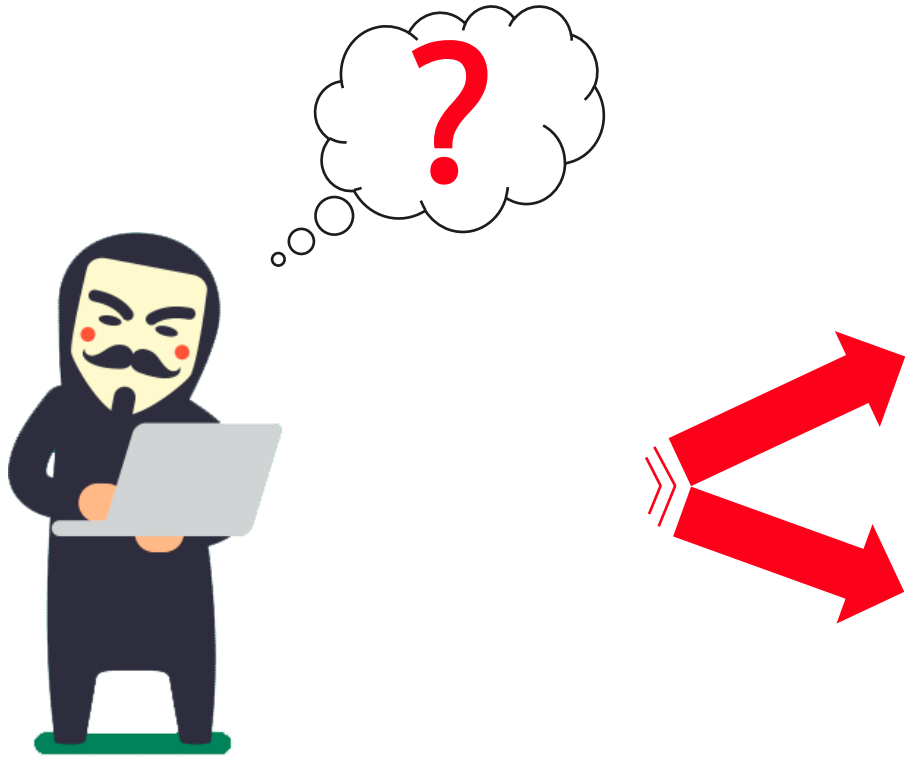
ГОССОПКА

ГосСОПКА:
основные задачи, функции
и реализуемые мероприятия

Докладчик:
Фатеев Егор Вадимович
УФСБ России по Смоленской области

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРОЦЕСС ДИНАМИЧЕСКИЙ

ГОССОПКА



Компьютерные атаки становятся сложнее,
могут провоцировать техногенные аварии,
экологические катастрофы, социальные потрясения
и наносить серьезный ущерб государству

НОРМАТИВНО-ПРАВОВАЯ БАЗА

ГОССОПКА

- Указ Президента РФ от 15 января 2013 г. N 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»
- «Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», утвержденная Президентом РФ 12.12.2014 №1274К
- Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
- Указ Президента РФ от 22 декабря 2017 г. N 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

ЗАДАЧИ ГОССОПКА

ГОССОПКА

- Прогнозирование ситуации в области обеспечения информационной безопасности РФ
- Обеспечение взаимодействия владельцев информационных ресурсов РФ, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак
- Осуществление контроля степени защищенности информационных ресурсов РФ
- Установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов РФ

СУБЪЕКТЫ ГОССОПКА

ГОССОПКА

В настоящее время создаются сегменты более чем в 20 министерствах и организациях

подписаны соглашения

в стадии рассмотрения/подписания

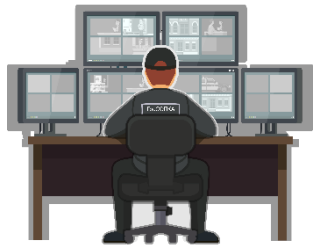
- ФСБ России
- Минэнерго России
- СВР России
- Минпромторг России
- МИД России
- Следственный комитет РФ
- ПАО «Россети»
- ГК «Роскосмос»
- Минобороны России
- Генеральная прокуратура РФ
- Минэкономразвития России
- Следственный комитет
- ФНС России
- ПАО «Сбербанк»
- ГК «Росатом»
- ГК «Ростех»
- АО «СО-ЕЭС»
- ООО «Р-Альфа Лаб»
- ООО «ЦБИ»
- Минтранс России
- МВД России
- ФСО России
- Центральный банк РФ
- АО «Лаборатория Касперского»
- ПАО «МТС»
- ООО «Позитивные технологии»
- Правительство Самарской области

СТРУКТУРА ГОССОПКА

ОСНОВНЫЕ ЗАДАЧИ СУБЪЕКТА (ЦЕНТРА) ГОССОПКА

ГОССОПКА

ОБЩИЕ ФУНКЦИИ ЦЕНТРА ГОССОПКА



Эксплуатация средств ГосСОПКА

Центр ГосСОПКА

НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Взаимодействие с НКЦКИ

Направление производителю информации об ошибках

Разработка документов

ЗАДАЧИ ГОССОПКА

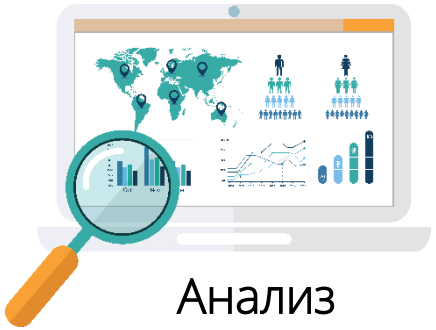
ГОССОПКА

- **Компьютерная атака** – попытка целенаправленного нарушения штатного режима функционирования объекта КИИ
- **Компьютерный инцидент** – состоявшийся факт нарушения штатного режима функционирования объекта КИИ
- Компьютерный инцидент не всегда является следствием компьютерной атаки

ФУНКЦИИ ЦЕНТРА ГОССОПКА ПО ОБНАРУЖЕНИЮ

ГОССОПКА

Центр ГосСОПКА



Анализ событий ИБ

Прием сообщений об инцидентах

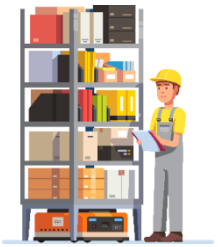
Регистрация событий

ФУНКЦИИ ЦЕНТРА ГОССОПКА ПО ПРЕДУПРЕЖДЕНИЮ

ГОССОПКА

Выдача рекомендаций по повышению защищенности

Центр ГосСОПКА



Инвентаризация информационных ресурсов

Составление перечня угроз

Выявление уязвимостей

Анализ угроз ИБ

ФУНКЦИИ ЦЕНТРА ГОССОПКА ПО РЕАГИРОВАНИЮ

ГОССОПКА

Выдача рекомендаций по повышению защищенности

Анализ результатов ликвидации последствий инцидентов

Установление причин возникновения инцидента

Центр ГосСОПКА

Ликвидация последствий инцидентов

Регистрация инцидентов

Сбор сведений об инцидентах

ФУНКЦИИ НКЦКИ

ГОССОПКА

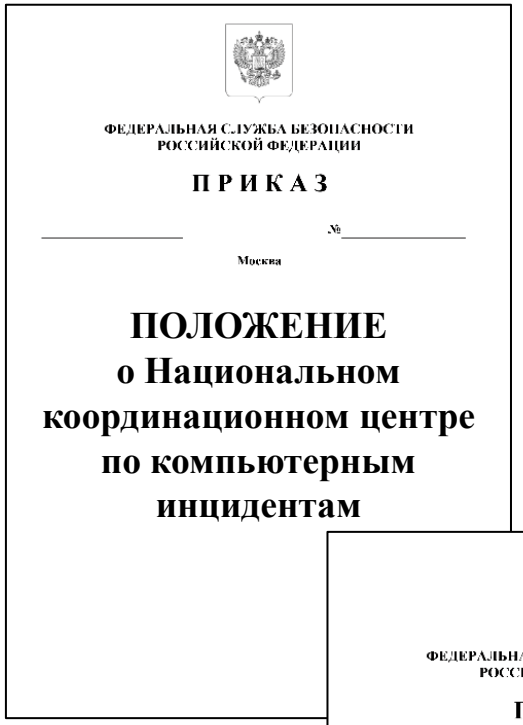
НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

- координация деятельности субъектов ГосСОПКА
- анализ информации, получаемой от субъектов ГосСОПКА
- взаимодействие с субъектами КИИ
- обмен информацией о компьютерных инцидентах с уполномоченными органами иностранных государств
- рассылку подготовленных НКЦКИ уведомлений об угрозах и способах противодействия

НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ ФСБ РОССИИ

ГОССОПКА



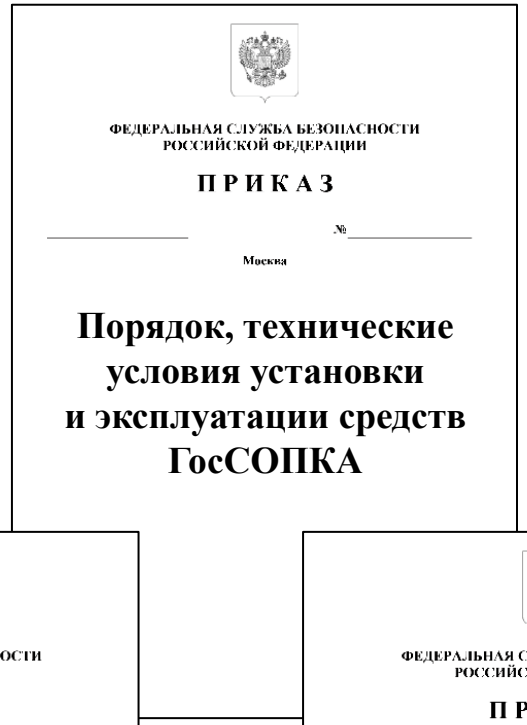
ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

П Р И К А З

_____ №_____

Москва

ПОЛОЖЕНИЕ
о Национальном координационном центре по компьютерным инцидентам



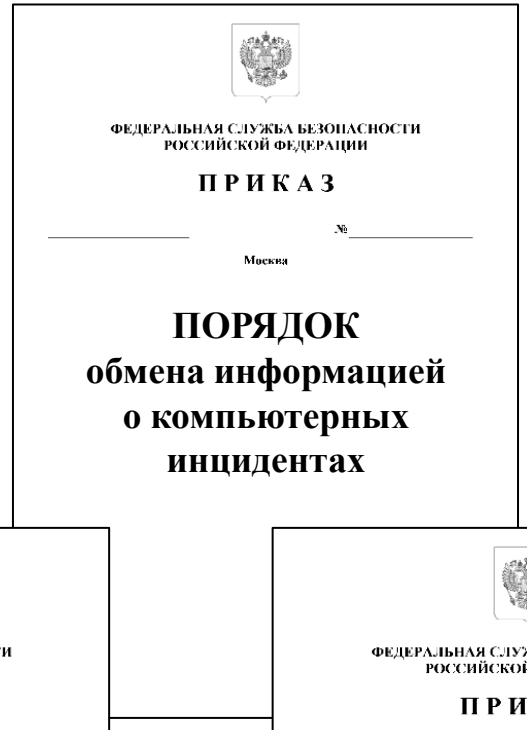
ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

П Р И К А З

_____ №_____

Москва

Порядок, технические условия установки и эксплуатации средств ГосСОПКА



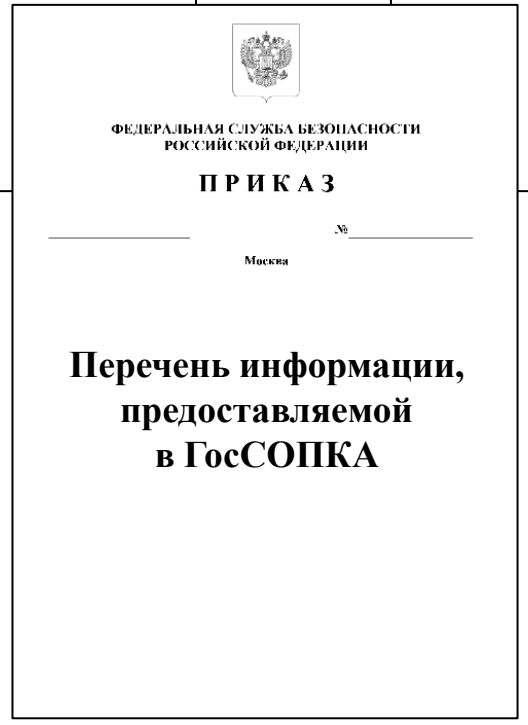
ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

П Р И К А З

_____ №_____

Москва

ПОРЯДОК
обмена информацией о компьютерных инцидентах



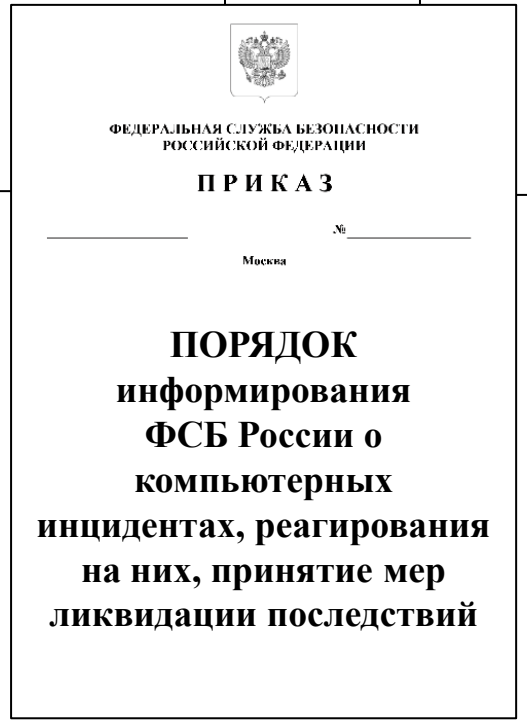
ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

П Р И К А З

_____ №_____

Москва

Перечень информации, предоставляемой в ГосСОПКА



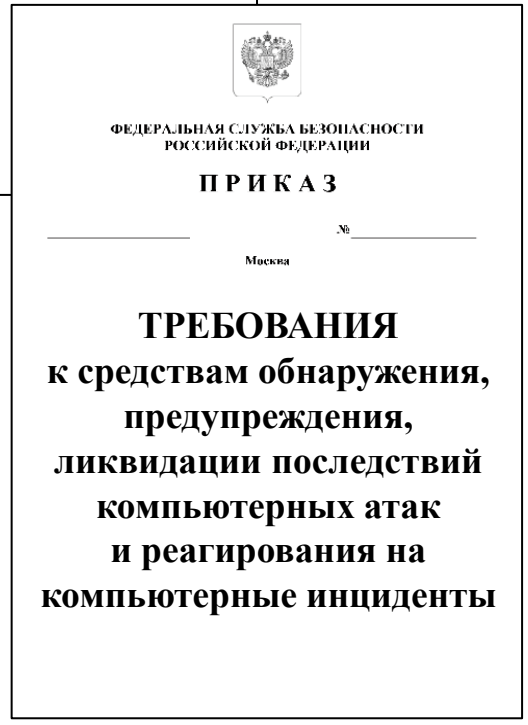
ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

П Р И К А З

_____ №_____

Москва

ПОРЯДОК
информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятие мер ликвидации последствий



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

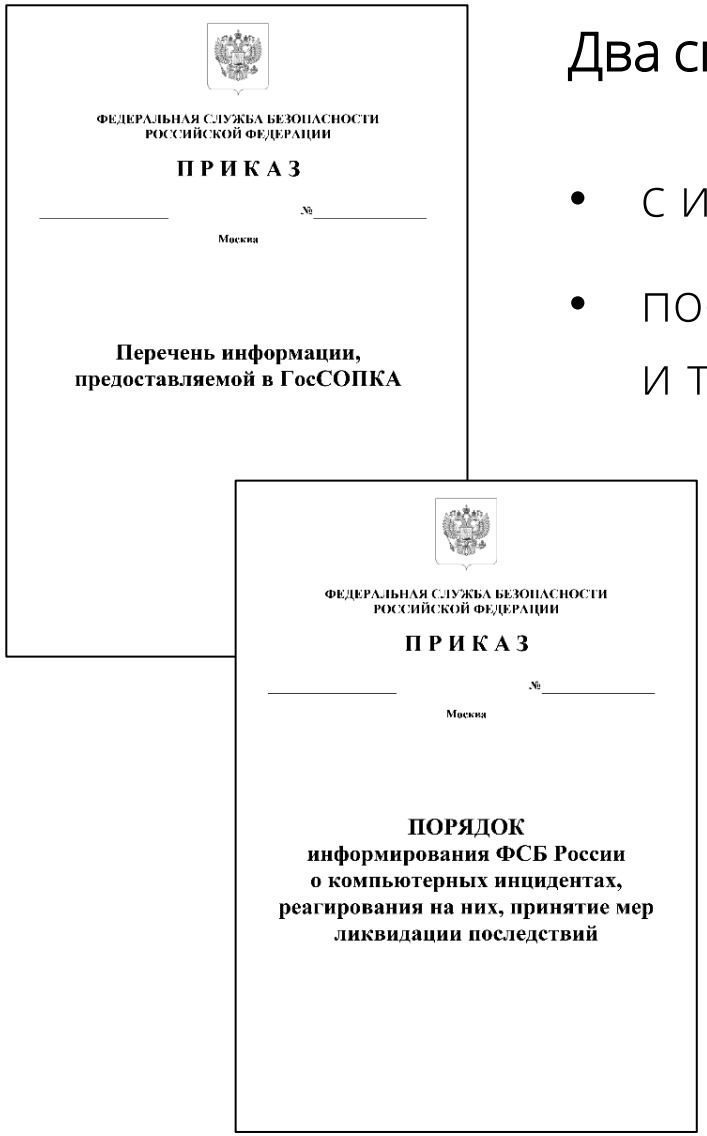
П Р И К А З

_____ №_____

Москва

ТРЕБОВАНИЯ
к средствам обнаружения, предупреждения, ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

ИНФРАСТРУКТУРА ОБМЕНА С НКЦКИ



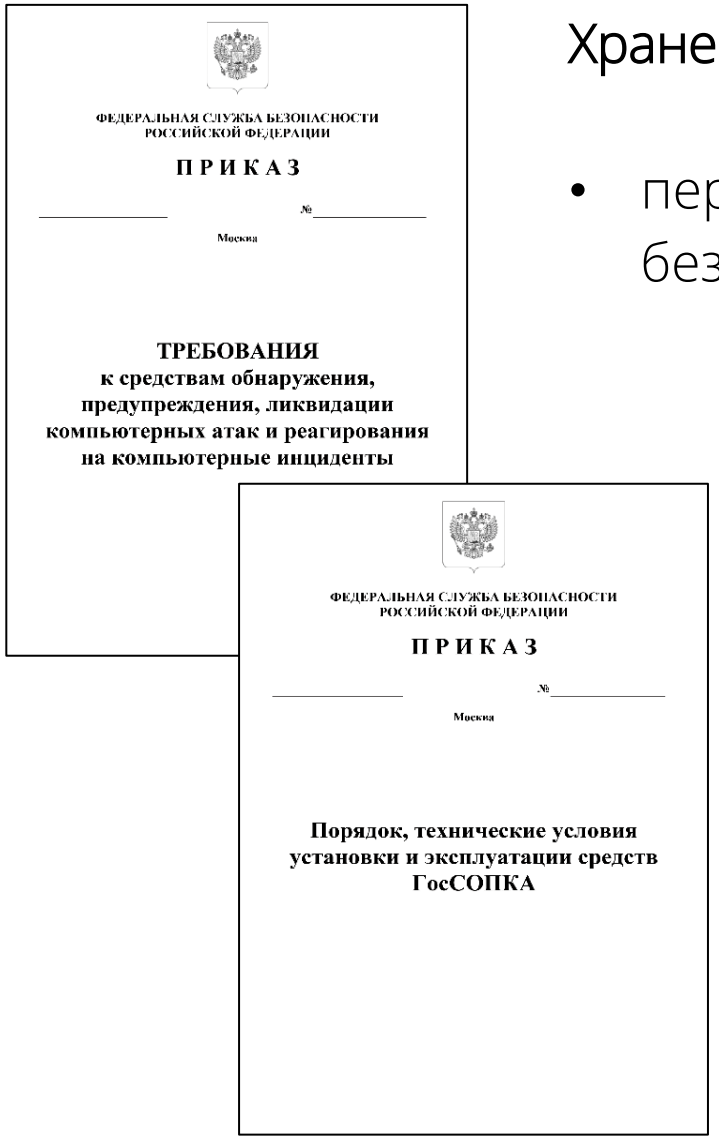
Два способа предоставления информации в НКЦКИ:

- с использованием технической инфраструктуры НКЦКИ
- посредством электронной, факсимильной, почтовой и телефонной связи

Субъекты КИИ:

- осуществляют реагирование на компьютерные инциденты с задействованием собственных сил и средств
- обращаются в ФСБ России для получения практической помощи

ТРЕБОВАНИЯ К СРЕДСТВАМ ГОССОПКА



Хранение информации о событиях ИБ

- период хранения информации о событиях информационной безопасности определяется субъектом КИИ самостоятельно

Установка средств ГосСОПКА

- субъект КИИ согласовывает установку средств с Центром защиты информации и специальной связи ФСБ России
- место установки средств определяется субъектом КИИ самостоятельно
- установка возможна организацией, осуществляющей лицензируемую деятельность в области защиты информации

ТРЕБОВАНИЯ К ЦЕНТРАМ ГОССОПКА

- Соглашение о взаимодействии с ФСБ России в области обнаружения, предупреждения и ликвидации последствий компьютерных атак
- Информационные ресурсы, в отношении которых планируется привлечь центр ГосСОПКА не входят в зону ответственности другого центра ГосСОПКА
- Наличие лицензий

ЛИЦЕНЗИИ ЦЕНТРА ГОССОПКА

ГОССОПКА

- Лицензия ФСБ России на право осуществления работ, связанных с использованием сведений, составляющих гостайну.
- Одна из лицензий ФСБ России на право:
  - осуществления работ, связанных с созданием средств защиты информации, содержащей сведения, составляющие гостайну;
  - деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств.

- Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации при оказании услуг по мониторингу информационной безопасности средств и систем информатизации.

УСЛУГИ ФСБ РОССИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КИИ

ГОССОПКА

- По обнаружению компьютерных атак:
  - подключение объектов КИИ в ведомственному центру ГосСОПКА ФСБ России
- По предупреждению компьютерных инцидентов:
  - аудит информационной безопасности объектов КИИ
  - мониторинг защищенности информационных систем общего пользования
- По реагированию на компьютерные инциденты:
  - реагирование на компьютерные инциденты

КОНТАКТЫ ДЛЯ ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ

ГОССОПКА

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

gov-cert@gov-cert.ru

+7 (4812) 20-37-37

ГОССОПКА

Спасибо за внимание!