# О методических рекомендациях по созданию ведомственных центров ГосСОПКА

Представитель 8 Центра ФСБ России

Новиков А.О.

# Коротко о нашем подразделении

Национальный координационный центр
по компьютерным инцидентам

GOV-CERT.RU

CERT.GOV.RU

# Вопросы о системе ГосСОПКА

Вопросов много:

- Что это?
- Для кого?
- Каков Use Case?
- В чем Profit?
- Сколько это будет «стоить»?
- и т.п.

Ну и традиционный вопрос:

- А оно того стоит?

# Субъекты ГосСОПКА


Владельцы объектов критической информационной инфраструктуры и информационных ресурсов

Операторы связи

Организации-лицензиаты в области защиты информации

# Сбор, анализ и обмен информацией об угрозах

- Источники угроз
- Атакованные системы
- Агрегация по инцидентам
- Состояние защищенности
- Уязвимости ПО
- Признаки компрометации
- Другие оперативные и значимые сведения

Обработка таких сведений позволяет нам сформировать адресный сигнал субъектам ГосСОПКА

# Задачи ведомственных (корпоративных) центров ГосСОПКА


Обнаружение атак

Предупреждение угроз

Ликвидация последствий

# Методические рекомендации

1. Общие положения
2. Функции ведомственного сегмента ГосСОПКА и способы их реализации
3. Рекомендации к средствам автоматизации
4. Обеспечение безопасности информации ведомственного сегмента
5. Варианты архитектуры ведомственного сегмента
6. Организационно-штатная структура ведомственного сегмента ГосСОПКА
7. Порядок создания ведомственного сегмента
8. Взаимодействие с главным центром ГосСОПКА

# Контактная информация

Национальный координационный центр
по компьютерным инцидентам

GOV-CERT.RU (CERT.GOV.RU)

gov-cert@gov-cert.ru

Новиков Алексей Олегович

nao@gov-cert.ru