



ОТРАСЛЕВОЙ ЦЕНТР КОМПЕТЕНЦИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТРАНСПОРТНОЙ ОТРАСЛИ

Отраслевой центр компетенций по ИБ

Совокупность ресурсов (организационных, технических, технологических, кадровых), механизмов, методов, направленных на координацию и обеспечение информационной безопасности с учетом отраслевой специфики путем создания соответствующей организационной структуры



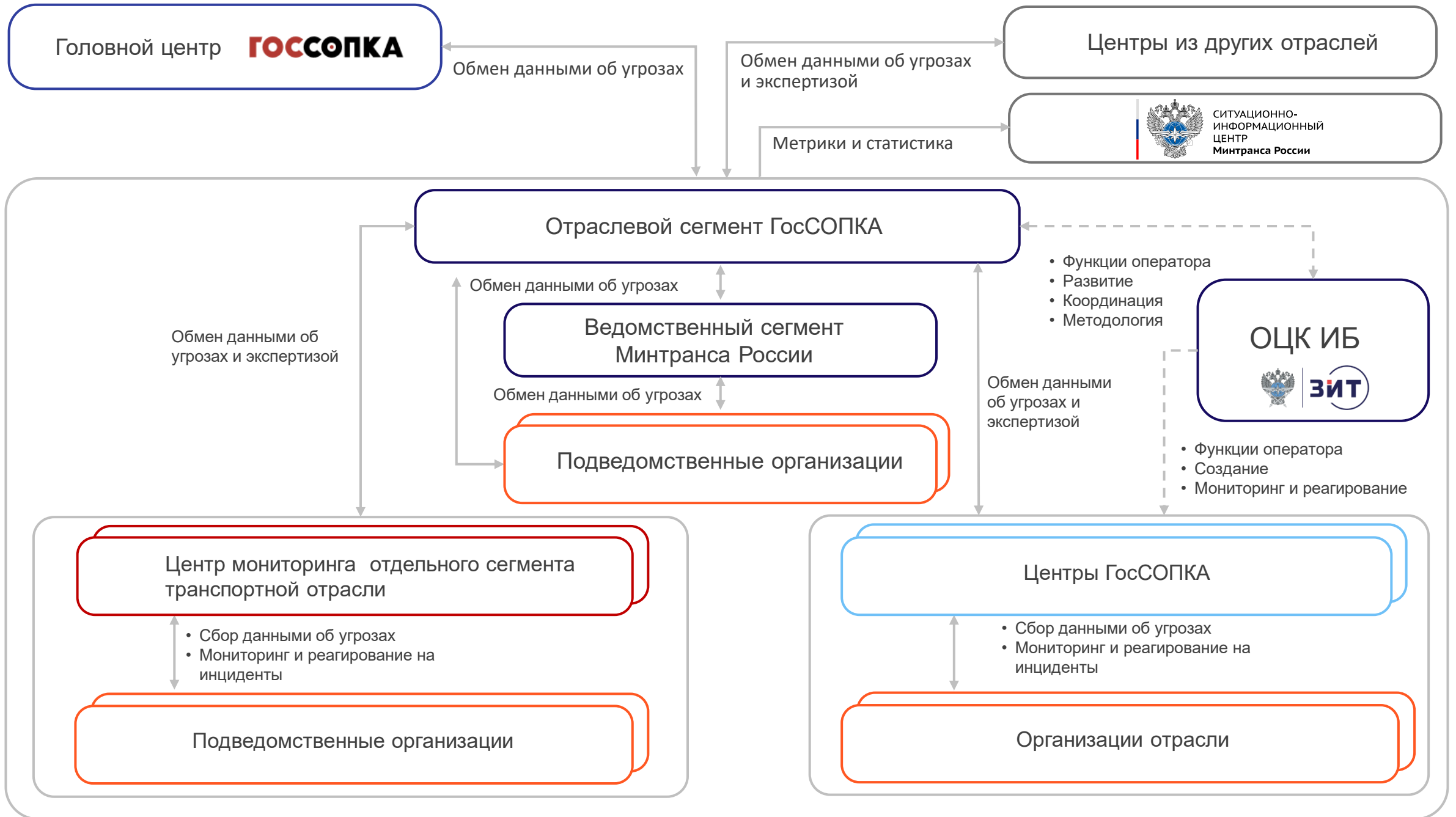
ФУНКЦИОНАЛ

- Взаимодействие (межотраслевое) с другими ОЦКИБ в целях обмена опытом, лучшими практиками, методиками, особенностями межотраслевой специфики
- Организация процесса реализации организациями транспортной отрасли мероприятий по защите информации (методики, стандарты, обучение, недопустимые события, импортозамещение, правовое регулирование)
- Предоставление механизмов обмена информацией об актуальных угрозах и индикаторах компрометации, лучших практиках
- Киберполигоны и повышение осведомленности работников организаций
- Осуществления мониторинга - выявления (потенциальных) компьютерных атак (инцидентов), угроз, уязвимостей



ПРЕИМУЩЕСТВА

- Понимание особенностей информационной инфраструктуры отрасли и как следствие повышение эффективности при оказании помощи при обнаружении, реагировании и ликвидации компьютерных атак и взаимодействии с НКЦКИ
- Учитываются индивидуальные особенности отрасли при формировании нормативных актов, рекомендаций и методических материалов
- Доверенная площадка для обмена компетенциями, экспертизой в рамках отрасли



Создание ВС
ГосСОПКА МТ

2022

2023-2024

Развитие

- ✓ Подключение значимых систем Минтранса России
- ✓ Эксплуатация ВС ГосСОПКА
- ✓ Отраслевой перечень типовых ПАК
- ✓ Отраслевые методические рекомендации по категорированию
- ✓ Решение о создании ОЦКИБ

2024

Планы

- ✓ Соглашение с Минтранс России и Положение ОЦКИБ
- ✓ Запуск эксперимента по взаимодействию на базе ОЦКИБ (киберучения)
- ✓ Типовые ПАК для тиражирования технических решений ВС ГосСОПКА

2025-2030

Масштабирование

- ✓ Подключение организаций (ЗОКИИ)
- ✓ Развитие сервисов (киберучения, обмен IoC, отраслевой центр мониторинга)



TransportCERT ценность для вовлеченных сторон

Участников

- **Снижение стоимости** киберзащиты
- **Снижение нагрузки** на подразделения ИБ
- Снижение возможности наступления **цепочек недопустимых событий** на кросс-субъектовом уровне
- Применение **стандартов и лучших практик** противодействия киберугрозам в рамках отрасли
- Площадка **экспертного сообщества** транспортной отрасли для обмена IoC и координации процессов реагирования

Минтранса России, Центров ГосСОПКА в рамках общей структуры

- Снижение риска **простоев и аварий** на ЗОКИИ
- Организация и контроль в части выполнения требований нормативно-правовых актов
- Наличие **актуальной статистики** по угрозам и атакам, а также их влиянию на **комплексные процессы**

Регуляторы

- Повышение киберустойчивости отрасли
- Наличие актуальной статистики по угрозам и атакам
- Снижение нагрузки
- Методологическое сопровождение субъектов отрасли



СПАСИБО ЗА ВНИМАНИЕ!

