Илья Егоркин
Руководитель специальных проектов
Positive Technologies

ГосСОПКА. Дорогу осилит идущий!

POSITIVE TECHNOLOGIES

ptsecurity.com

Вместо статистики

POSITIVE TECHNOLOGIES

*ФСБ РФ обнаружила вредоносное ПО для **шпионажа в госучреждениях**.*

Scarab attackers took aim at select Russian targets since 2012

*Турецкие хакеры осуществили **дефейс сайта посольства РФ** в Израиле*

*Хакеры сняли почти **100 миллионов рублей** со счетов коммерческого банка*

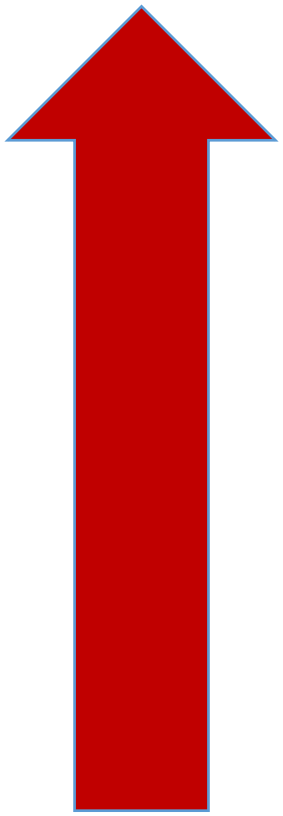
Вице Президент США Джо Байден обещает кибератаки на инфраструктуру России

Как вы узнаете об инциденте?

POSITIVE TECHNOLOGIES

КАК ЕСТЬ

КАК НАДО



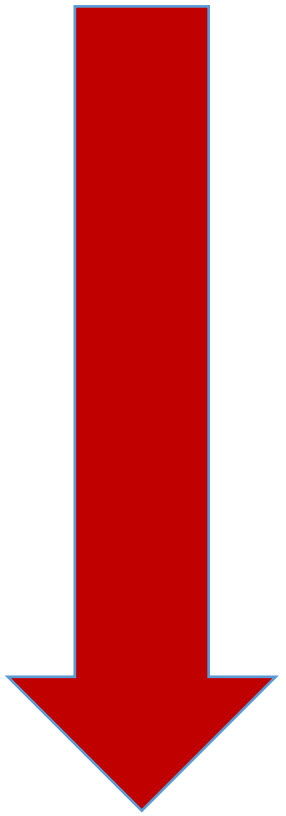
Вас «громко порадуют»

Вас «тихо порадуют»

«Почувствуете»

Выявят приглашенные эксперты

Выявят собственные эксперты



Кто ходит в гости по утрам?

POSITIVE TECHNOLOGIES

Мошенники

Криминальные группировки

Хактивисты

Экспериментаторы

Спонсируемые государством команды

ГосСОПКА в терминал SOC

POSITIVE TECHNOLOGIES

1. **Обнаружение, предупреждение и ликвидация последствий компьютерных атак**, направленных на контролируемые информационные ресурсы.
2. **Проведение мероприятий по оценке степени защищенности** контролируемых информационных ресурсов.
3. **Поведение мероприятий по установлению причин компьютерных инцидентов**, вызванных компьютерными атаками на контролируемые информационные ресурсы.
4. **Сбор и анализ данных о состоянии информационной безопасности** в контролируемых информационных ресурсах.
5. **Осуществление взаимодействия** между центрами;
6. **Информирование заинтересованных лиц и субъектов Системы** по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак.

1. Prevention of cybersecurity incidents through proactive:
   a. Continuous threat analysis
   b. Network and host scanning for vulnerabilities
   c. Countermeasure deployment coordination
   d. Security policy and architecture consulting.
2. Monitoring, detection, and analysis of potential intrusions in real time and through historical trending on security-relevant data sources
3. Response to confirmed incidents, by coordinating resources and directing use of timely and appropriate countermeasures
4. Providing situational awareness and reporting on cybersecurity status, incidents, and trends in adversary behavior to appropriate organizations
5. Engineering and operating CND technologies such as IDSes and data collection/analysis systems.

MITRE Carson Zimmerman
Ten Strategies of a World-Class Cybersecurity Operations Center

Три уровня или идем от простого к сложному

POSITIVE TECHNOLOGIES

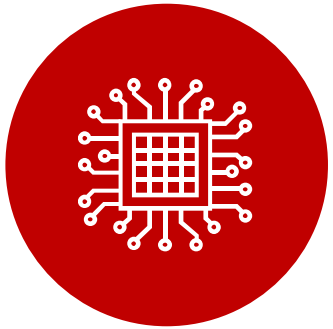
1. Контроль внешнего периметра
2. Контроль внутреннего периметра
3. Защита от таргетированных атак

POSITIVE TECHNOLOGIES

Подготовка

Инвентаризация информационных ресурсов

Анализ уязвимостей информационных ресурсов



Анализ угроз информационной безопасности

Антивирусная защита информационных ресурсов

POSITIVE TECHNOLOGIES

Обнаружение и реагирование

Прием сообщений о возможных инцидентах от персонала и пользователей информационных ресурсов

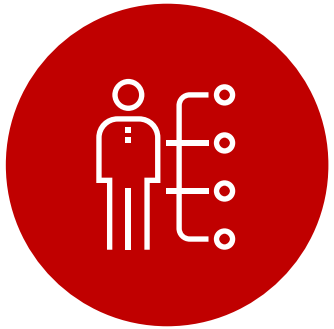
Обнаружение компьютерных атак

Анализ данных о событиях безопасности

Регистрация инцидентов

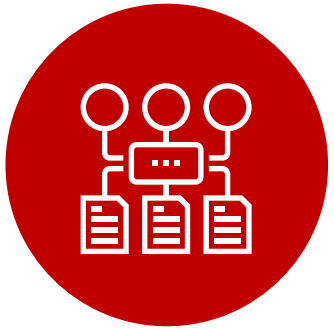
POSITIVE TECHNOLOGIES

Анализ и взаимодействие



Повышение квалификации персонала информационных ресурсов

Реагирование на инциденты и ликвидация их последствий



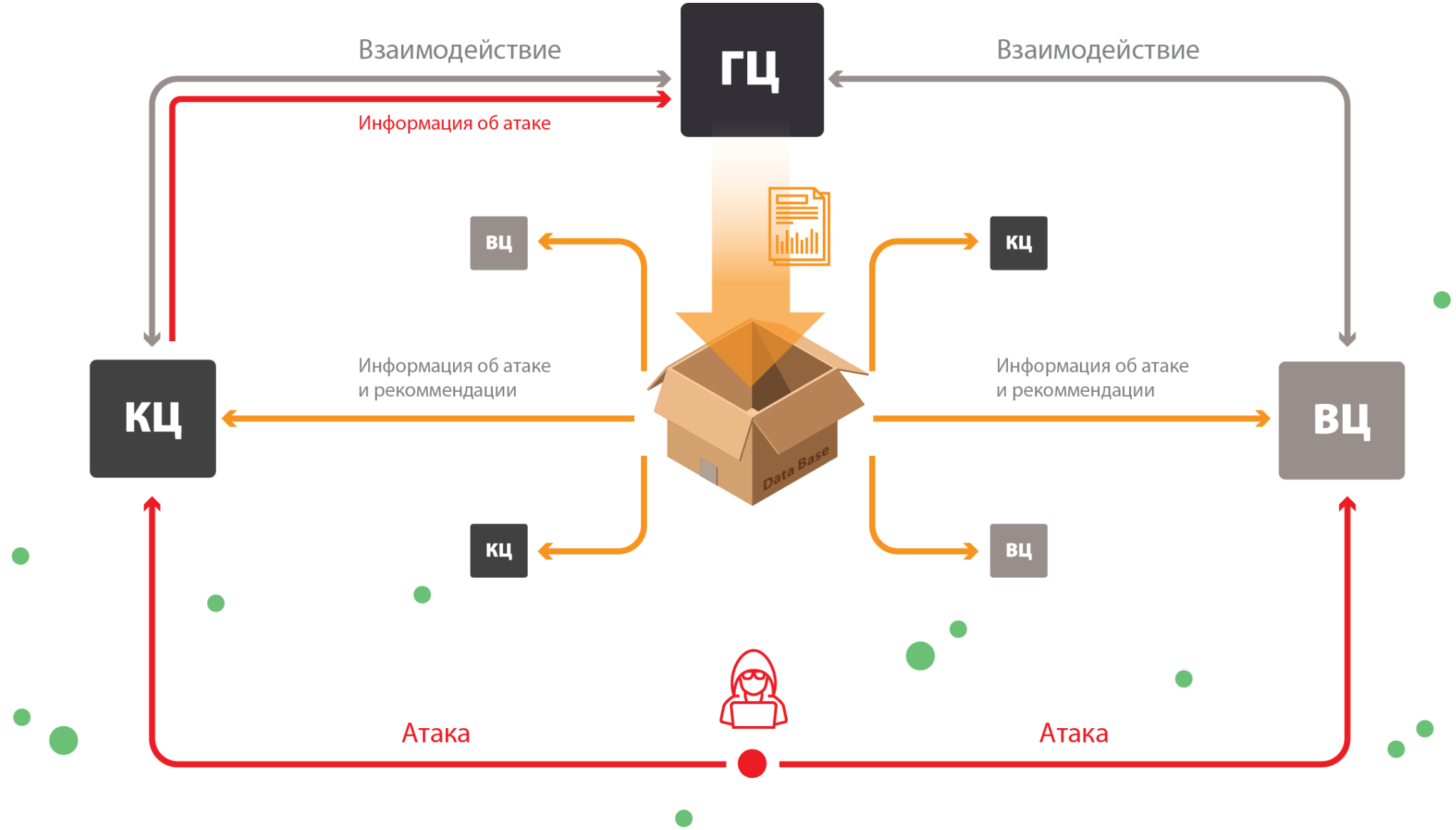
Установление причин инцидентов

Анализ результатов устранения последствий инцидентов

Взаимодействие

Практическая польза от взаимодействия

POSITIVE TECHNOLOGIES



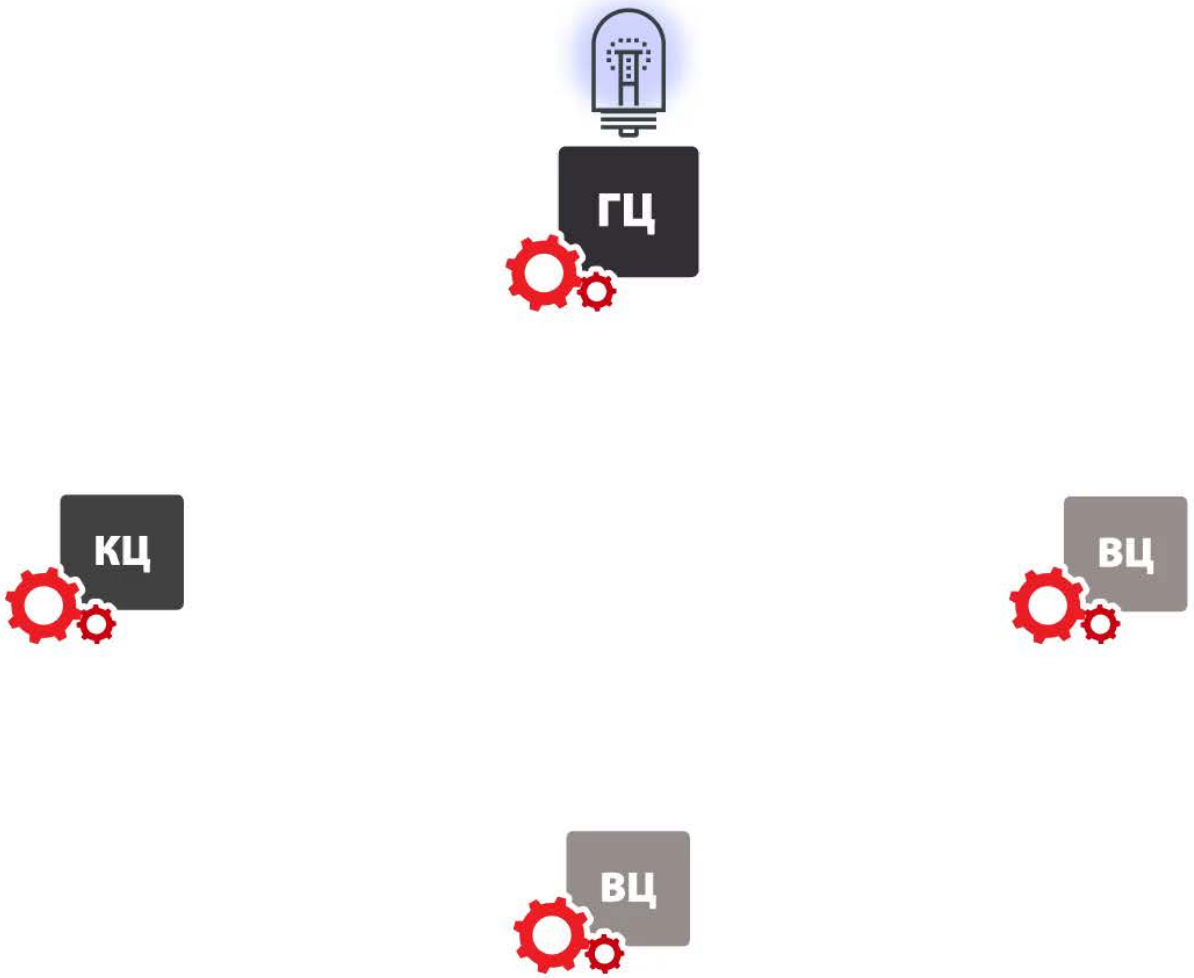
Информация для обмена

POSITIVE TECHNOLOGIES

- Зона ответственности
- Защищенность
- Угрозы
- Эксплоиты
- Индикаторы
- TTP (Kill chains)
- Рекомендации и уведомления
- **Экспертиза**

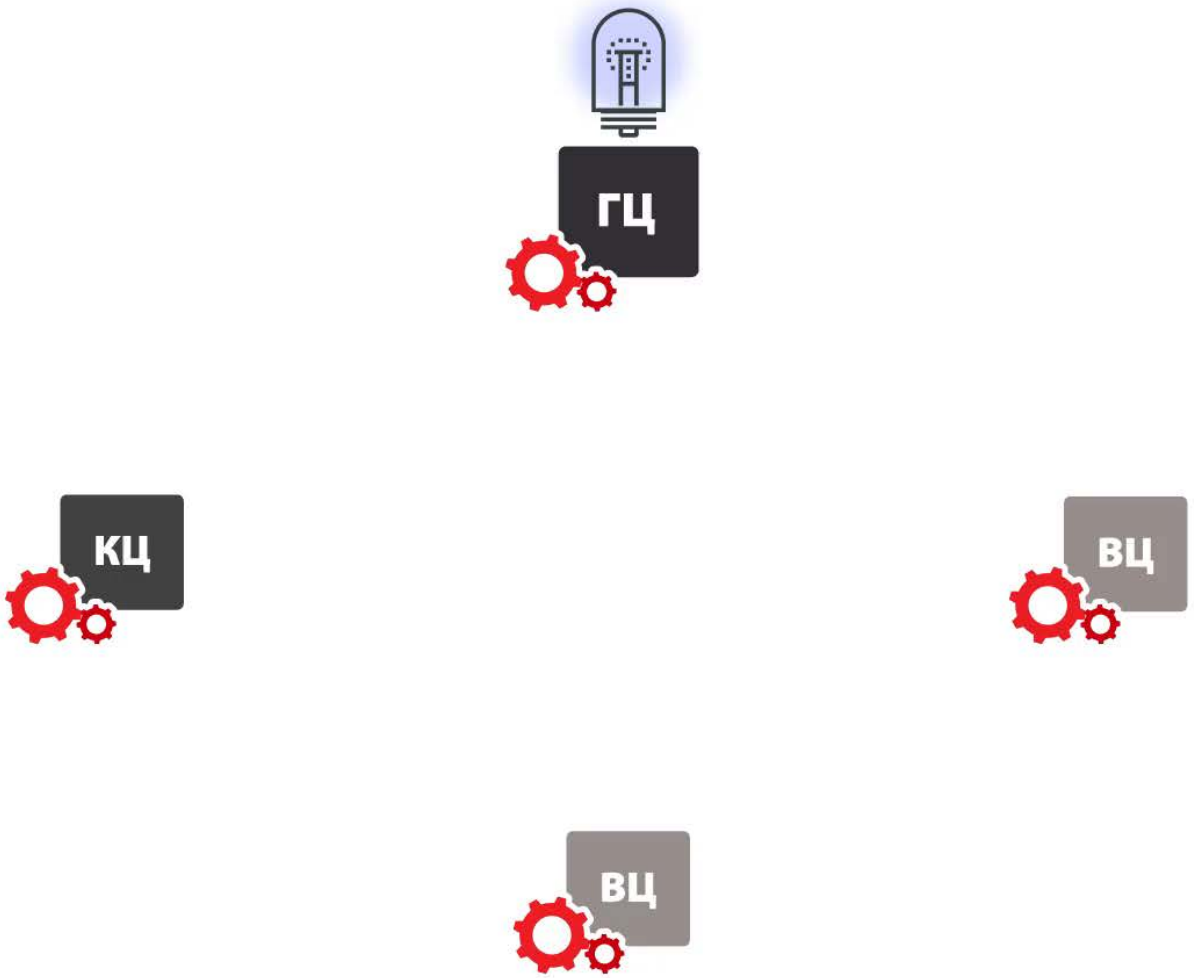
В результате имеем

POSITIVE TECHNOLOGIES



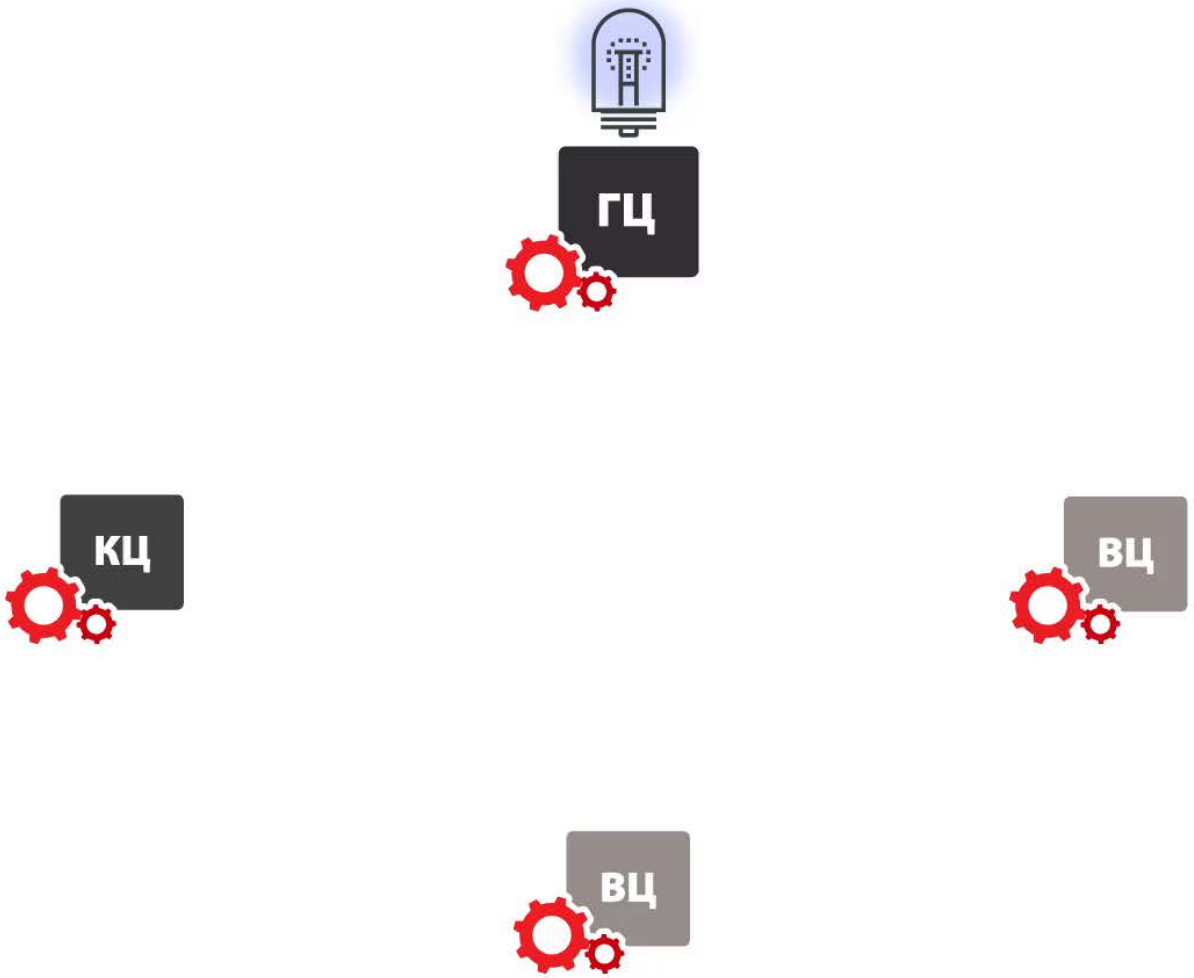
В результате имеем

POSITIVE TECHNOLOGIES



В результате имеем

POSITIVE TECHNOLOGIES




Спасибо!
POSITIVE TECHNOLOGIES
ptsecurity.ru