PT Platform 187 – фундамент построения центра ГосСОПКА.

Опыт запуска центра кибербезопасности за один месяц

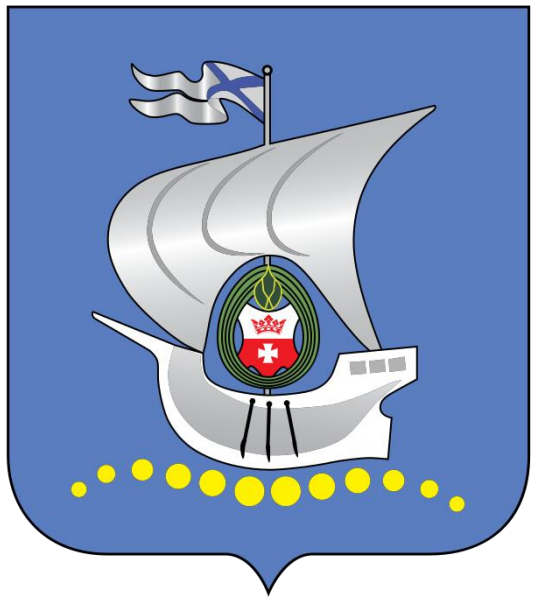
POSITIVE TECHNOLOGIES

ptsecurity.com

Цель

POSITIVE TECHNOLOGIES

Оперативно построить один из первых региональных центров ГосСОПКА и обеспечить безопасность объектов КИИ органов власти Калининградской области.

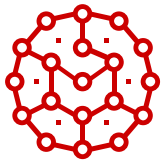


Задачи обеспечения безопасности объекта КИИ

POSITIVE TECHNOLOGIES

Защита от неправомерного доступа к информации, обрабатываемой КИИ

Защита от негативных воздействий, в результате которых может быть нарушено и (или) прекращено функционирование объекта КИИ

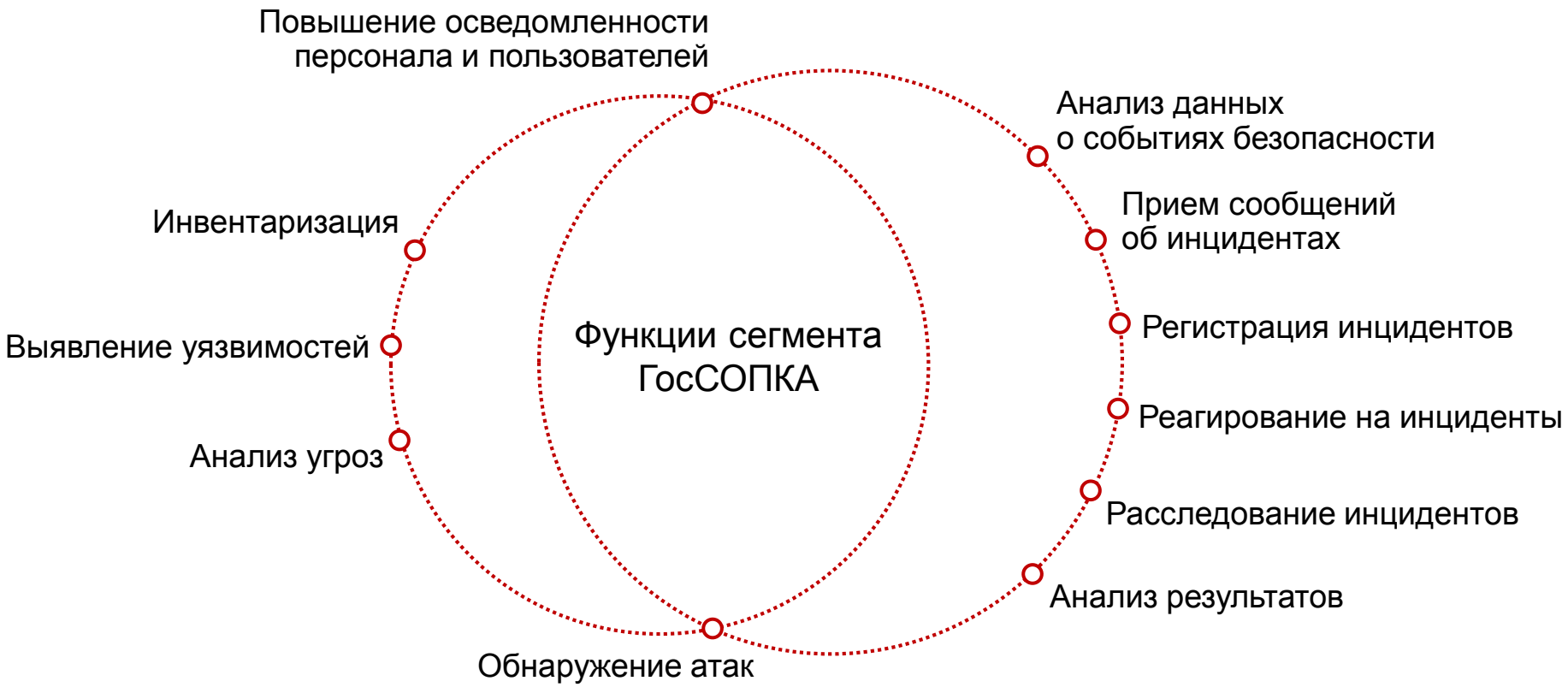


Восстановление функционирования объекта КИИ

Непрерывное взаимодействие с ГосСОПКА

Методические рекомендации ФСБ России по построению центров ГосСОПКА

POSITIVE TECHNOLOGIES



MaxPatrol 8

MaxPatrol SIEM

MaxPatrol SIEM

ПТ Ведомственный центр

PT MultiScanner

PT Network Attack Discovery

PT Platform 187

Реализация основных требований 187-ФЗ
и функций центров ГосСОПКА
для небольших обособленных инфраструктур

Состав PT Platform 187

POSITIVE TECHNOLOGIES

MaxPatrol SIEM

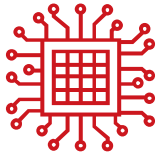
Система мониторинга событий и выявления инцидентов

MaxPatrol 8

Система контроля защищенности

PT MultiScanner

Система выявления вредоносного контента



PT Network Attack Discovery

Система комплексного анализа сетевого трафика

ПТ Ведомственный центр

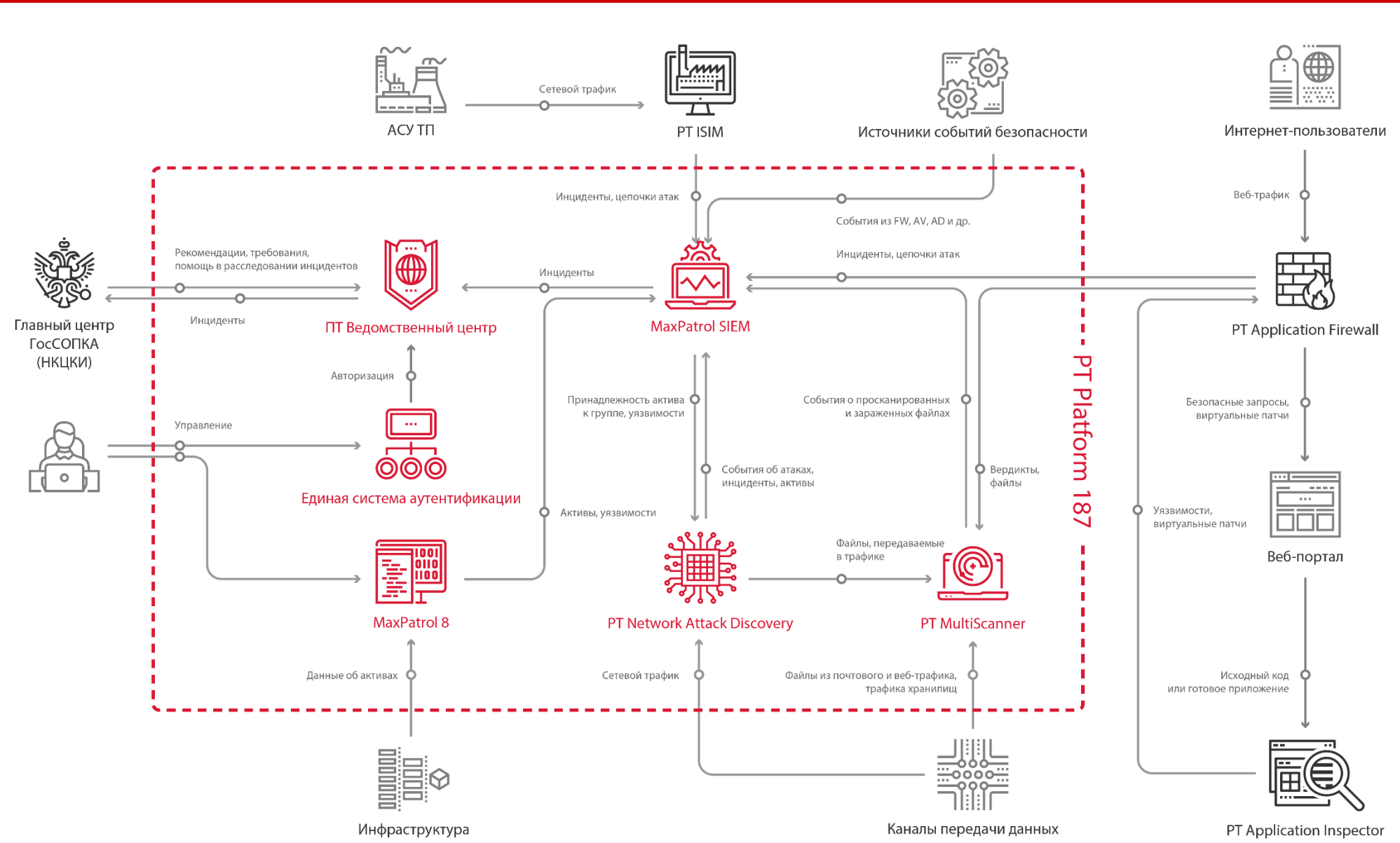
Система управления инцидентами и взаимодействия с НКЦКИ

Опциональное подключение:

+ PT ISIM
+ PT Application Firewall
+ PT Application Inspector

Архитектура PT Platform 187

POSITIVE TECHNOLOGIES



Для небольших инфраструктур – не более 250 узлов

Продажи в виде ПАК = сервер + ПО

Сложности внедрения и их решение

POSITIVE TECHNOLOGIES

MaxPatrol 8

- Сетевой доступ
- Учетные записи

Отлично документированная схема сетевого взаимодействия и права доступа

MaxPatrol SIEM

- Сетевой доступ
- Настройки аудита

Готовые рекомендации от PT ESC по расширенному аудиту событий на источниках

Итоги проекта

POSITIVE TECHNOLOGIES

С помощью PT Platform 187 региональный центр безопасности на базе КГ НИЦ выполняет следующие задачи:

- Непрерывно инвентаризует информационные ресурсы;
- Проводит анализ защищенности и выявляет уязвимости;
- Предотвращает распространение вредоносного ПО;
- Контролирует и анализирует сетевой трафик;
- Обрабатывает инциденты и помогает управлять процессом реагирования в соответствии с методическими рекомендациями ФСБ России по созданию центров ГосСОПКА.

Плюсы использования платформы

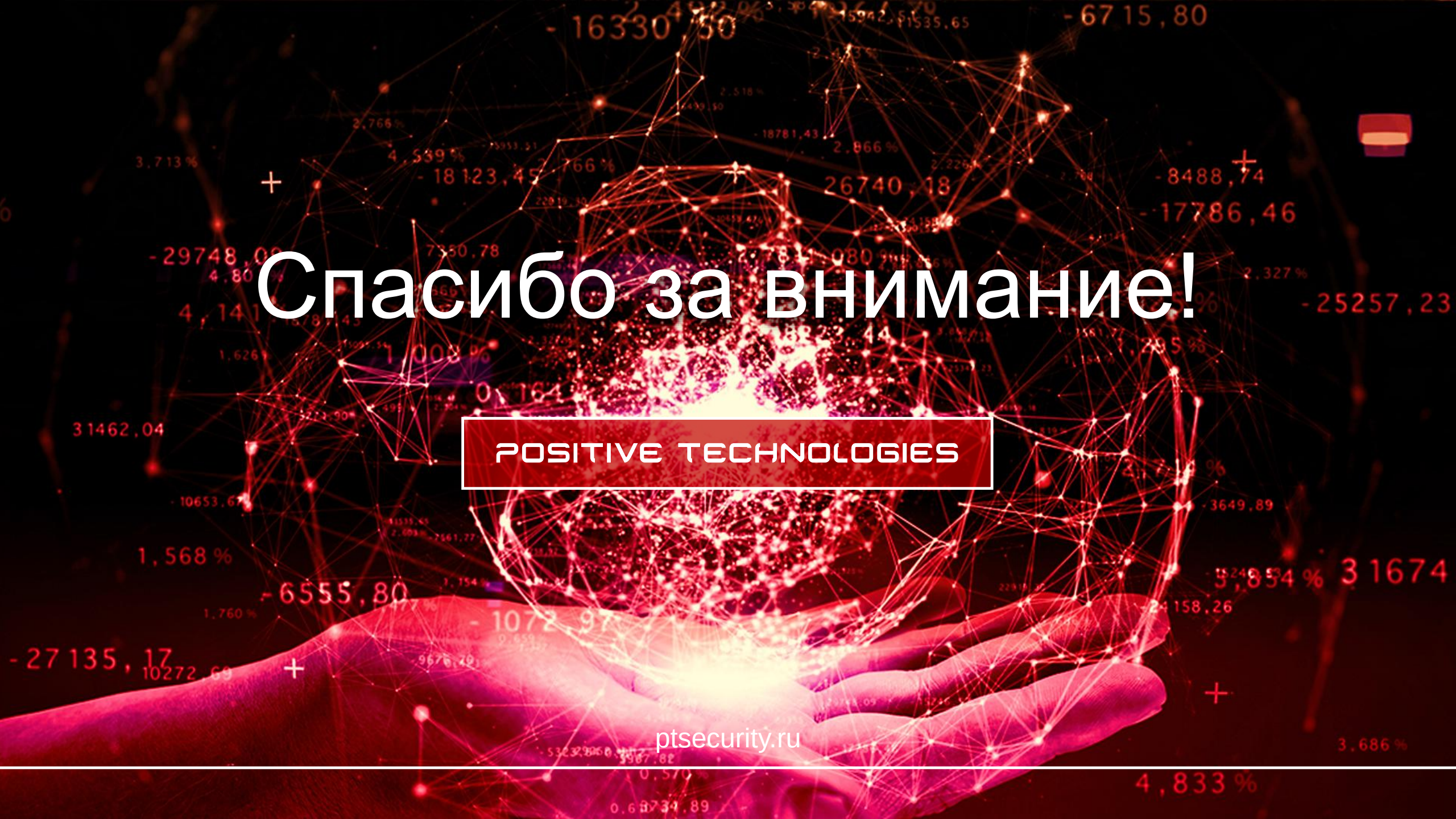
POSITIVE TECHNOLOGIES

Соответствие законодательству

Взаимодействие с НКЦКИ

Быстрая инсталляция

Единая система авторизации


Спасибо за внимание!
POSITIVE TECHNOLOGIES
ptsecurity.ru