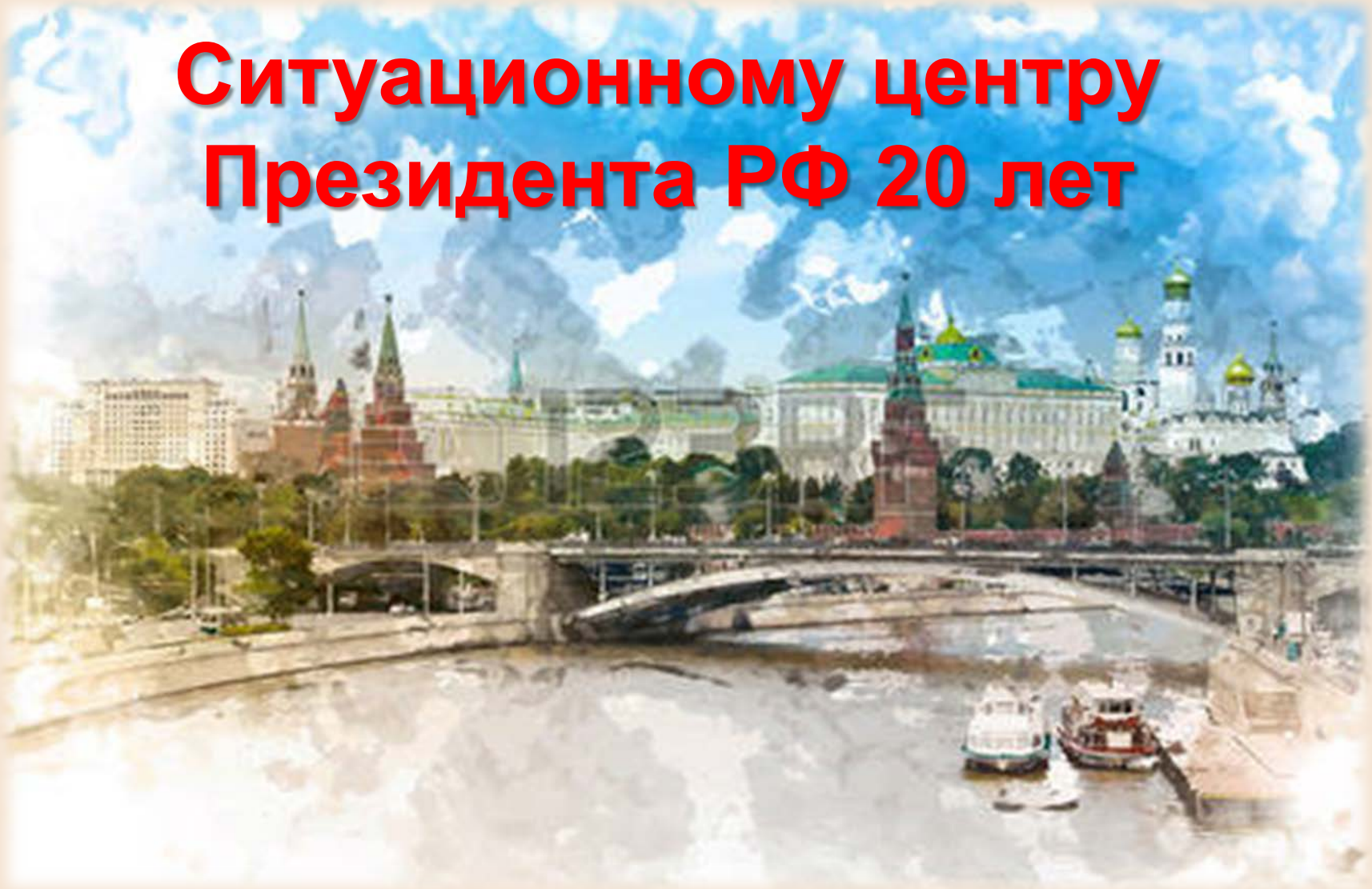
SOC-Forum v 2.0,
Практика противодействия кибератакам
и построения центров мониторинга ИБ

# Аспекты защиты информации при информационном взаимодействии центров мониторинга информационной безопасности

**В.Е. Гаврилов**
**Советник директора ФИЦ ИУ РАН**
**по информационной безопасности**

# Ситуационному центру Президента РФ 20 лет



**Указ Президента РФ**
от 25 июля 2013 г. №648
«О формировании системы распределенных ситуационных центров, работающих по единому регламенту взаимодействия»

- Межведомственная комиссия
- Совет конструкторов СР СЦ
- Концепция создания системы распределенных ситуационных центров, работающих по единому регламенту взаимодействия, утвержденная Президентом РФ (№ Пр-2308 от 3 октября 2013 г.)
- Концепция информационной безопасности системы распределенных ситуационных центров, работающих по единому регламенту взаимодействия (утв. решением МВК от 5.12.13г.)

# Концепция информационной безопасности СР СЦ

- **Общая характеристика СР СЦ**
- **Основные объекты защиты СР СЦ**
- **Основные угрозы информационной безопасности СР СЦ**
- **Модель нарушителя СР СЦ**
- **Основные требования по противодействию угрозам ИБ**

**Меры и средства обеспечения информационной безопасности СР СЦ**

- законодательные;
- организационные;
- технические (программно-технические);
- управление системой обеспечения безопасности информации;
- технология организации работ и контроль эффективности системы защиты информации.

**Указ Президента РФ**
от 15.01.2013 N 31с
«О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

# Проблемы защиты информации

## при организации информационного взаимодействия центров мониторинга информационной безопасности

### Правовые

*Стимулирование участников*

### Организационные

*Нечеткие критерии КА*

*Сложность администрирования*

*Многообразие форм собственности участников*

### Технические

*Разнообразие платформ и технологий*

# Безопасность информации

**Формальная**
***(по бумагам)***

**Реальная**
***(функциональная)***

# Повышение эффективности защиты информации за счет использования технологий искусственного интеллекта

- Антивирусная защита
- Система предупреждения и обнаружения компьютерных атак
- Мониторинг действий пользователей
- Контентный анализ информационных потоков
- Выявление скрытых логических каналов утечки защищаемой информации
- Инструментарий администрирования системы

# «Экспоненциальное проклятье» и спецвычислители

- Ассоциативные вычислители
- Квантовые вычислители
- Универсальные  мем-машины

# Актуальные научные проблемы

- Разработка математических моделей компьютерных атак
- Разработка спецвычислителей, ориентированных на работу с большими объемами данных (ассоциативные, квантовые)
- Разработка алгоритмов шифрования, позволяющих обрабатывать хранимые данные без расшифрования

# Спасибо за внимание !

*В. Е. Гаврилов*
*Советник директора ФИЦ ИУ РАН*
*по информационной безопасности*
*119333 Москва, ул. Вавилова, д.44 кор.2*
*Тел. (495)135-53-23*
*e-mail: vgavrilov@ipiran.ru*