Опыт создания корпоративного центра ГосСОПКА для Госкорпорации «Роскосмос»

Графеев Олег Евгеньевич

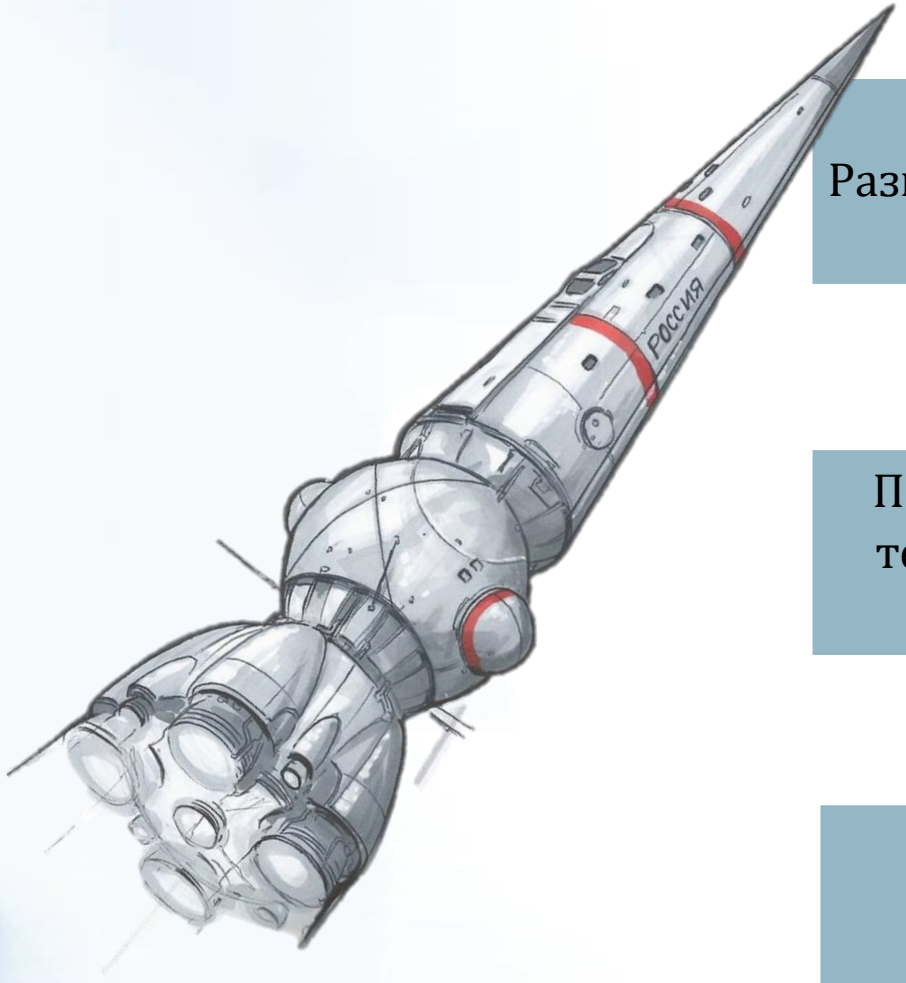
Заместитель начальника Управления –
начальник Центра мониторинга информационной безопасности
ФГУП «НТЦ «Заря»

2022 г.

ОБОМНЕ

- Графеев Олег Евгеньевич
- ФГУП «НТЦ «Заря» (г. Москва), заместитель начальника Управления безопасности информации – начальник центра мониторинга информационной безопасности

Угрозы информационной безопасности

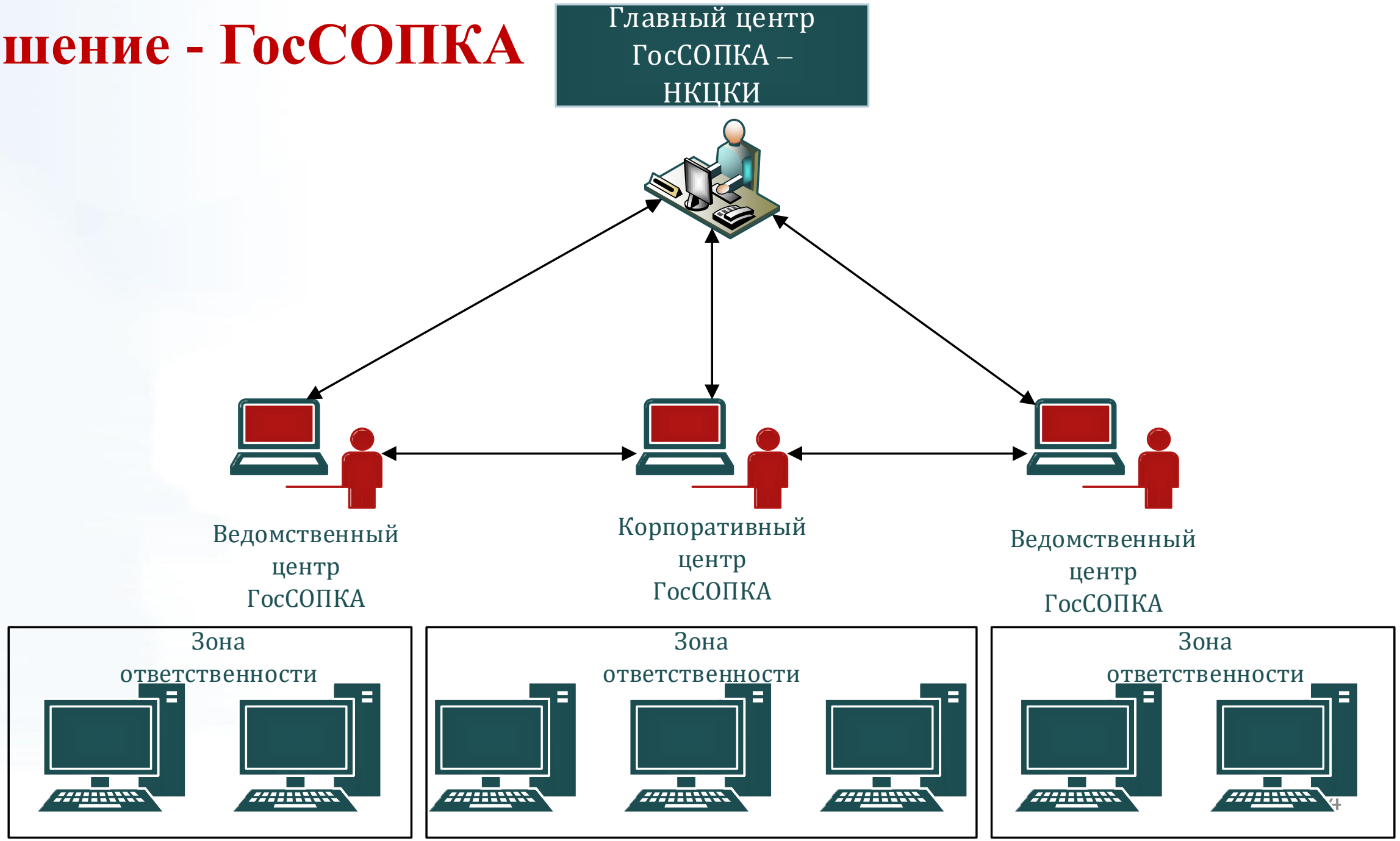


Развитие информационных технологий

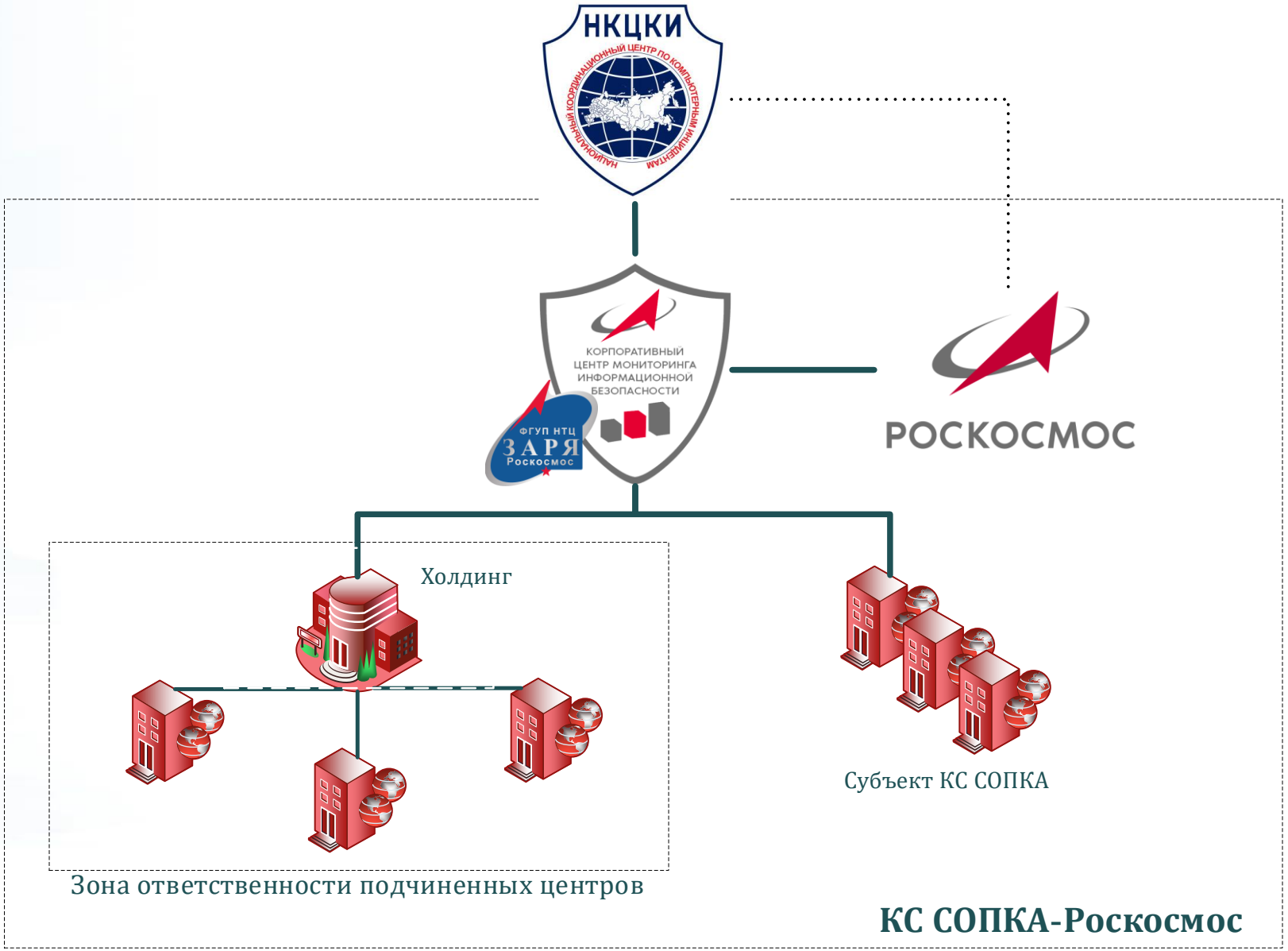
Повышение роли информационных технологий в ракетно-космической промышленности

Компьютерные атаки

Решение - ГосСОПКА



Отраслевое решение – КС СОПКА-Роскосмос



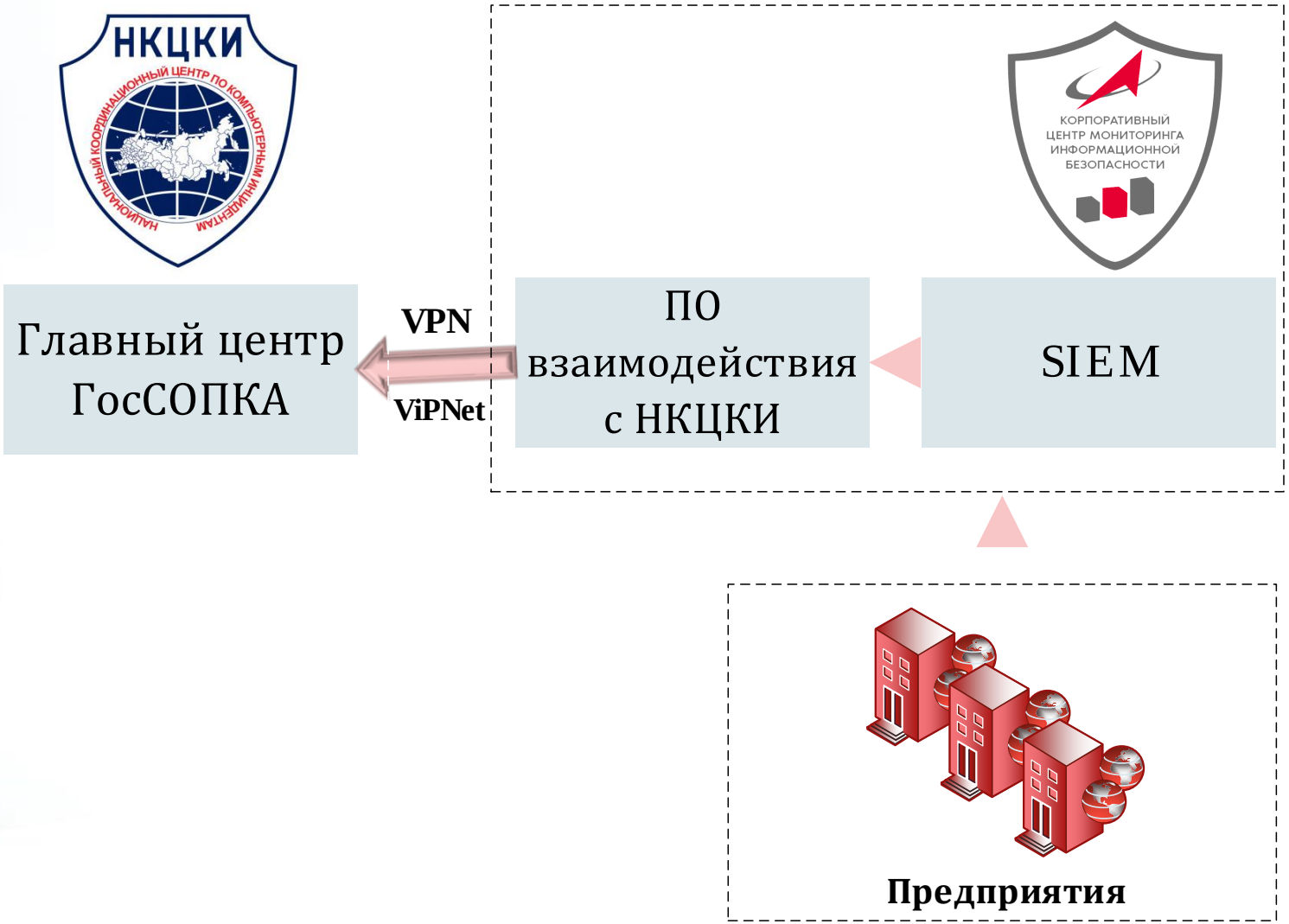
Корпоративный центр мониторинга

Анализ защищенности информационных систем

Мониторинг информационной безопасности информационных систем

Реагирование на компьютерные инциденты

Взаимодействие НКЦКИ и КЦМ



Отраслевой форум информационной безопасности

Актуальные угрозы и уязвимости

Взаимодействие
с КС СОПКА-Роскосмос

Бюллетени НКЦКИ

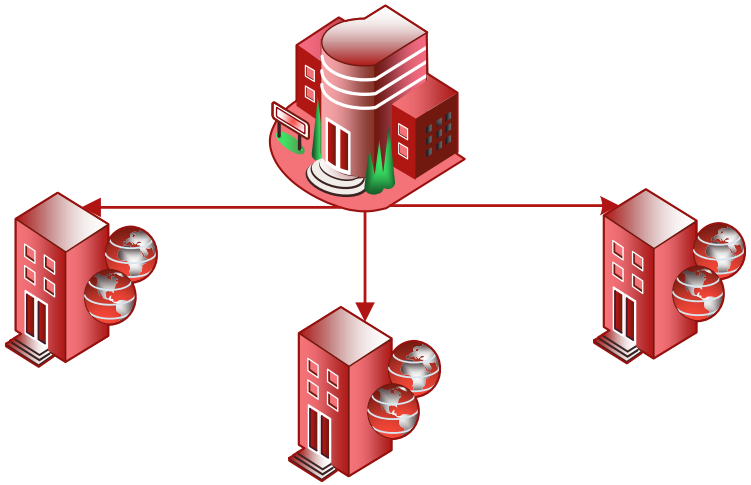
Информационные письма
Госкорпорации «Роскосмос»
по информационной безопасности

Документы по информационной безопасности, обнаружению и противодействию компьютерным атакам

Кадровые вопросы

Создание подчиненных центров

Получение актуальной и полной информации о состоянии информационной безопасности на дочерних предприятиях



Диверсификация своей деятельности за счет оказания услуг по мониторингу информационной безопасности

Координация действий при реагировании на компьютерные инциденты на дочерних предприятиях

Лицензия ФСТЭК России на деятельность по ТЗКИ в части мониторинга информационной безопасности

Самостоятельное получение лицензии

Подготовка к лицензированию при содействии ФГУП «НТЦ «Заря»

Функции подчиненного центра КС СОПКА-Роскосмос реализуются ФГУП «НТЦ «Заря»

Иные субъекты КС СОПКА-Роскосмос

Предприятие входит в состав холдинга, создающей подчиненный центр КС СОПКА-Роскосмос

Подключение к подчиненному центру

Предприятие входит в состав холдинга, не создающей подчиненный центр КС СОПКА-Роскосмос

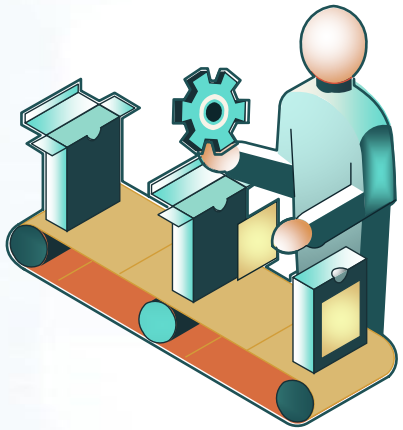
Предприятие не входит в состав холдинга

Подключение к корпоративному центру мониторинга КС СОПКА-Роскосмос

Способы подключения

- Использование SIEM-системы
- Использование агента SIEM-системы корпоративного центра мониторинга

Варианты построения АСУ ТП



Система, имеющая онлайн-соединение с глобальной сетью

Система, имеющая оффлайн-соединение с глобальной сетью

Система, не имеющая соединения с глобальной сетью

Система, имеющая онлайн-соединение с глобальной сетью

Получение информации о событиях безопасности с элементов существующей системы защиты информации системой	Потребует интеграции системы защиты информации с используемой SIEM-системой
Внедрение системы защиты информации АСУ ТП на основе типовых решений	Позволит использовать программные и программно-аппаратные средства, способные передавать информацию о событиях безопасности в SIEM-систему
Внедрение комплексных средств защиты АСУ ТП, предлагаемых коммерческими разработчиками	SIEM-система корпоративного центра мониторинга может быть доработана для сбора информации, передаваемой данными системами

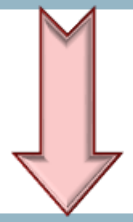
Система, имеющая оффлайн-соединение с глобальной сетью

Построение канала однонаправленной передачи информации на основе диодов и последующая передача по защищенному каналу

Перенос журналов с элементов существующей системы защиты информации с использованием съемных носителей информации и последующая передача информации по защищенному каналу

Система, не имеющая соединения с глобальной сетью

АСУ ТП, изолированные от компьютерных сетей и защищенные от использования съемных носителей информации



Мониторинг информационной безопасности не требуется

Графеев Олег Евгеньевич

Заместитель начальника Управления –
начальник Центра мониторинга информационной безопасности
ФГУП «НТЦ «Заря»

2022 г.