Шаг за шагом на пути к созданию регионального SOC.

Опыт Свердловской области в применении комплексного подхода в обнаружении и предотвращении компьютерных атак на информационные ресурсы региона

Кислов Роман Сергеевич

Первый заместитель директора

ГБУ СО «Оператор электронного правительства».

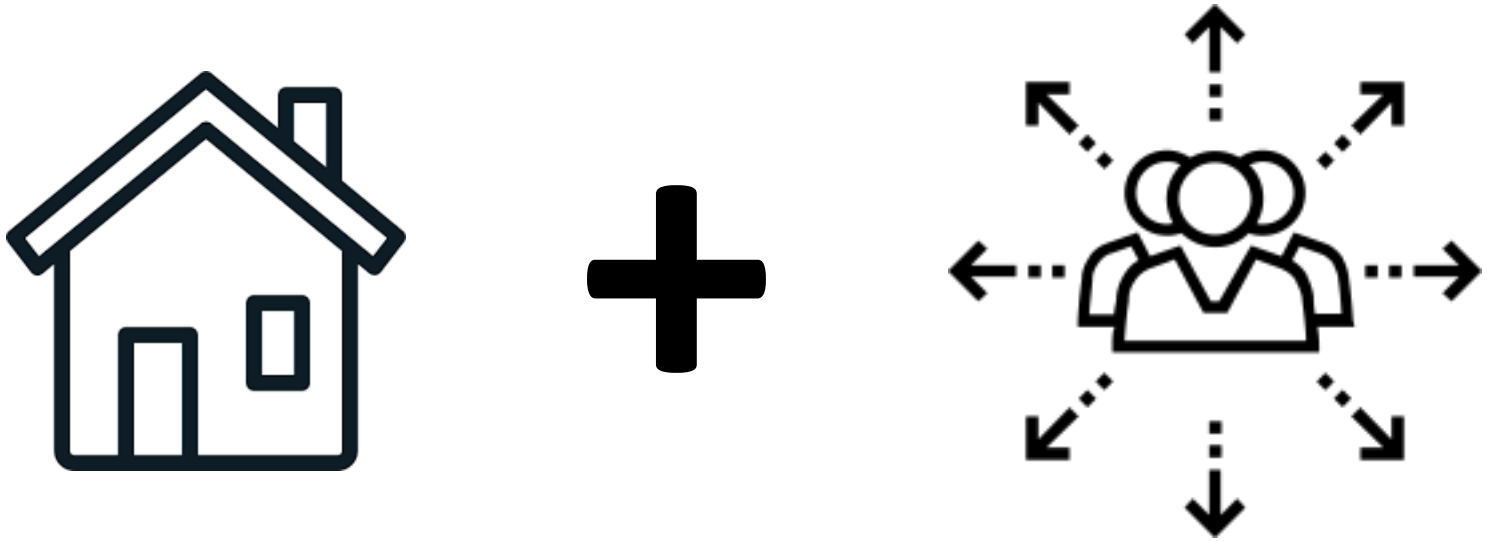
Цели

- Обеспечение защиты информации.
- Обнаружение, предупреждение, реагирование и ликвидация последствий компьютерных атак и инцидентов.
- Установление причин компьютерных инцидентов.
- Сбор и анализ данных о текущем состоянии информационной безопасности и его изменениях.
- Выполнение требований законодательства в области КИИ.

Проблемы, с которыми столкнулись:

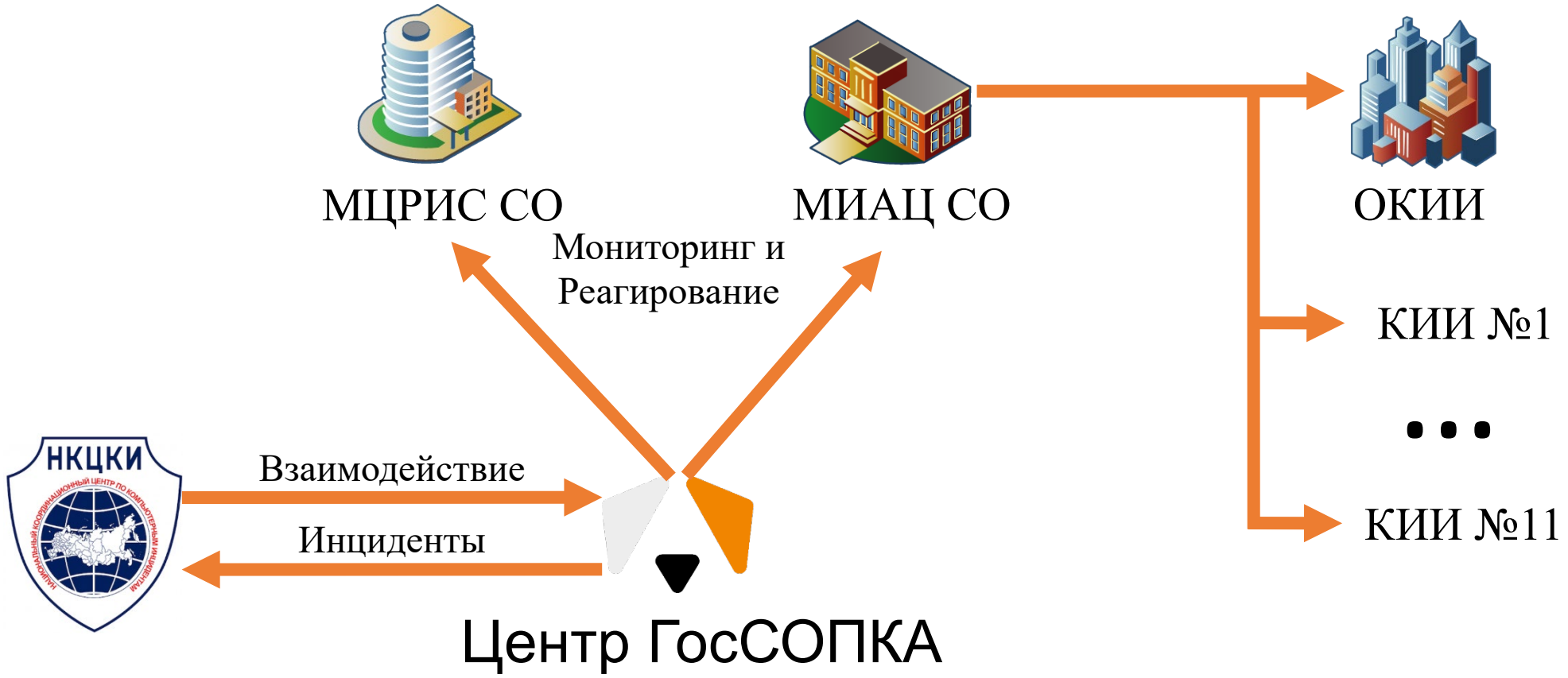
- Нехватка квалифицированного персонала.
- Сложность в управлении безопасностью распределенной информационной инфраструктуры.
- Необходимость синхронизации пересекающихся требований регуляторов.
- «Сырость» отечественных программно-аппаратных средств обеспечения информационной безопасности.

Выбранный путь решения



Строительство собственного SOC и поддержка внешним коммерческим центром ГосСОПКА

Решение


МЦРИС СО
МИАЦ СО
ОКИИ
Мониторинг и
Реагирование
КИИ №1
• • •
КИИ №11
НКЦКИ
Взаимодействие
Инциденты
Центр ГосСОПКА

Преимущества собственного SOC

- Автономность.
- Полный контроль.
- Мультивендорность решения:

infotecs

kaspersky

positive technologies

Преимущества аутсорсинговых решений

- Мониторинг 24/7.
- Возможность привлечения высококвалифицированных специалистов.
- Экономия на штате.

Проделанная работа

- Подключение к Интернет централизовано на 95% и контролируется при помощи шлюза UserGate
- Проводится тестирование аутентификации на базе стандарта IEEE 802.1X
- Создана многоуровневая система защиты информации, которая обеспечивает мониторинг масштабной
- IT-инфраструктуры 24/7
- Организовано взаимодействие с НКЦКИ
- Специалисты информационной безопасности имеют возможность проводить анализ подозрительных событий, расследование инцидентов информационной безопасности

Планы дальнейшего развития - централизация

Благодарю за внимание!