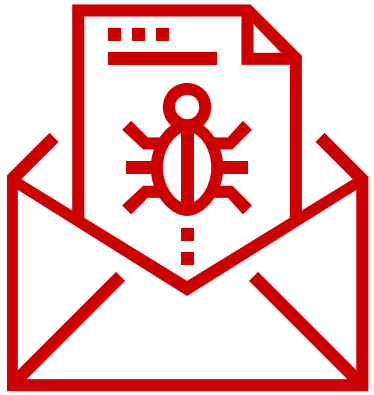
Аттестация

Прием сообщений об инцидентах

POSITIVE TECHNOLOGIES

Возможные способы взаимодействия с персоналом и пользователями

Телефонная связь



Электронная почта

Веб-портал

Обнаружение компьютерных атак

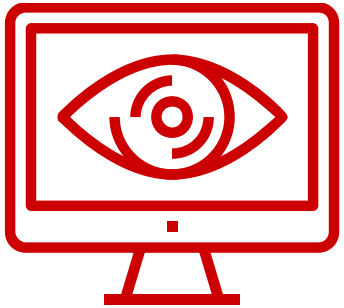
POSITIVE TECHNOLOGIES

Обнаружение атак – это постоянный процесс

Обнаружение сигнатур известных атак

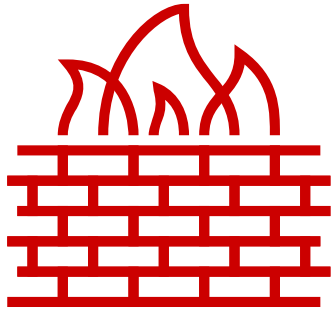
Анализ сетевого трафика и разработка сигнатур для неизвестных атак

“Коробочные” средства антивирусной защиты



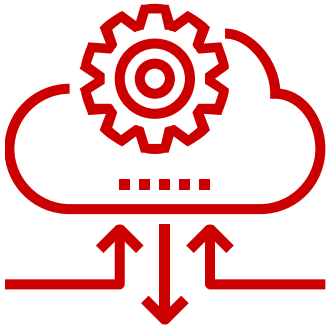
Поведенческий анализ подозрительного ПО

Источники данных для SIEM

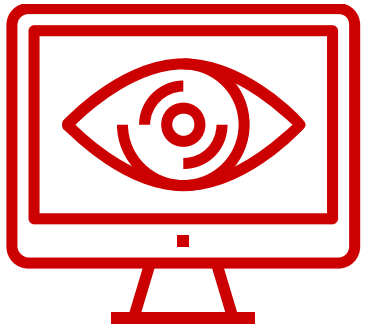


Средства обнаружения вторжений, межсетевые экраны

Средства анализа сетевого трафика, WAF



Средства регистрации событий ПО и СЗИ



“Песочницы”

Реагирование и ликвидация последствий

POSITIVE TECHNOLOGIES

Реагирование на инцидент

- Определение “повреждений”
- Формирование совместной рабочей группы
- Локализация “повреждений”
- Локализация свидетельств

Устранение последствий

- Восстановление работоспособности
- “Чистка”
- …

Расследование

- Сбор свидетельств для внутреннего расследования
- Предоставление материалов правоохранительным органам

Ретроспективный анализ

- Анализ недостатков в защите
- Оценка успешности мер реагирования
- Рекомендации по совершенствованию защиты

Вопросы?

Нормативные ссылки

POSITIVE TECHNOLOGIES

Законопроект «О безопасности критической информационной инфраструктуры Российской Федерации»

http://asozd2.duma.gov.ru/main.nsf/%28Spravka%29?OpenAgent&RN=47571-7

«Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации»

http://www.scrf.gov.ru/security/information/document113/

«Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (выписка)

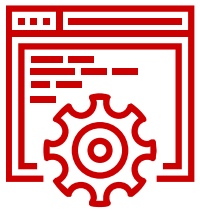
http://www.fsb.ru/files/PDF/Vipiska_iz_koncepcii.pdf

Указ «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (выписка)

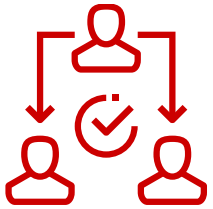
https://rg.ru/2013/01/18/komp-ataki-site-dok.html

Что дальше?

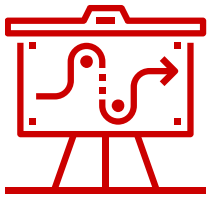
POSITIVE TECHNOLOGIES



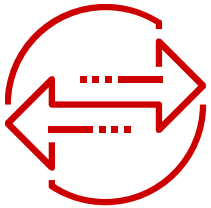
Особенности выполнения требований



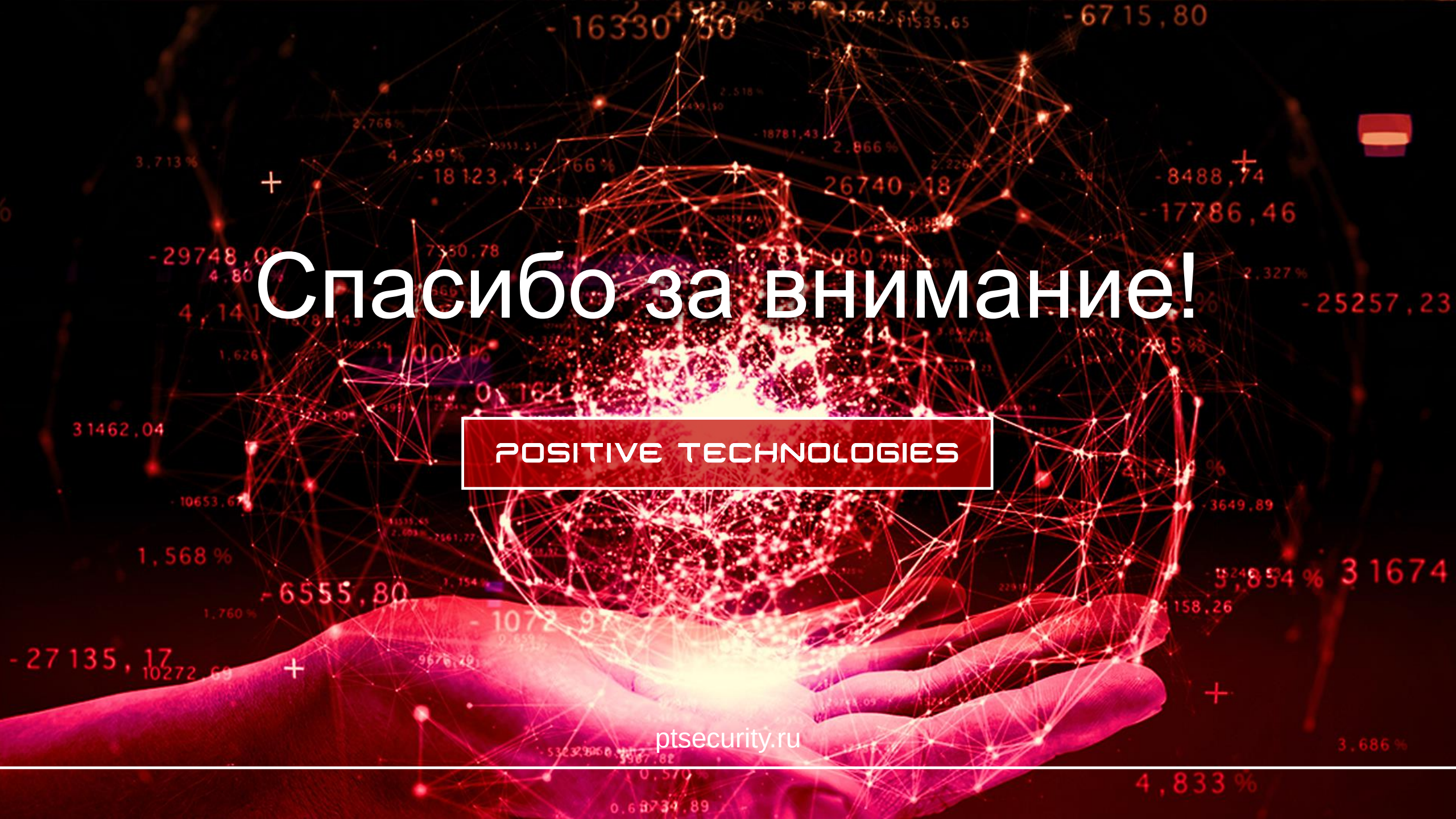
Кадровый вопрос



Процедура и этапы создания центра ГосСОПКА



Об этих и других нюансах – в следующей части вебинара 23.03.2016


Спасибо за внимание!
POSITIVE TECHNOLOGIES
ptsecurity.ru