О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

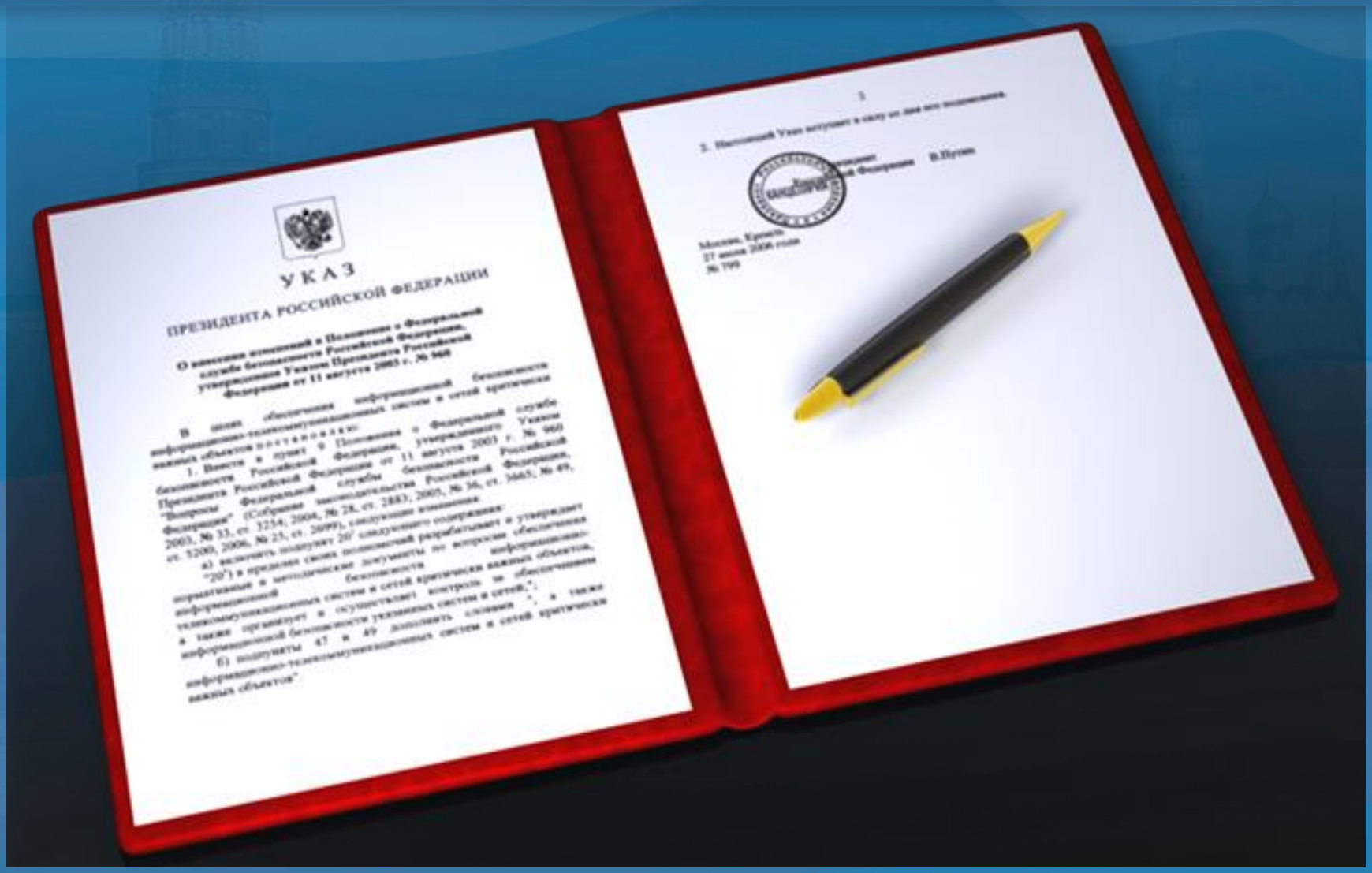
Юдин Сергей Николаевич
ФСБ России

2015 г.

Основные виды угроз информационной безопасности

- нарушение доступности информационных ресурсов (блокирования доступа к информации);
- нарушение конфиденциальности (несанкционированный доступ к информации);
- нарушение целостности (искажение информации).

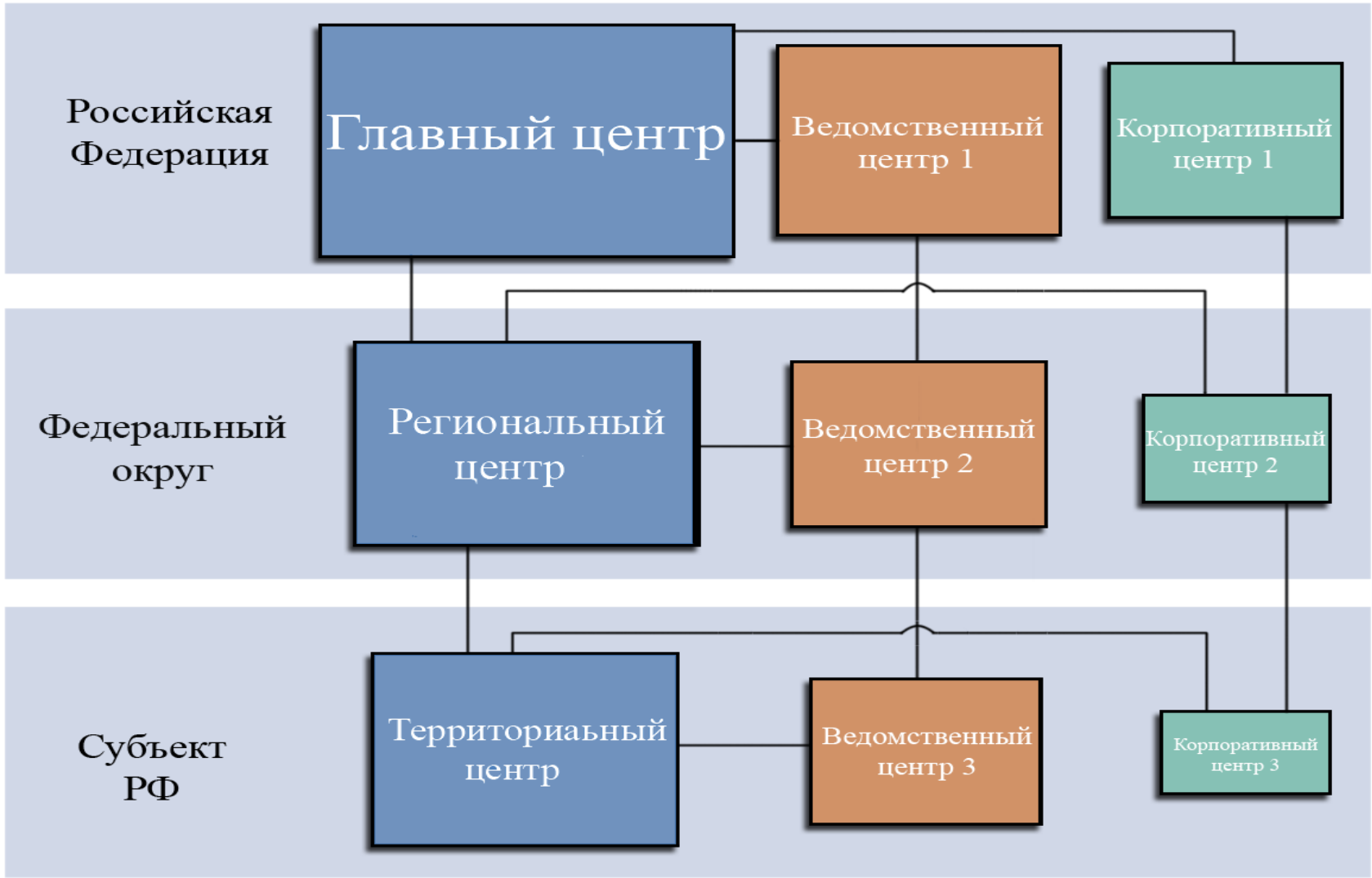
Указ от 15 января 2013 года № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»



Основные задачи ГосСОПКА

- прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации;
- обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий КА;
- осуществление контроля степени защищенности критической информационной инфраструктуры Российской Федерации от КА;
- установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации.

Структура центров ГосСОПКА



Задачи сегментов ГосСОПКА

- обнаружение КА;
- проведение мероприятий по оценке защищенности от КА и вирусных заражений информационных ресурсов ведомства;
- ликвидация последствий КА и вызванных ими компьютерных инцидентов;
- обработка информации о выявленных КА, зафиксированных компьютерных инцидентах и обнаруженных уязвимостях;
- принятие управляющих решений по обеспечению информационной безопасности информационных ресурсов, находящихся в зоне ответственности ведомственного сегмента;
- информационный обмен с Главным центром ГосСОПКА сообщениями о зафиксированных инцидентах.

Проект ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Подходы к обеспечению безопасности объектов критической информационной инфраструктуры:

- разработка критериев отнесения объектов к различным категориям опасности;
- категорирование объектов в соответствии с указанными критериями;
- ведение реестра объектов с учетом категории их опасности;
- установление требований по обеспечению безопасности объектов с учетом категории их опасности;
- обеспечение взаимодействия с ГосСОПКА;
- осуществление оценки степени защищенности объектов;
- осуществление государственного контроля в области безопасности критической информационной инфраструктуры Российской Федерации.

Спасибо за внимание!