

POSITIVE TECHNOLOGIES

PT Platform 187

Реализация требований 187-ФЗ
для небольших инфраструктур





MaxPatrol SIEM

Система мониторинга событий и выявления инцидентов



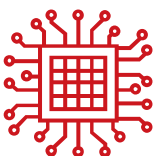
MaxPatrol 8

Система контроля защищенности



PT MultiScanner

Система выявления вредоносного контента



PT Network Attack Discovery

Система комплексного анализа сетевого трафика



PT Ведомственный центр

Система управления инцидентами и взаимодействия с НКЦКИ

Оptionальное подключение:

- + PT ISIM
- + PT Application Firewall
- + PT Application Inspector
- + Доп. хранилище до 36 ТБ

ФСТЭК России

[Приказ ФСТЭК России №235](#) к созданию систем безопасности значимых объектов в части выявления уязвимостей и обеспечения функционирования системы безопасности

[Приказ ФСТЭК России №239](#) к обеспечению безопасности значимых объектов в части аудита безопасности, антивирусной защиты на потоке, обнаружения вторжений, анализа сетевого трафика, выявления и реагирования на инциденты

ФСБ России

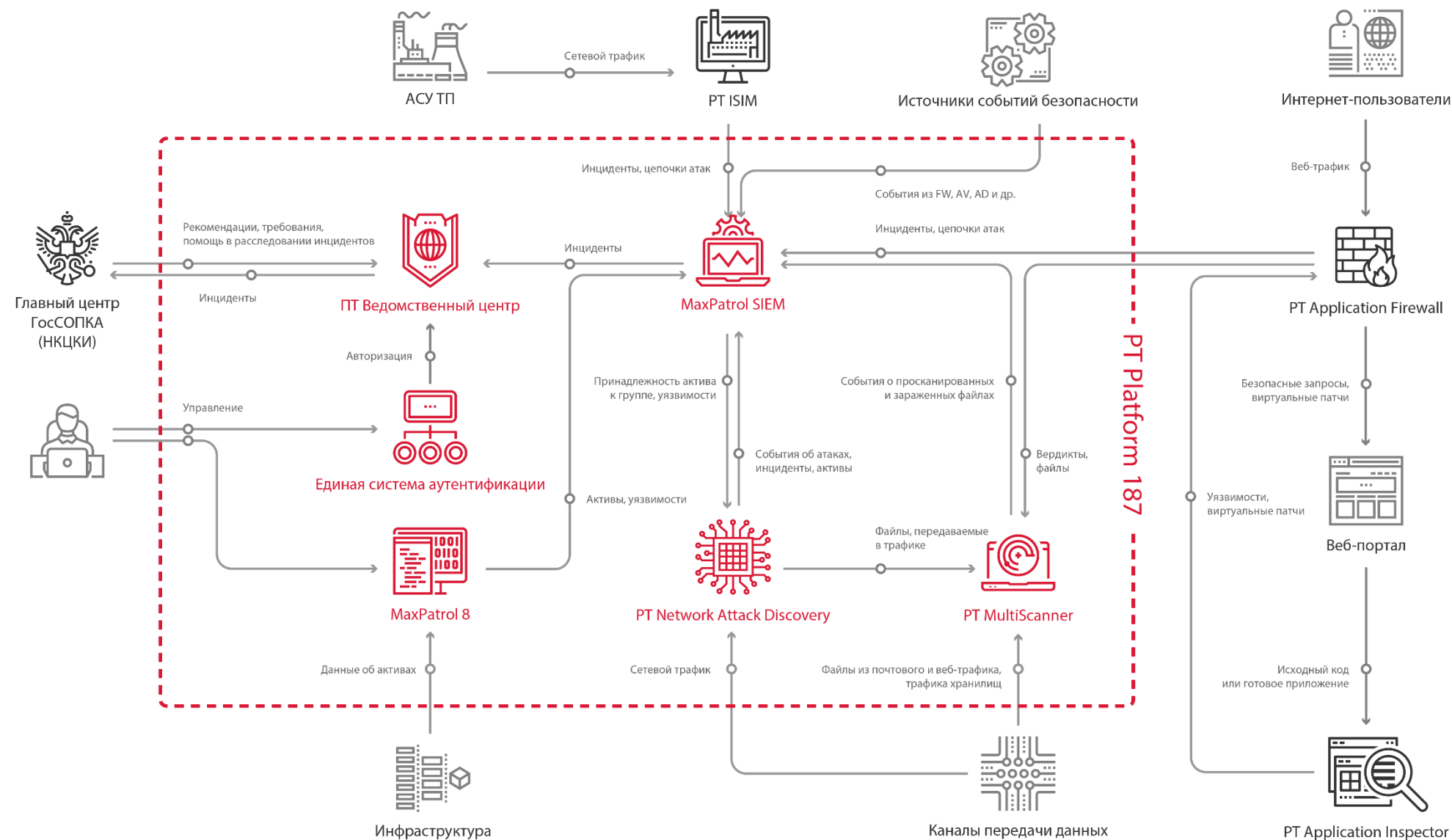
Методические рекомендации по построению центров ГосСОПКА в части реализации функций центра ГосСОПКА

[Приказ ФСБ России № 367](#) об утверждении Перечня информации, представляемой в ГосСОПКА, и Порядка представления информации в ГосСОПКА в части подключения к технической инфраструктуре НКЦКИ и обмена информацией об инцидентах в соответствии с определенными НКЦКИ форматами

[Приказ ФСБ России № 368](#) об утверждении Порядка обмена информацией о компьютерных инцидентах в части взаимодействия с НКЦКИ через техническую инфраструктуру

[Требования к средствам](#) ГосСОПКА в части анализа событий безопасности, выявления инцидентов, выявления уязвимостей, взаимодействия с НКЦКИ

Архитектура PT Platform 187



Для небольших инфраструктур – не более 250 узлов



Продажи в виде ПАК = сервер + ПО

Пример сценария использования



Ограничения

РТ

до **250** узлов

включаются в мониторинг
MaxPatrol SIEM
и MaxPatrol 8

до **1000** Мбит/с

пропускная способность
PT Network Attack
Discovery

до **3000** файлов

в час - пропускная
способность
PT MultiScanner



В реестре российского ПО:

- MaxPatrol 8
- MaxPatrol SIEM
- PT MultiScanner
- ПТ Ведомственный центр
- PT Network Attack Discovery



Сертификаты ФСТЭК России:

- MaxPatrol 8 – сертификат № 2922
- MaxPatrol SIEM – сертификат № 3734
- PT Network Attack Discovery – сертификат № 4042
- PT MultiScanner coming soon

Плюсы использования платформы

PT



Соответствие
законодательству



Взаимодействие
с НКЦКИ



Быстрая
инсталляция



Единая система
авторизации

Краткое описание PT Platform 187:

ptsecurity.com/upload/corporate/ru-ru/products/platform-187/PT-Platform-187-rus.pdf



Перед нами стоит серьезная задача — оперативно построить один из первых региональных центров ГосСОПКА и обеспечить безопасность объектов КИИ органов власти Калининградской области. Благодаря комплексному решению PT Platform 187 за месяц удалось запустить центр безопасности и начать выполнение требований законодательства.



Сергей Чуприс,
Директор Калининградского государственного научно-исследовательского центра информационной и технической безопасности

[Читать историю успеха](#)

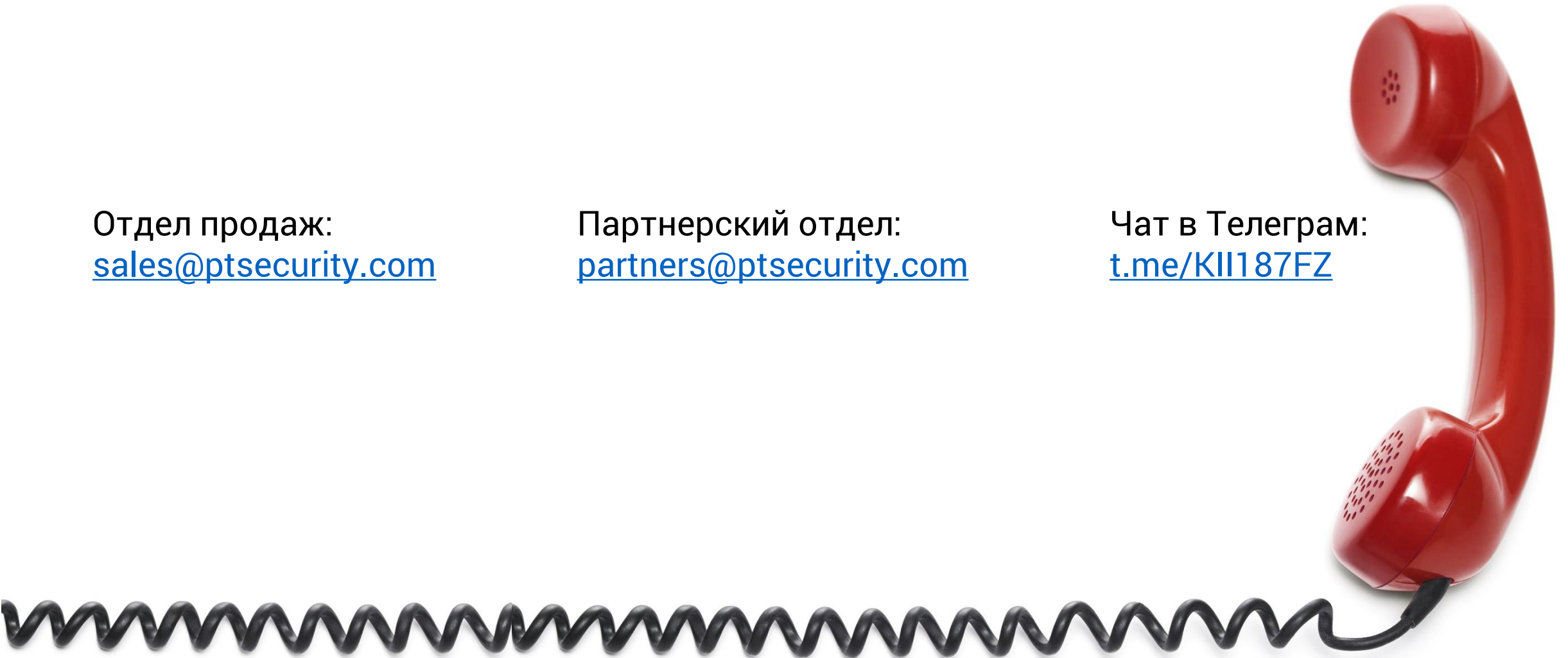
Продолжим общение

PT

Отдел продаж:
sales@ptsecurity.com

Партнерский отдел:
partners@ptsecurity.com

Чат в Телеграм:
t.me/K11187FZ





План по выполнению требований 187-ФЗ

ptsecurity.com/ru-ru/research/knowledge-base/plan-187-fz-full-version/



Обзор нормативно-правовых актов

ptsecurity.com/ru-ru/research/knowledge-base/terminology-gossopka-kii-full-version/

POSITIVE TECHNOLOGIES

Спасибо
за внимание

