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

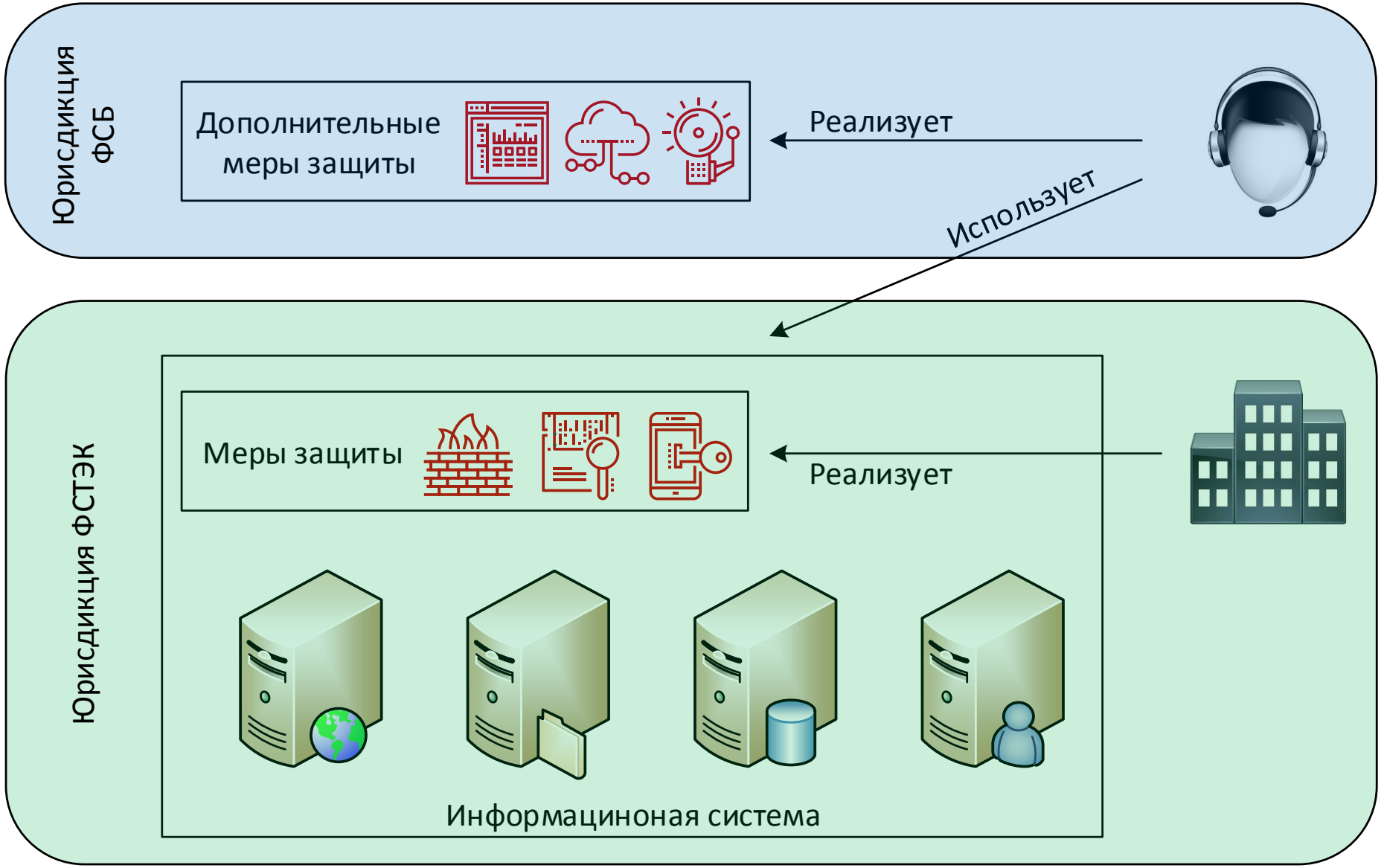
Практика построения центров ГосСОПКА

Часть 2: Особенности развертывания

Взаимодействие

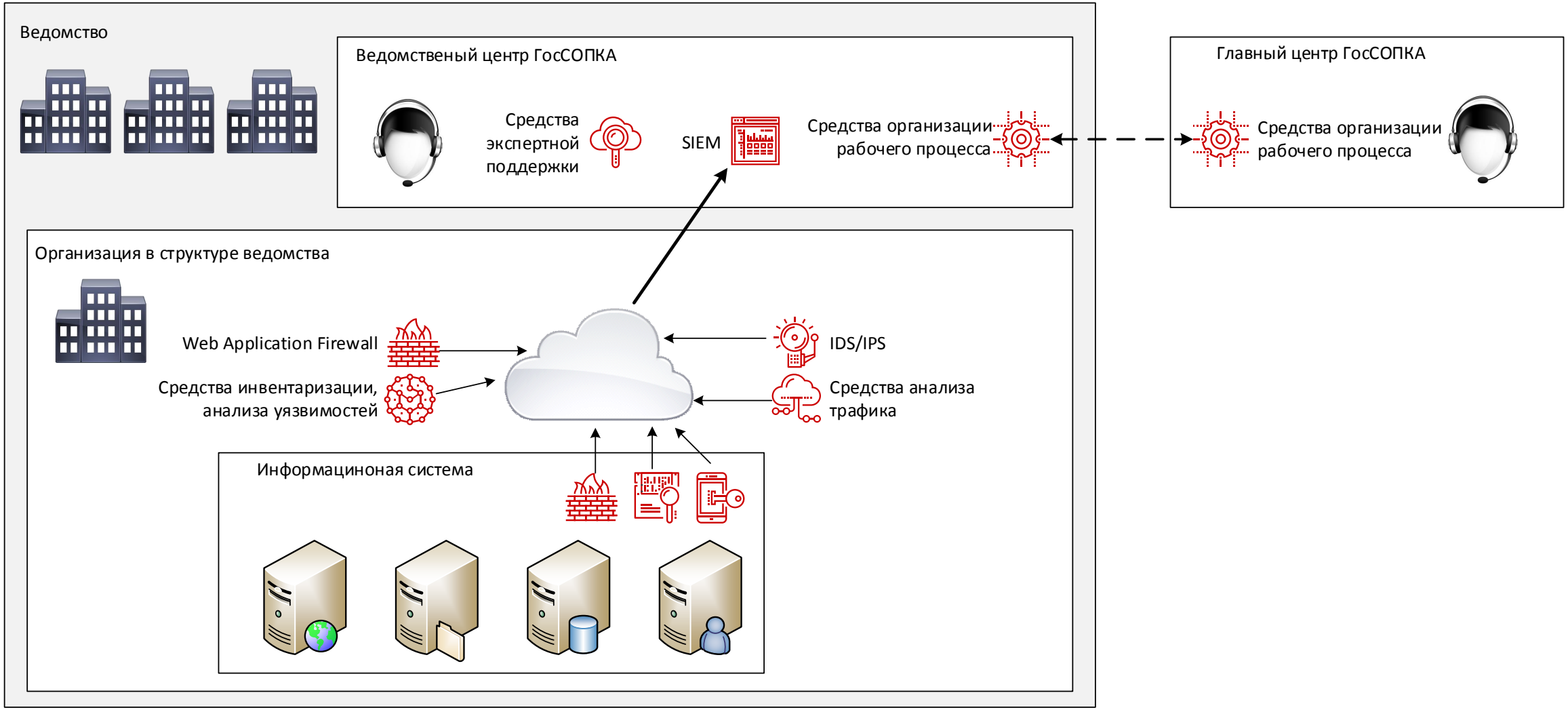
И снова о юрисдикциях

POSITIVE TECHNOLOGIES



Кому и как поступает информация

POSITIVE TECHNOLOGIES



Персонал центра ГосСОПКА

Персонал центра ГосСОПКА

POSITIVE TECHNOLOGIES

Первая линия

Непосредственное взаимодействие с персоналом и пользователями

Типовые операции, не требующие высокой квалификации

Вторая линия

Квалифицированные типовые действия

Третья линия

Руководство, экспертная поддержка, действия в непредвиденных ситуациях

Роли персонала: первая линия

POSITIVE TECHNOLOGIES

Специалист колл-центра

Взаимодействие с пользователями, персоналом ИС

Специалист по обнаружению компьютерных атак

Первичная фильтрация вердиктов антивирусных средств и систем обнаружения вторжений, оповещений SIEM, уточнение контекста

Администратор технических средств центра ГосСОПКА

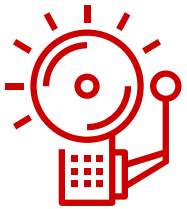
Настройка технических средств и дополнительных СЗИ, размещаемых на объектах

Роли персонала: вторая линия

POSITIVE TECHNOLOGIES

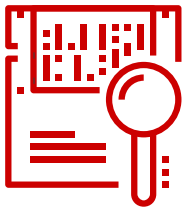
Специалист по оценке защищенности

Проведение/координация тестов на проникновение, анализ уязвимостей и угроз



Специалист по реагированию на инциденты

Координация действий при инцидентах

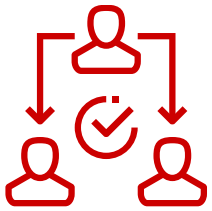


Специалист по расследованию инцидентов

Сбор и анализ свидетельств, взаимодействие с правоохранительными органами

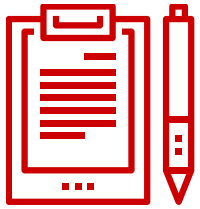
Роли персонала: третья линия

POSITIVE TECHNOLOGIES



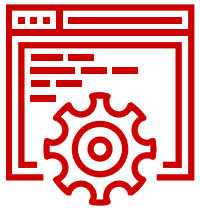
Руководитель

Управление деятельностью сегмента ГосСОПКА



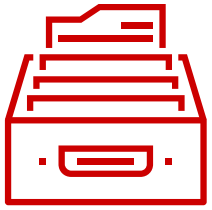
Аналитик-методист

Обобщение и формализация знаний



Технический эксперт

Экспертная поддержка в соответствии со специализацией



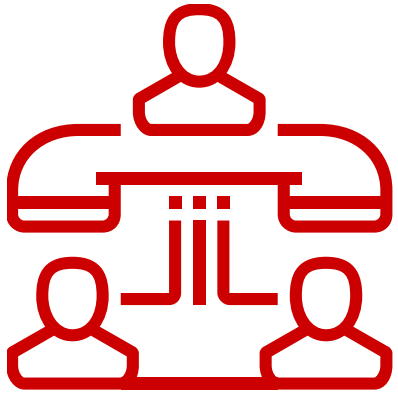
Юрист

Нормативно-правовое сопровождение

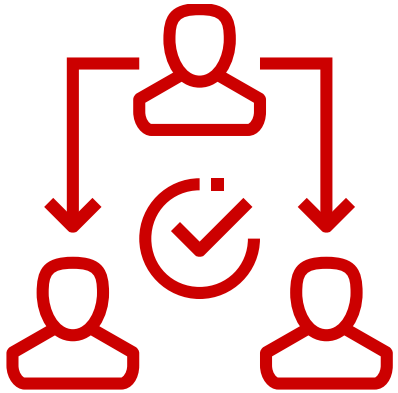
Где взять людей

POSITIVE TECHNOLOGIES

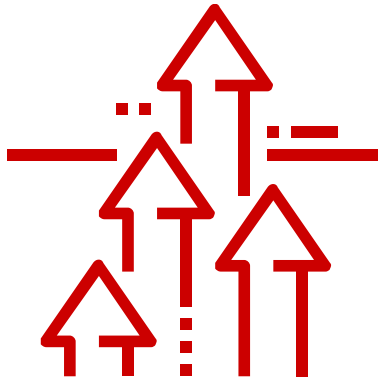
Взаимодействие с контрагентами



Аутсорсинг первой и третьей линий



Делегирование функций



Рамочные договоры на отдельные компетенции

Практическая реализация

Наши решения в сегменте ГосСОПКА

POSITIVE TECHNOLOGIES

Продукт	Для чего используется
MaxPatrol 8	Анализ защищенности, контроль конфигураций, инвентаризация
PT Application Firewall	Web Application Firewall (в информационных системах или на периметре) Экспертный инструмент для расследования web-based атак
MaxPatrol SIEM	Анализ и сопоставление событий и инвентаризационной информации, ядро центра
PT Ведомственный (Корпоративный) Центр	Управление инцидентами, взаимодействие с главным центром ГосСОПКА
PT Application Inspector	Экспертный инструмент для анализа защищенности веб-приложений
PT MultiScanner	Потоковое средство антивирусной защиты Экспертный инструмент для ретроспективного анализа

Процедура создания центра ГосСОПКА

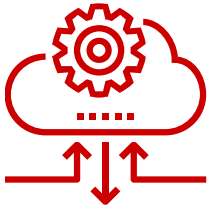
POSITIVE TECHNOLOGIES

1. Разработка технического задания
2. Разработка технического проекта
3. Добавление в зону ответственности внешних ИС, уточнение технического проекта
4. Добавление в зону ответственности основных ЦОД, уточнение технического проекта
5. Добавление в зону ответственности ИС и АРМ подразделений
6. Центр ГосСОПКА создан

“ИС в области действия центра ГосСОПКА” — это…

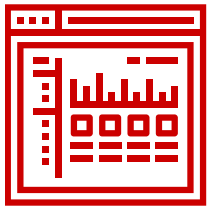
POSITIVE TECHNOLOGIES

В ИС реализованы “нормативные” меры защиты



Средства защиты ИС интегрированы с техническими средствами ГосСОПКА

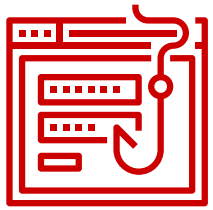
Если мер защиты ИС недостаточно – реализованы дополнительные меры защиты



Центр ГосСОПКА выполняет свои функции в отношении ИС

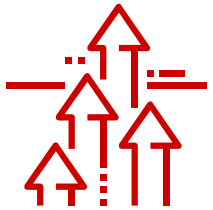
Вместо заключения

POSITIVE TECHNOLOGIES



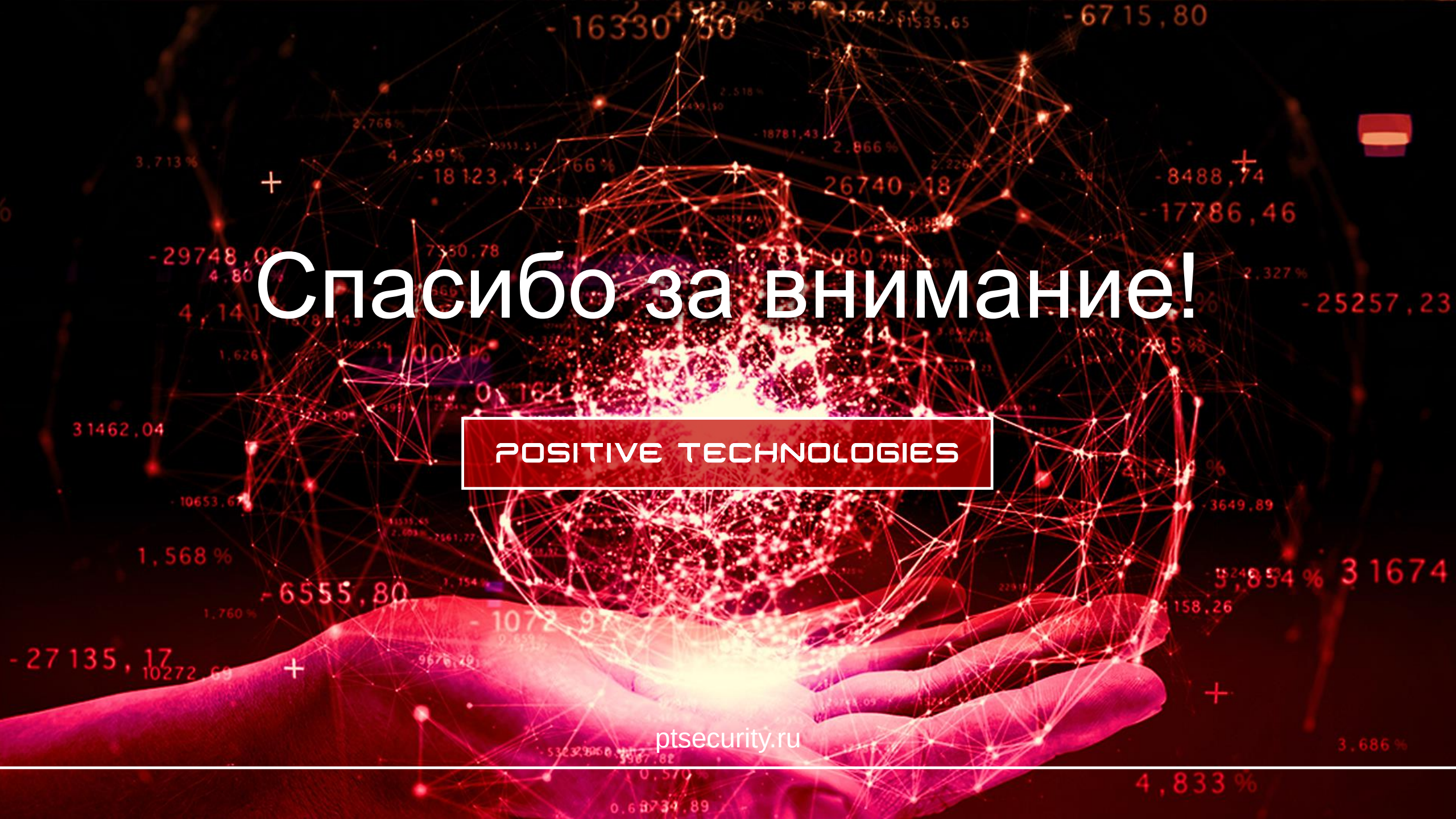
Важен практический результат, а не формальное соответствие

Самое сложное и трудоемкое – организация процессов



“Запланировали за год создать центр ГосСОПКА” – это даже не утопия

Вопросы?


Спасибо за внимание!
POSITIVE TECHNOLOGIES
ptsecurity.ru