

# Об организации взаимодействия при создании и функционировании ГосСОПКА

Гончаренко В.Е.

# Основнополагающие документы ГосСОПКА

1. «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» от 03.02.2012 г. № 803.
2. «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» от 15.01.2013 г. № 31с.
3. Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации от 12.12.2014 г. № К 1274.

# Минкомсвязь России в ГосСОПКА

1. «О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов» от 24.05.2010 г. № 365.
2. «Концепция перевода обработки и хранения государственных информационных ресурсов, не содержащих сведения, составляющие государственную тайну, в систему федеральных и региональных центров обработки данных» от 07.10.2015 г. № 1995-Р.

# ФСТЭК России в ГосСОПКА

1. «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» от 11.02.2013 г. № 17.
2. «Меры защиты информации в государственных информационных системах» от 11.02.2014 г.
3. «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей среды» от 14.03.2014 г. № 31.

## Соглашение. Термины и определения

- «Ведомственный центр обнаружения, предупреждения и ликвидации последствий компьютерных атак»;
- «зона ответственности»
- «информационные ресурсы»
- «критическая информационная инфраструктура Российской Федерации»
- «объекты критической информационной инфраструктуры»

# Соглашение. Предмет соглашения

Организация взаимодействия при решении задач ГосСОПКА

Задачи ГосСОПКА:

- прогнозирование ситуации в области обеспечения информационной безопасности
- обеспечение взаимодействия владельцев информационных ресурсов, операторов связи, иных субъектов
- осуществление контроля степени защищенности
- установление причин компьютерных инцидентов

## **Соглашение. Направления взаимодействия**

- проведение мероприятий по обнаружению КА
- проведение мероприятий по реагированию на КА
- совершенствование методической базы
- обмен сведениями о КА
- отработка механизмов и процедур взаимодействия
- проведение совместных тренировок и учений
- взаимодействие в вопросах повышения уровня осведомленности и квалификации
- проведение совместных семинаров

## **Соглашение. Требования к организации**

- согласование с ФСБ России документации и методических документов;
- выявление, сбор и анализ сведений об уязвимостях;
- сбор и анализ сведений о компьютерных инцидентах;
- проведение мероприятий по оценке степени защищенности, оперативному реагированию и ликвидации последствий компьютерных атак и компьютерных инцидентов;
- предоставление сведений о технологиях, инфраструктуре, состоянии защищенности, компьютерных атаках и компьютерных инцидентах.



# Соглашение. Требования к ФСБ России

- разработка перечня сведений, передаваемых в ходе взаимодействия;
- разработка и предоставление методических рекомендаций;
- участие в совместных мероприятиях;
- предоставление сведений об угрозах информационной безопасности;
- взаимодействие с уполномоченными органами иностранных государств.

# Соглашение. Дополнительно

- безвозмездно
- ограничения на передаваемую информацию
- совместные консультации

**Спасибо за внимание!**