



XXI МЕЖДУНАРОДНАЯ ВЫСТАВКА

**INTERPOLITEX**

СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ГОСУДАРСТВА



## Современные средства ИТ-мониторинга для нужд силовых структур

**Докладчик:**

Директор по информационным технологиям и  
инновациям ЗАО «ГЛОБУС-ТЕЛЕКОМ»

Рыбаков Сергей



# Критическая информационная инфраструктура



«Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы.» Указ Президента РФ N 203 от 09.05.2017.

## Критическая информационная инфраструктура Российской Федерации (КИИ)

совокупность объектов критической информационной инфраструктуры, а также сетей электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры между собой.



**Органы государственной власти**



**Силовые структуры**



**Предприятия оборонно-промышленного комплекса**



**Промышленность; народное хозяйство**

# Объекты критической информационной инфраструктуры Российской Федерации"

## Объекты КИИ:

- Информационные системы.
- Информационно-телекоммуникационные сети.
- Автоматизированные системы управления технологическими процессами.

*Федеральный закон от 26.07.2017 N 187-ФЗ О безопасности критической информационной инфраструктуры РФ"*

- Объекты, осуществляющие управление, контроль и мониторинг критических процессов КИИ.

*Проект постановления Правительства РФ от 25.09.2017 «Об утверждении показателей критериев значимости объектов критической информационной инфраструктуры...»*



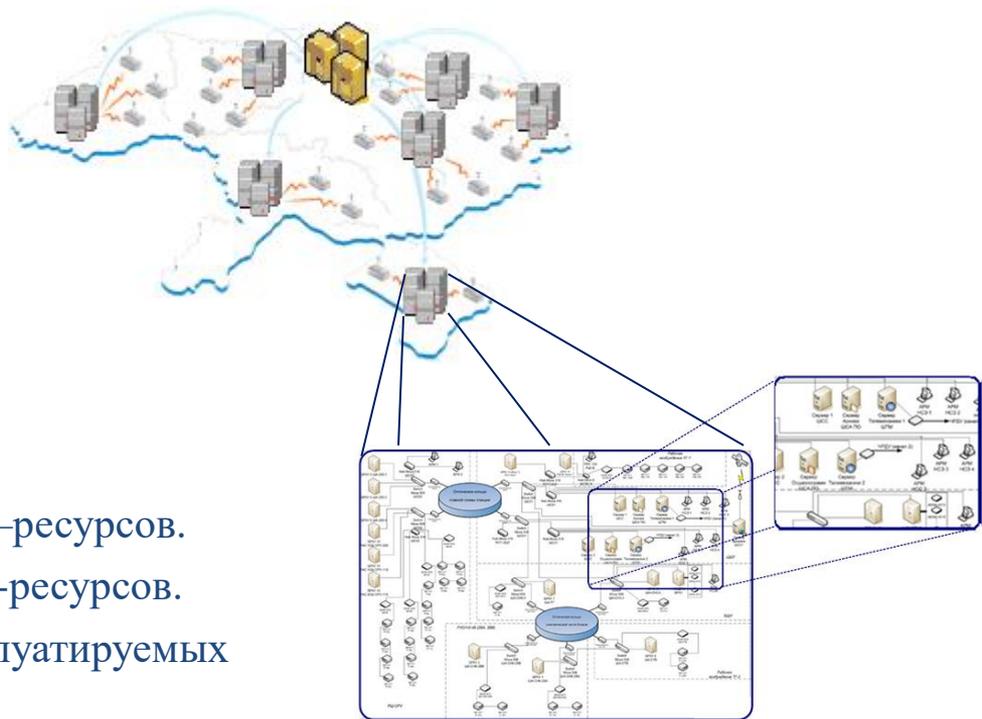
# Мониторинг и управление критической информационной инфраструктурой

## Цели:

- Обеспечение непрерывности, отказоустойчивости и катастрофоустойчивости ИТ-инфраструктуры.
- Постоянное и планомерное развитие ИТ-инфраструктуры в соответствии с задачами.
- Снижение эксплуатационных затрат.

## Задачи:

- Учет и постоянный мониторинг состояния ИТ –ресурсов.
- Недопущение / снижение времени простоя ИТ-ресурсов.
- Планирование и согласование изменений эксплуатируемых ИТ- комплексов.





# «СКИТ» – постоянное развитие



## ПАК «СКИТ» в защищенном исполнении

### Тест пройден.

- программное обеспечение «СКИТ»;
- операционная система АстраЛинукс (ОАО «РусБИТех»);
- СУБД ЛИНТЕР БАСТИОН (ЗАО «Релэкс»);
- Серверное оборудование Etegro, ЭВМ СH Арбор.



## Тестирование совместной работы ПАК «СКИТ» с производителями

### Тест пройден.

Проведено несколько десятков тестов совместимости СКИТ с аппаратными и программными телекоммуникационными решениями; в том числе передовыми российскими криптошлюзами:

- Континент;
- VipNet;
- С-Терра.



## Тестирование ПАК «СКИТ» как системы мониторинга СЭД

### Тест пройден.

- мониторинг качества и скорости распознавания документов при потоковом сканировании;
- мониторинг механизмов интеграции СЭД с другими системами (1С, корпоративный портал);
- мониторинг доступности пользовательских лицензий и т.д.

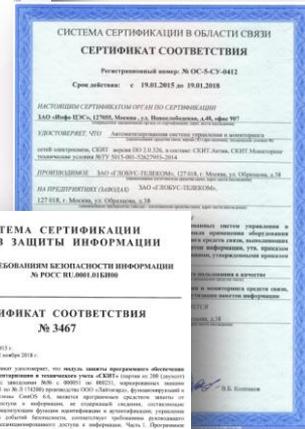


# «СКИТ» – система управления и мониторинга критической информационной инфраструктурой



## Документальная основа ПАК «СКИТ»:

- **Роспатент.** Свидетельство о государственной регистрации программ для ЭВМ.
- **Минкомсвязь.** Сертификат соответствия требованиям к автоматизированным системам управления и мониторинга сетей электросвязи.
- **ФСТЭК.** Сертификат соответствия требованиям руководящего документа «Защита от НСД к информации ... классификация по 4 уровню контроля отсутствия НДС».
- **Реестр российского ПО.** Приказ Минкомсвязи №426 от 06.09.2016. Регистрационный номер 64388.
- **Национальный фонд алгоритмов и программ** (опосредовано, через ГИС).





**Спасибо за внимание!**