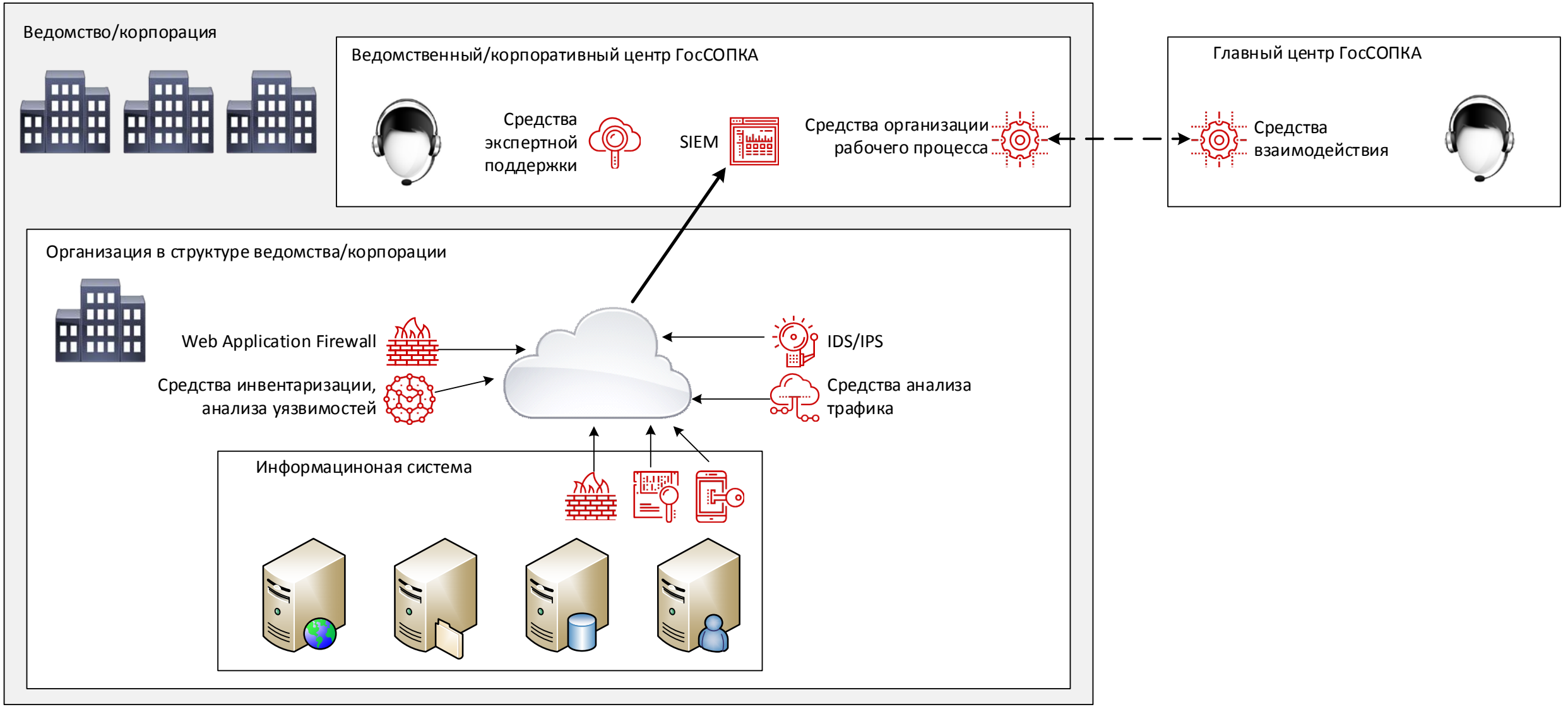
Дмитрий Кузнецов
Директор по методологии и стандартизации
dkuznetsov@ptsecyurity.com

Инструментарий ГосСОПКА

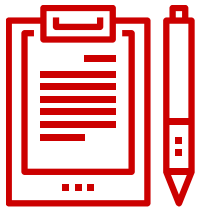
Еще раз об иерархии

POSITIVE TECHNOLOGIES

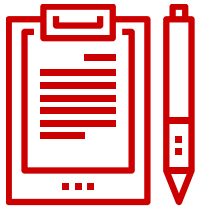


Где описаны инструменты

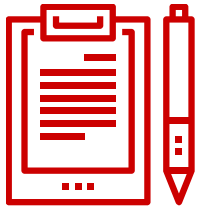
POSITIVE TECHNOLOGIES



“Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты”



“Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования”

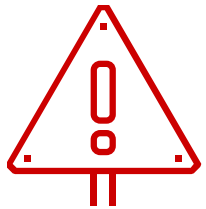


“Меры защиты информации в государственных информационных системах”

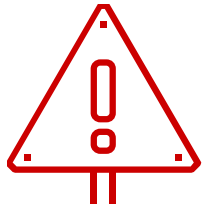
СТО и РС БР ИББС

Общие требования

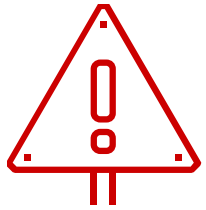
POSITIVE TECHNOLOGIES



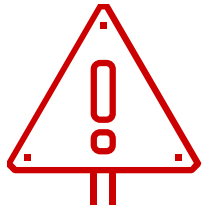
Отсутствие возможности несанкционированной передачи информации



Отсутствие принудительного обновления зарубежным производителем



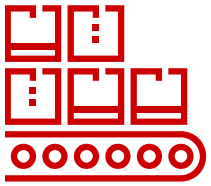
Возможность модернизации, гарантийной и технической поддержки без участия компаний с иностранным участием



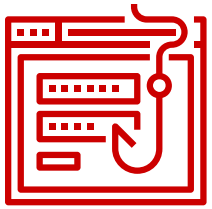
Отсутствие недекларированных возможностей

Функции средств ГосСОПКА

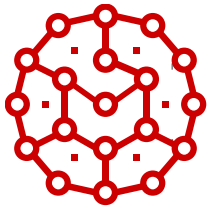
POSITIVE TECHNOLOGIES



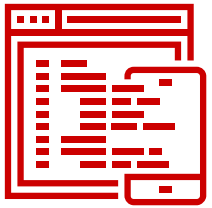
Сбор информации о защищаемых объектах



Менеджмент угроз



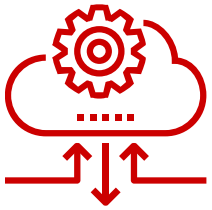
Поиск и анализ уязвимостей



Сбор и анализ событий безопасности

Поиск признаков сетевых атак

Автоматизация реагирования на инцидент



Автоматизация взаимодействия с НКЦКИ

Информационно-аналитическое сопровождение

Из интересного

POSITIVE TECHNOLOGIES

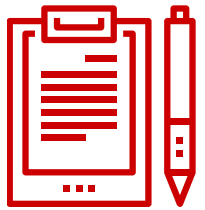
"*Обнаружение атак*" не равно "*использованию СОВ/СОА*"

Работа с типовыми угрозам и типовыми сценариями реагирования на инциденты

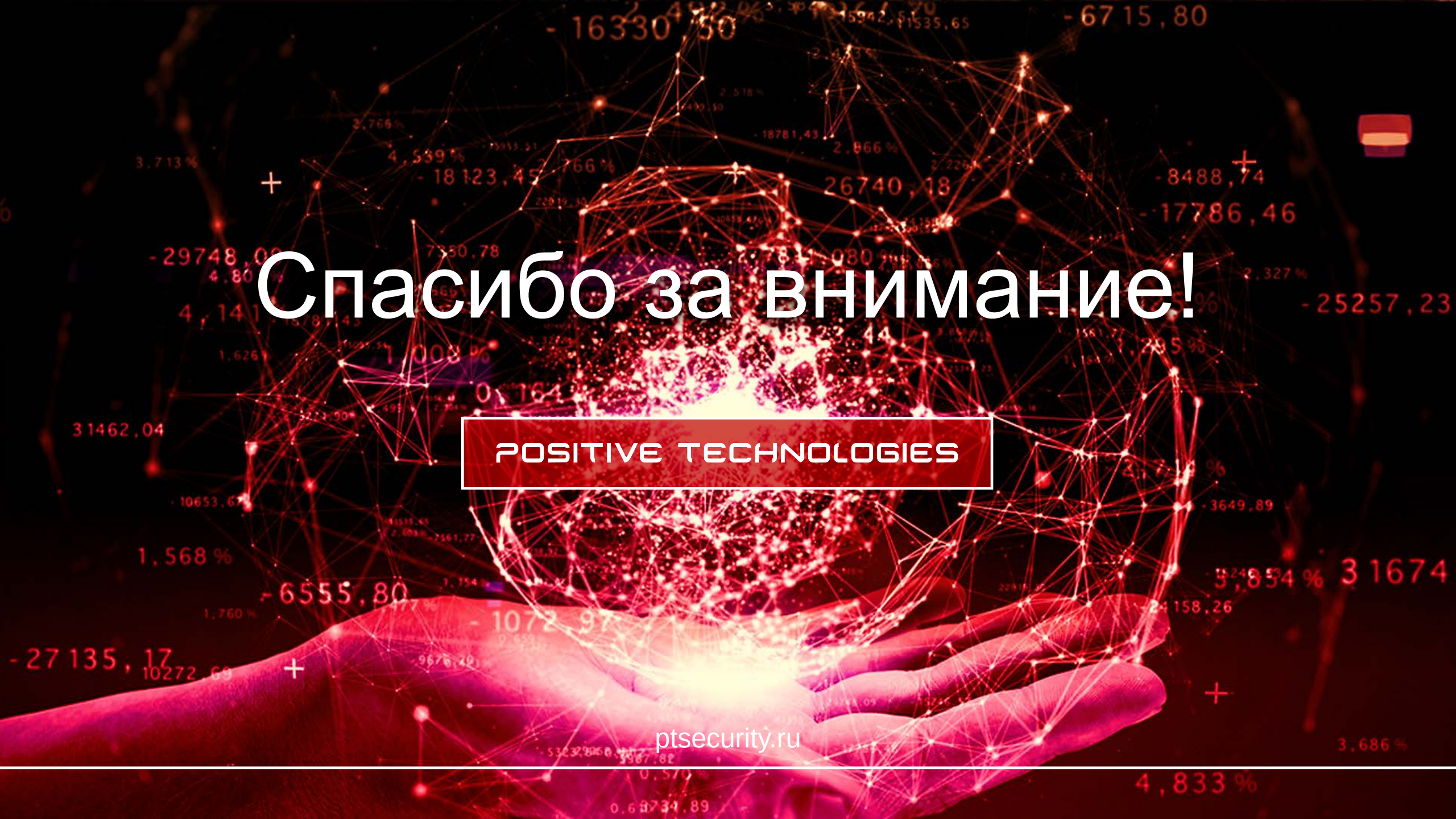
"Онлайн-анализ" угроз

Особая роль Банка России

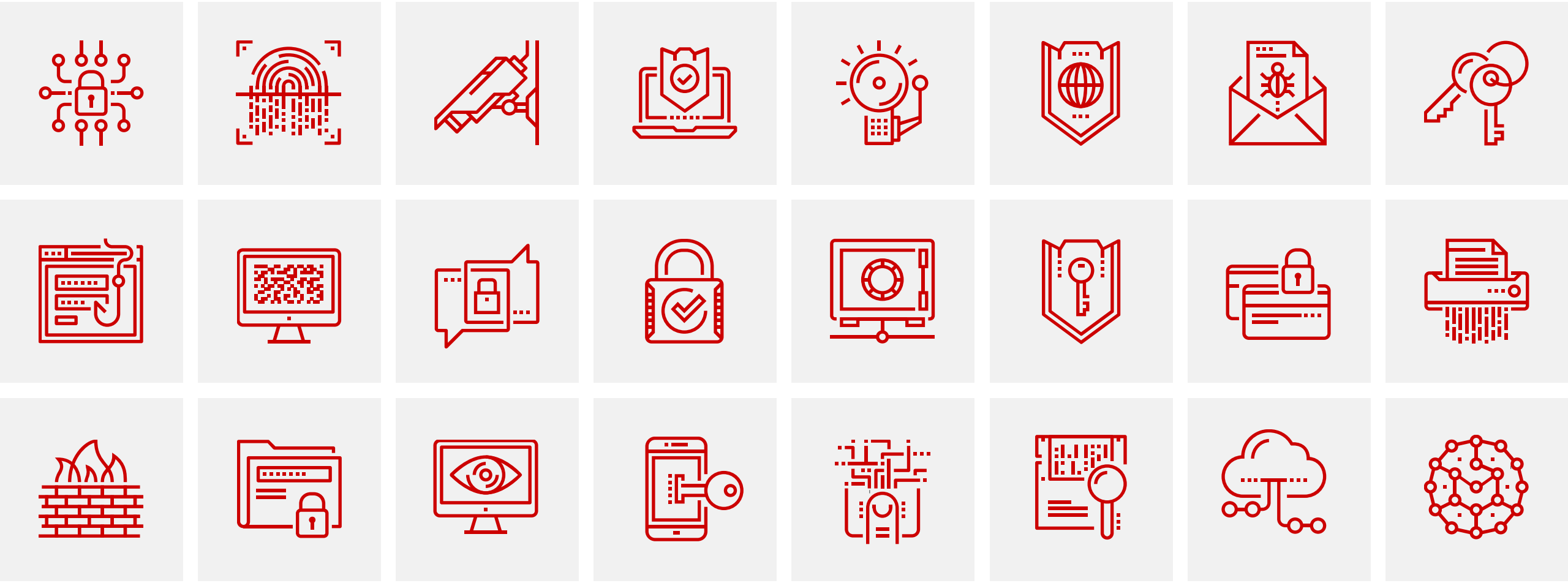
"*Технические средства ГосСОПКА*" - не "*средства защиты информации*"



СТО/РС БР ИББС как источники решений

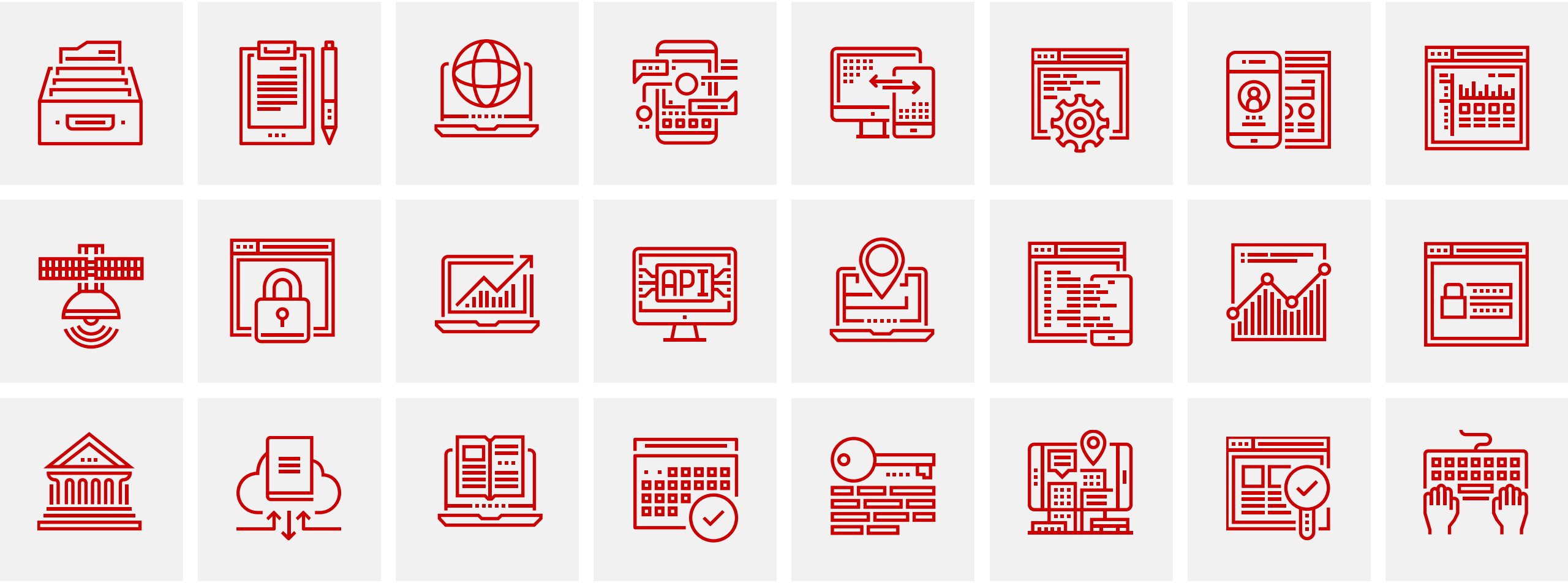

Спасибо за внимание!
POSITIVE TECHNOLOGIES
ptsecurity.ru

POSITIVE TECHNOLOGIES

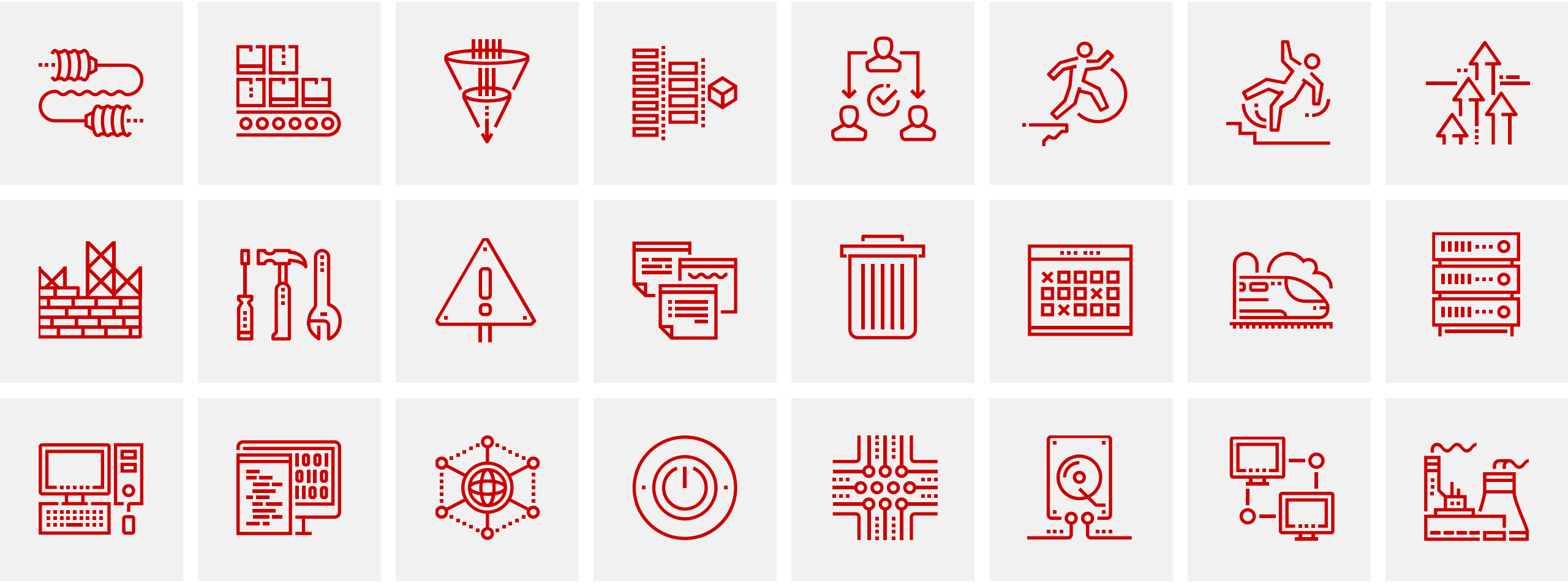


POSITIVE TECHNOLOGIES

POSITIVE TECHNOLOGIES



POSITIVE TECHNOLOGIES



PT ISIM	PT AF	PT AI	PT SS7 AD	PT MS