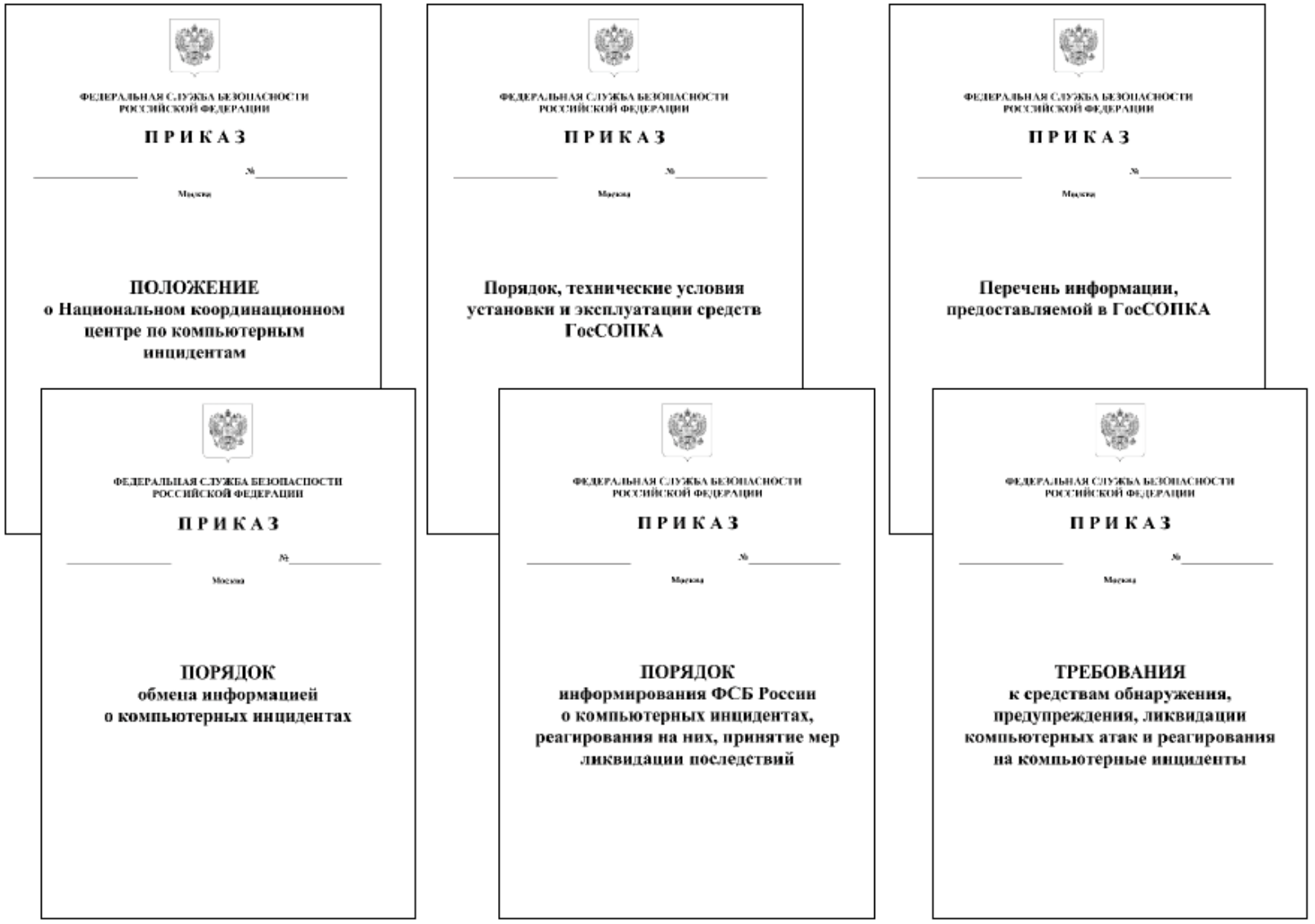
Дмитрий Кузнецов
Директор по методологии и стандартизации
dkuznetsov@ptsecurity.com

Требования к техническим средствам ГосСОПКА глазами проектировщика

Нормативная база в разработке ФСБ России для 187-ФЗ

POSITIVE TECHNOLOGIES



Развитием **ГосСОПКА** занимается **НКЦКИ** – Национальный координационный центр по компьютерным инцидентам

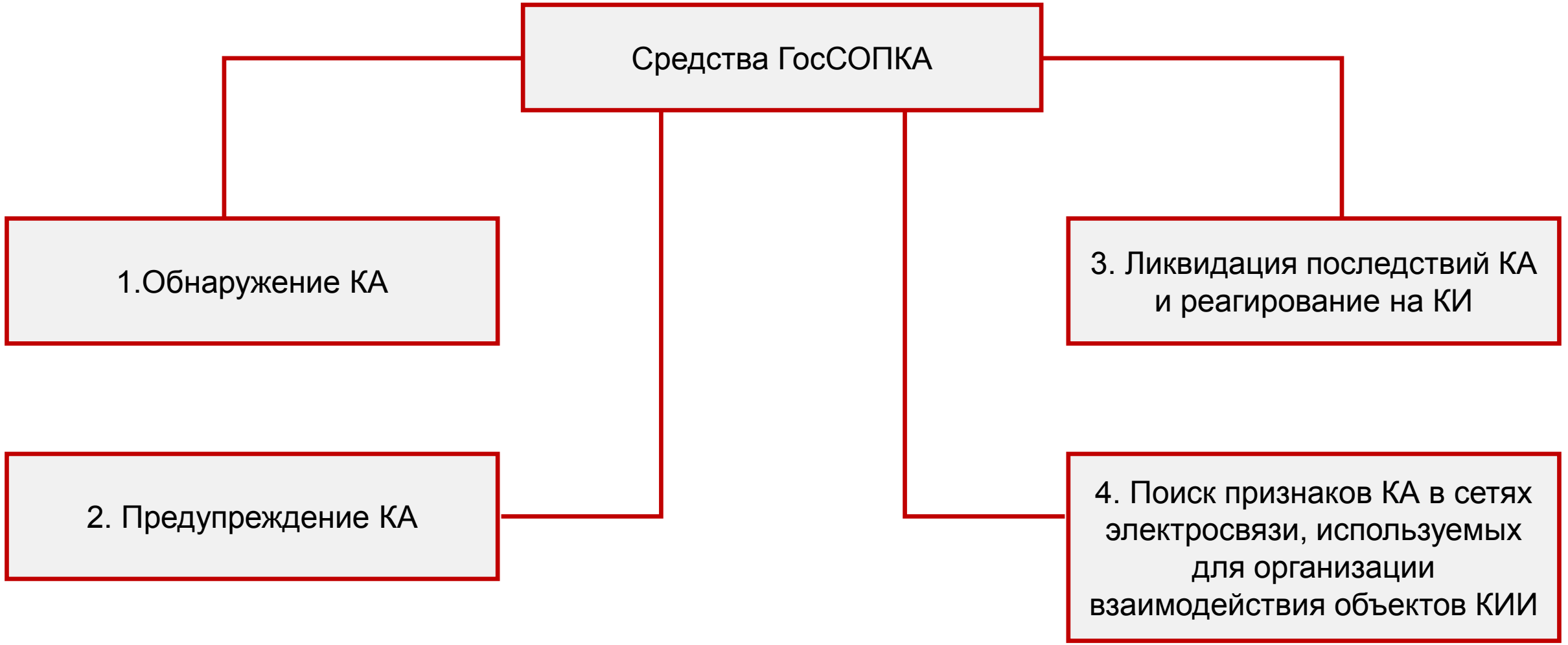
Russian GOV CERT

ГОССОПКА

Федеральная служба безопасности Российской Федерации

Требования ФСБ России: задачи средств ГосСОПКА

POSITIVE TECHNOLOGIES



Предупреждение компьютерных атак

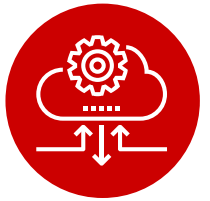
POSITIVE TECHNOLOGIES

- Сбор и обработка инвентаризационной информации
- Сбор и обработка справочной информации
  - Сведения о “репутации” узлов
  - Сведения о “владельцах” узлов
  - Сведения о геолокации узлов
- Сбор и обработка сведений о защищенности
- Учет угроз безопасности информации

САЗ

База знаний

Внешние источники

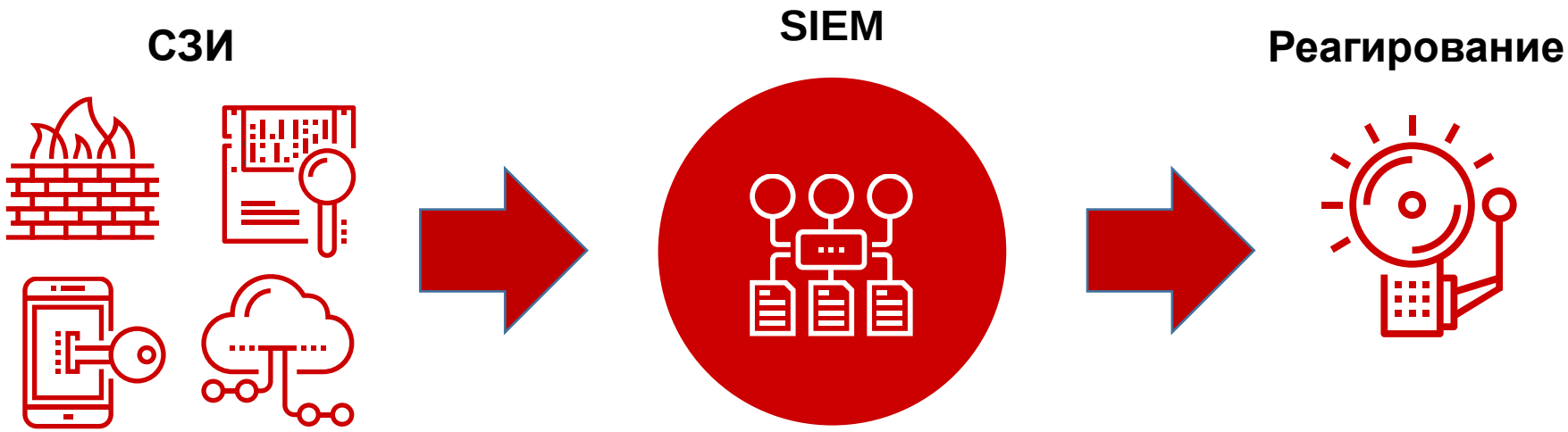


Обнаружение компьютерных атак

POSITIVE TECHNOLOGIES

Средства обнаружения КА – функциональные возможности решений класса SIEM

- Сбор и первичная обработка событий ИБ из различных источников
- Автоматический анализ событий ИБ и выявление КИ
- Ретроспективный анализ



Реагирование и ликвидация последствий

POSITIVE TECHNOLOGIES

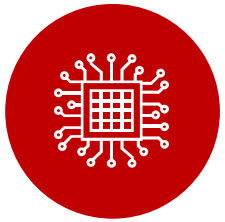
- Учет и обработка инцидентов
- Управление процессами реагирования на инциденты и ликвидации их последствий
- Обеспечение взаимодействия с НКЦКИ
- Информационно-аналитическое сопровождение

Поиск признаков КА в сетях связи

POSITIVE TECHNOLOGIES

- Контроль настроек телеком оборудования
- Обнаружение признаков управления
- Обнаружение аномалий трафика и признаков компьютерных атак
- Анализ и хранение копий трафика
- Извлечение файлов из трафика
- Уведомление о фактах обнаружения признаков компьютерных атак

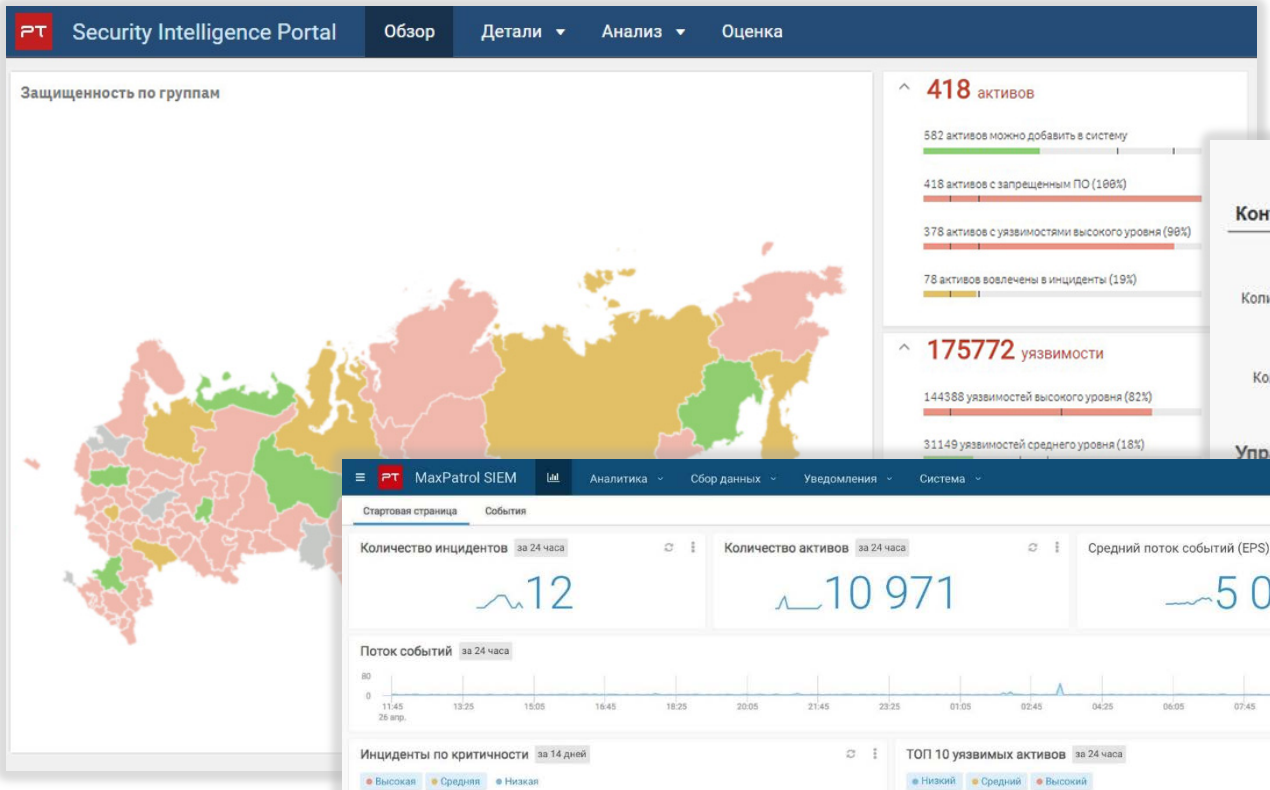
САЗ

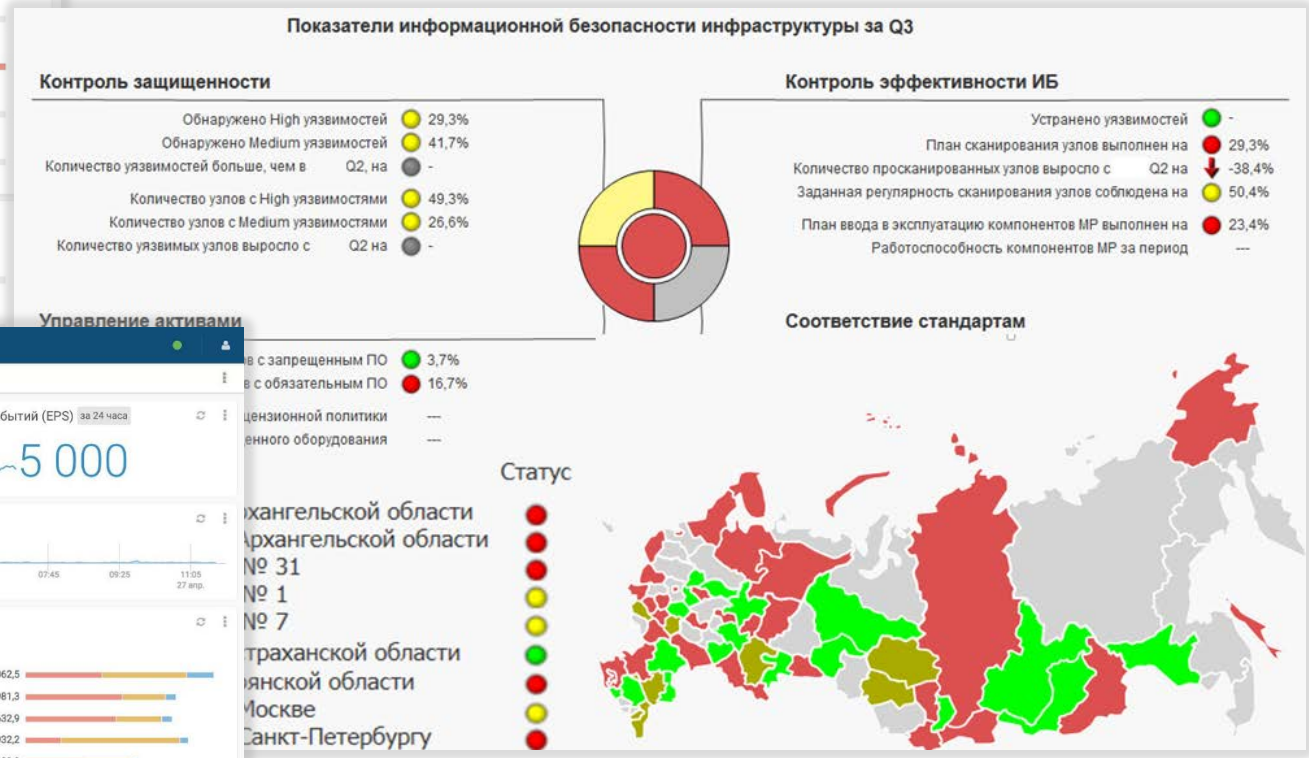


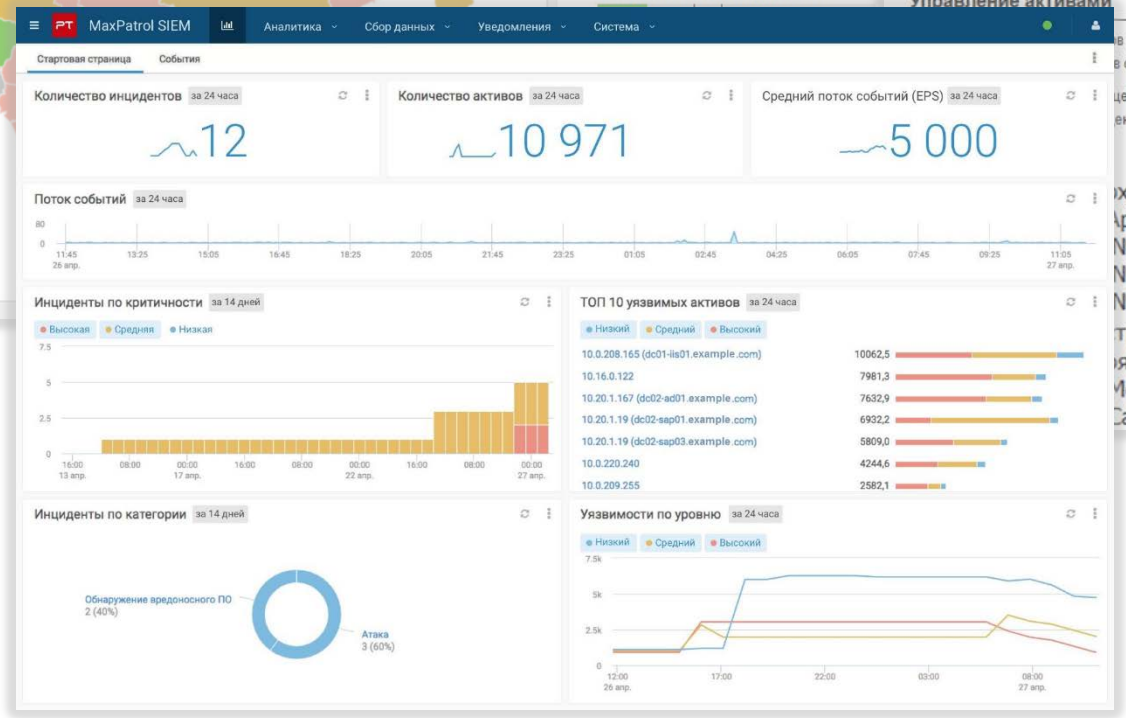
Средства анализа сетевого трафика

Визуализация

POSITIVE TECHNOLOGIES







Выводы

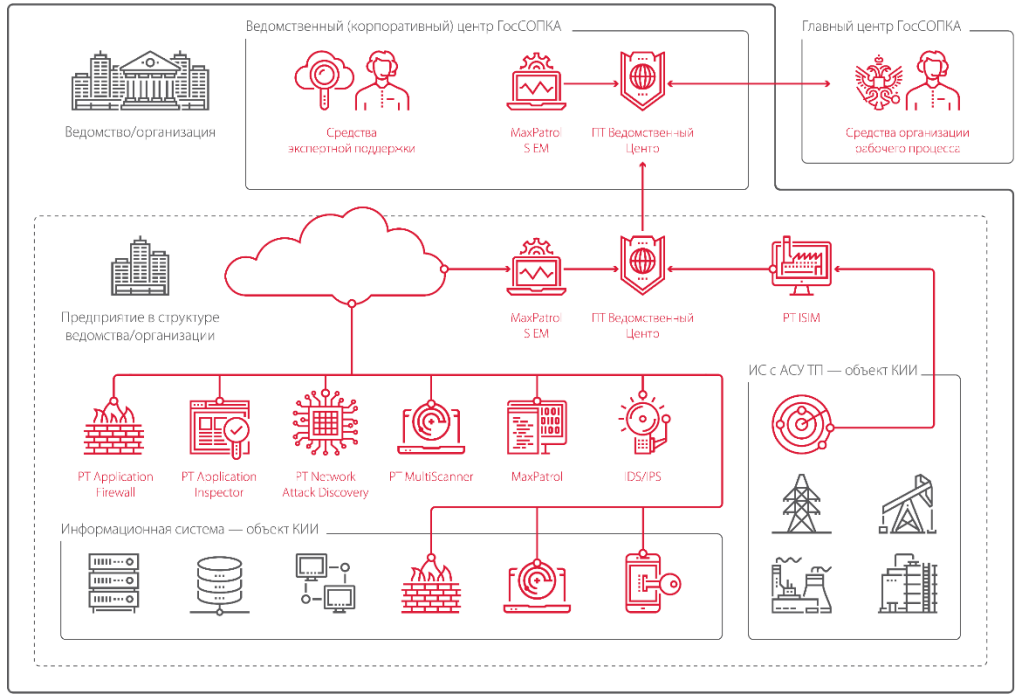
POSITIVE TECHNOLOGIES

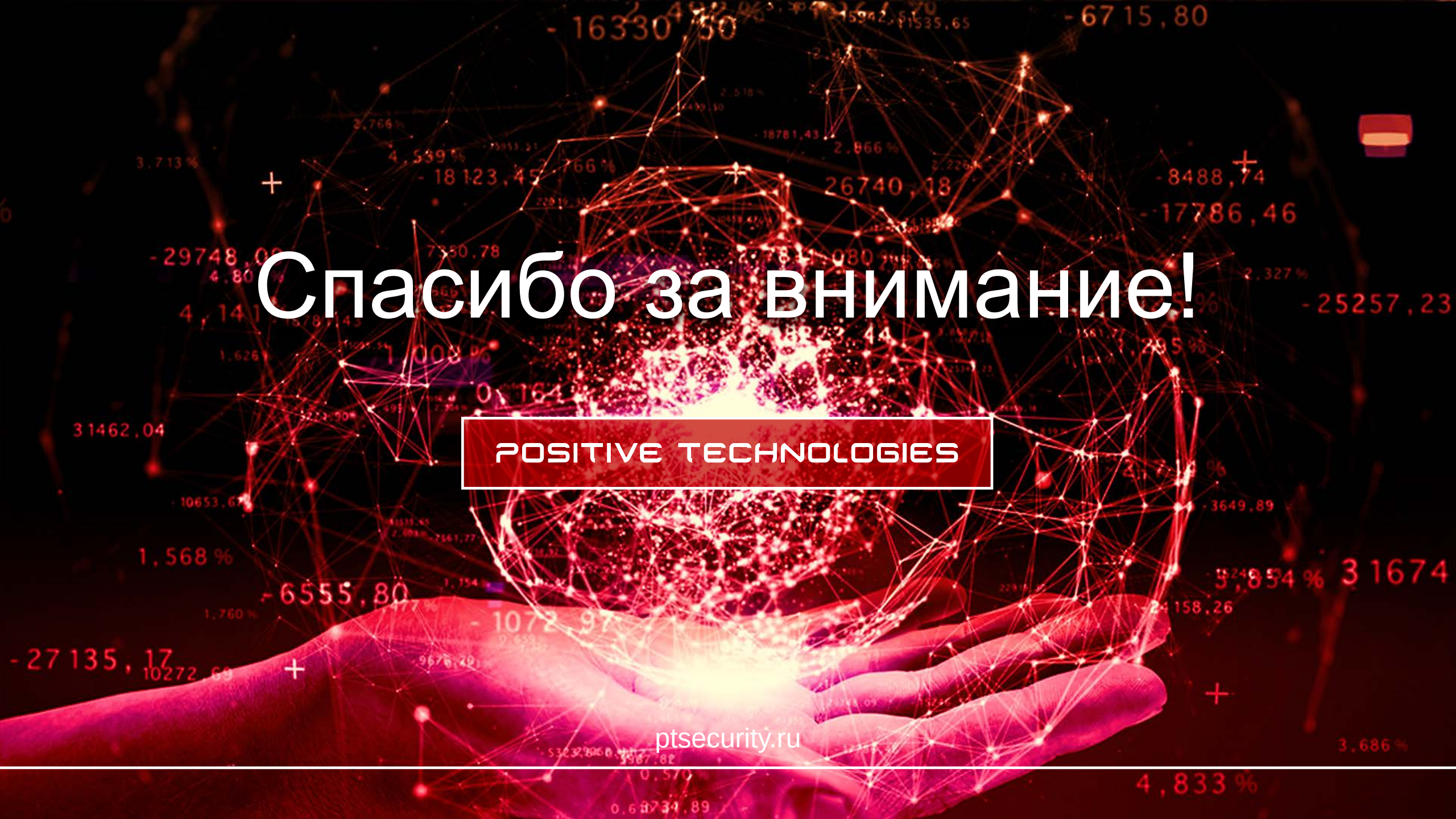
1. Средства ГосСОПКА субъекта КИИ – комплексная система

2. Только часть функций выполняется “коробочными” решениями

3. Средства ГосСОПКА взаимосвязаны с системой защиты объекта КИИ

4. Трудно обойтись без централизации




Спасибо за внимание!
POSITIVE TECHNOLOGIES
ptsecurity.ru