Нормативное правовое регулирование вопросов обмена информацией о компьютерных инцидентах

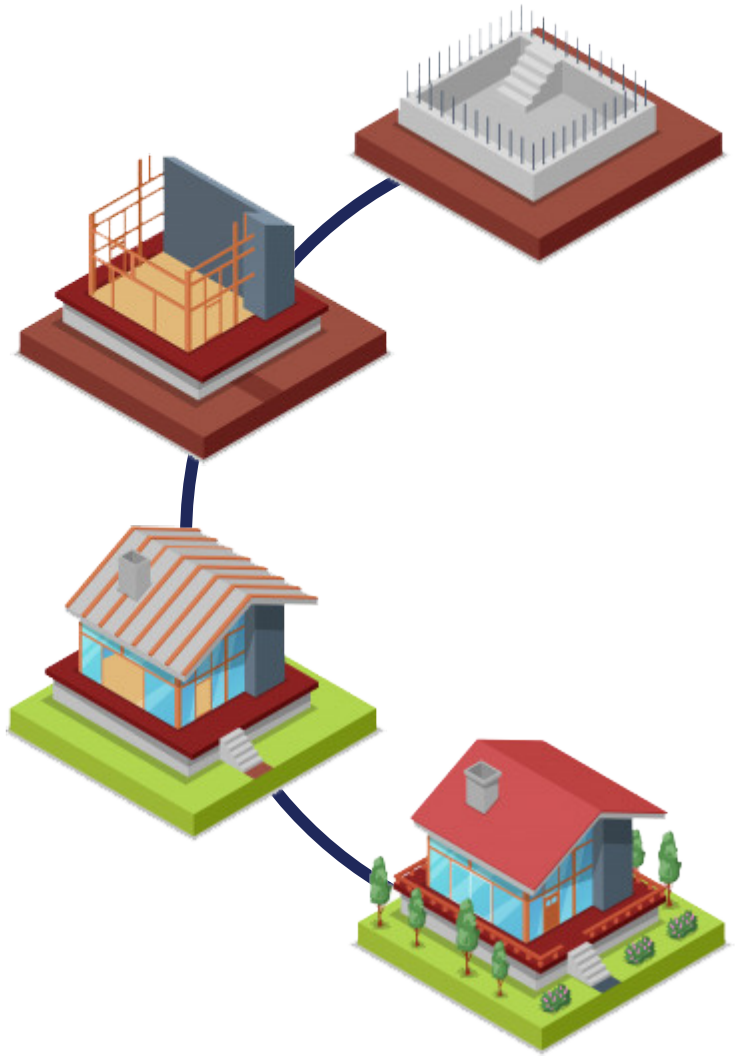
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

«Того, кто не задумывается о далеких трудностях, непременно поджидают близкие неприятности»

Конфуций

Критерии зрелости системы регулирования

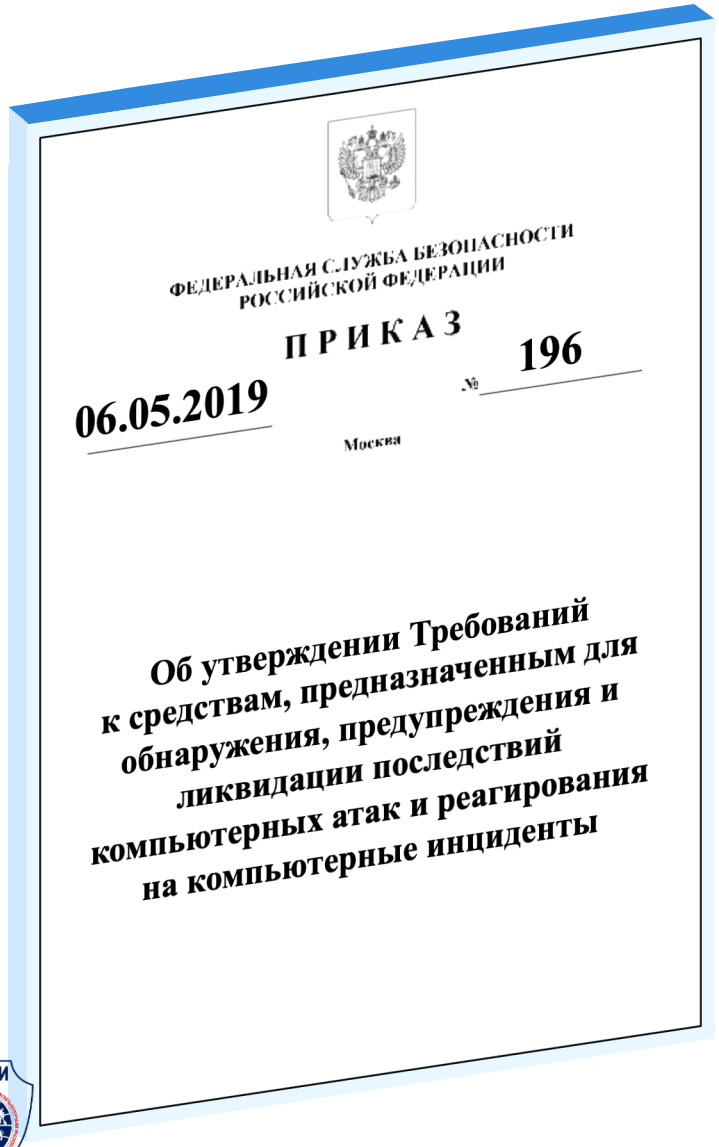
- Уполномоченные органы, осуществляющие регуляторную политику
- Профильное законодательство
- Неотвратимость наказания за несоблюдение НПА в области безопасности КИИ



Показатель зрелости системы регулирования

Уровень вовлеченности субъектов КИИ и иных органов и организаций в процесс взаимодействия

Нормативные правовые акты ФСБ России



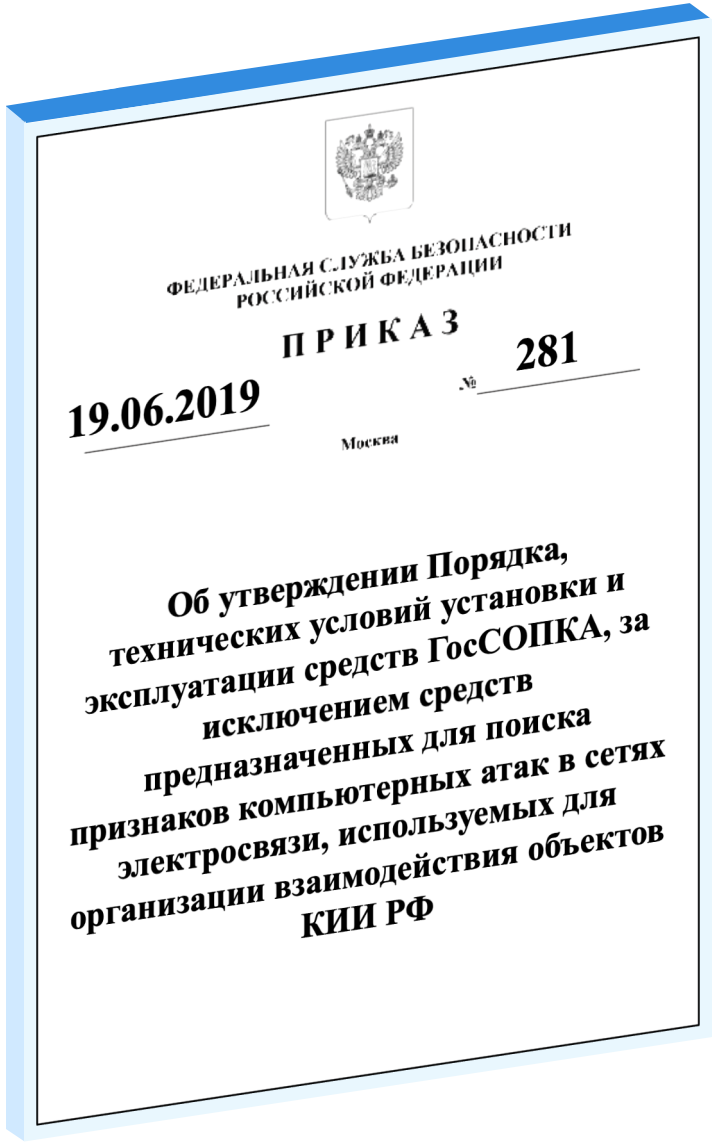
ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

П Р И К А З

06.05.2019 № 196

Москва

Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты



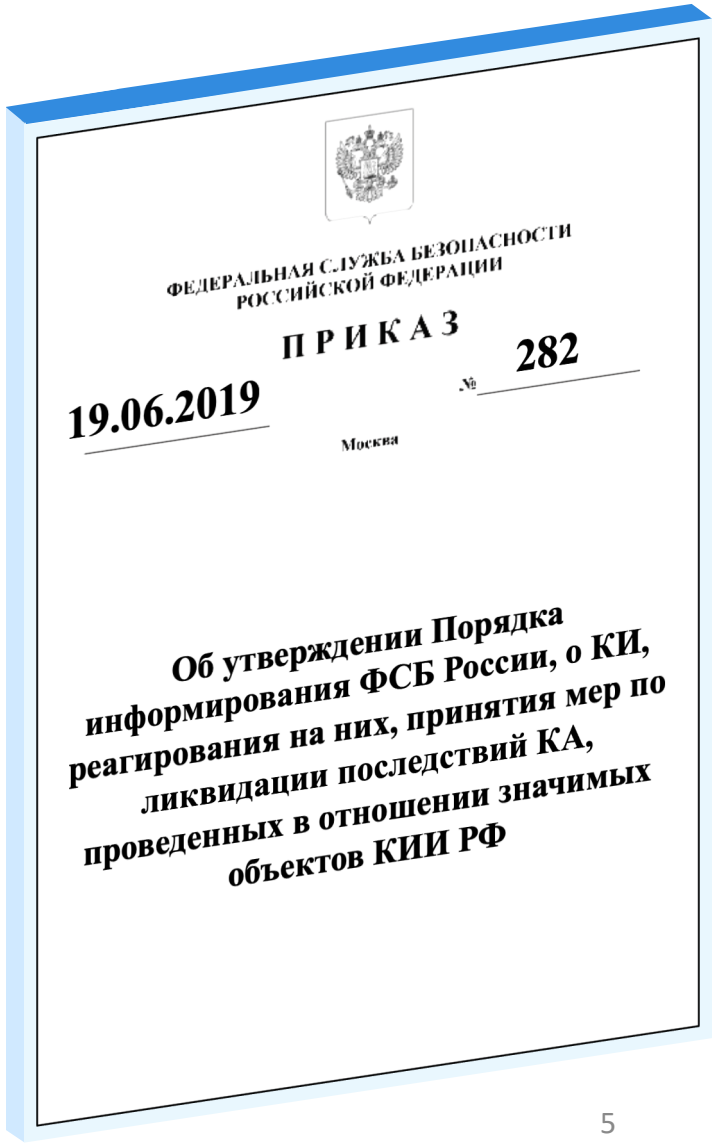
ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

П Р И К А З

19.06.2019 № 281

Москва

Об утверждении Порядка, технических условий установки и эксплуатации средств ГосСОПКА, за исключением средств предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ РФ



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

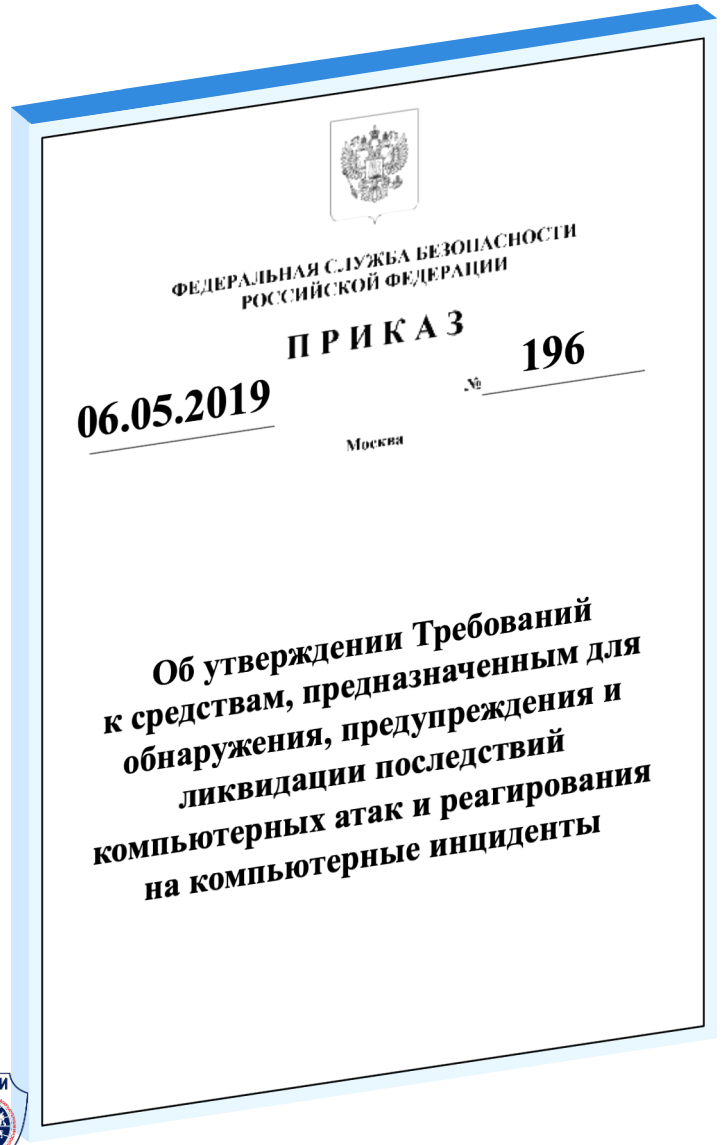
П Р И К А З

19.06.2019 № 282

Москва

Об утверждении Порядка информирования ФСБ России, о КИ, реагирования на них, принятия мер по ликвидации последствий КА, проведенных в отношении значимых объектов КИИ РФ

Два вида средств ГосСОПКА



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

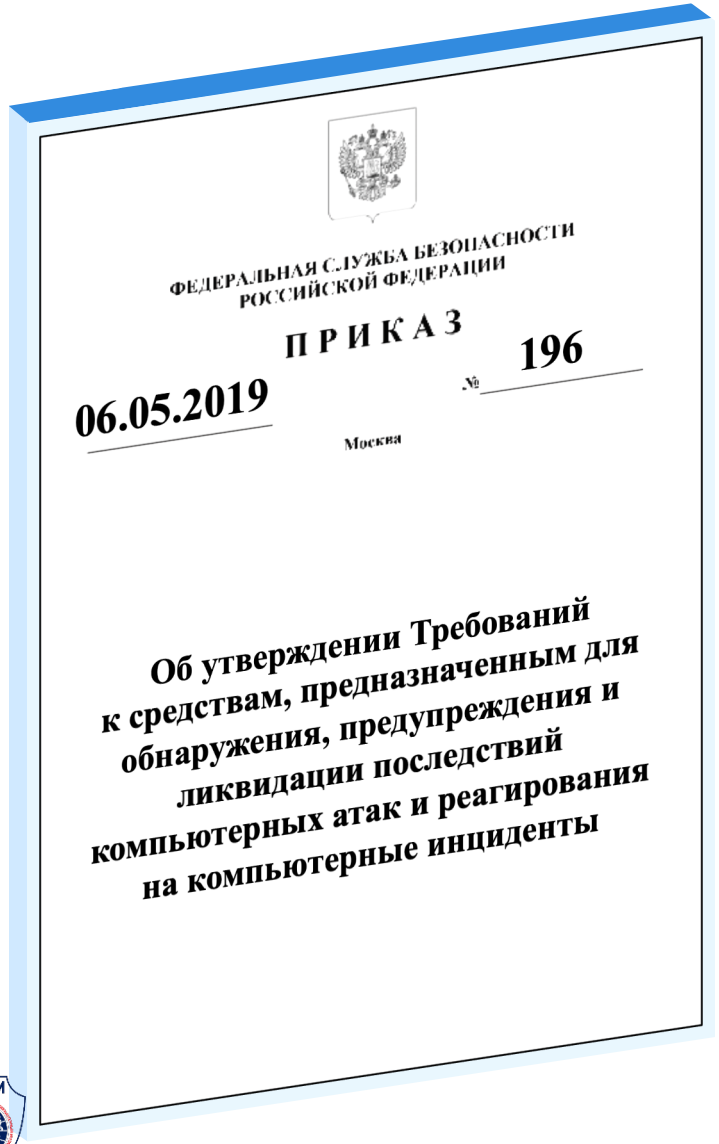
06.05.2019 № 196

Москва

Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

- Системы учёта событий ИБ (Security Information and event management, SIEM)
- Системы управления процессами реагирования на инциденты ИБ (Incident Response Platforms, IRP)

Назначение средств ГосСОПКА



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

06.05.2019 № 196

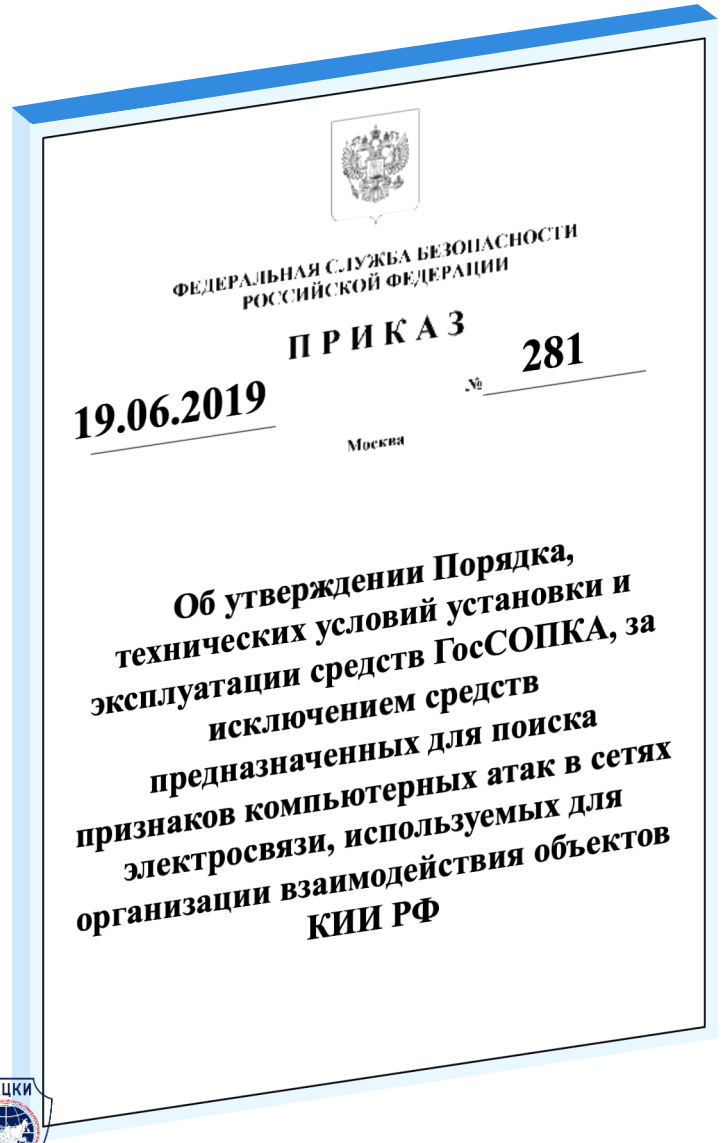
Москва

Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

Сбор, анализ и обработка событий ИБ, поступающих от **различных источников информации**:

- системы обнаружения вторжений
- межсетевых экранов
- антивирусных средств
- средств контроля защищенности и др.

Установка средств ГосСОПКА



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

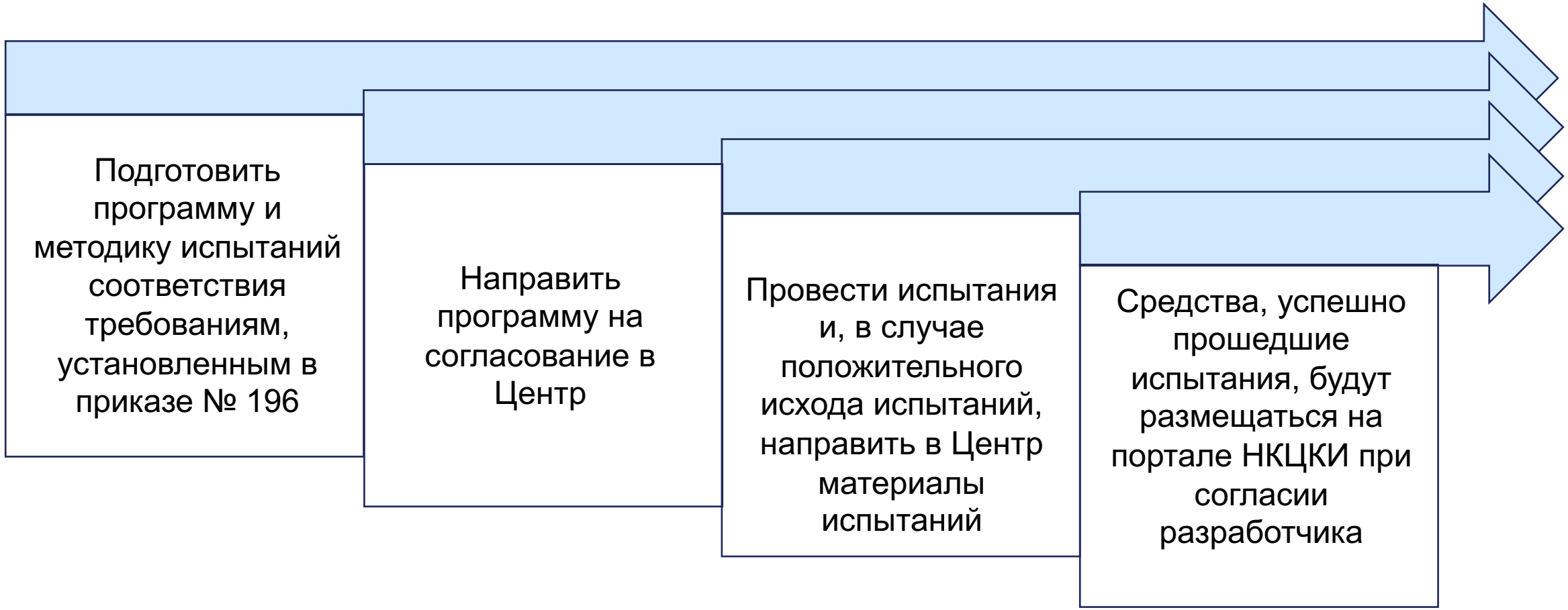
19.06.2019 № 281

Москва

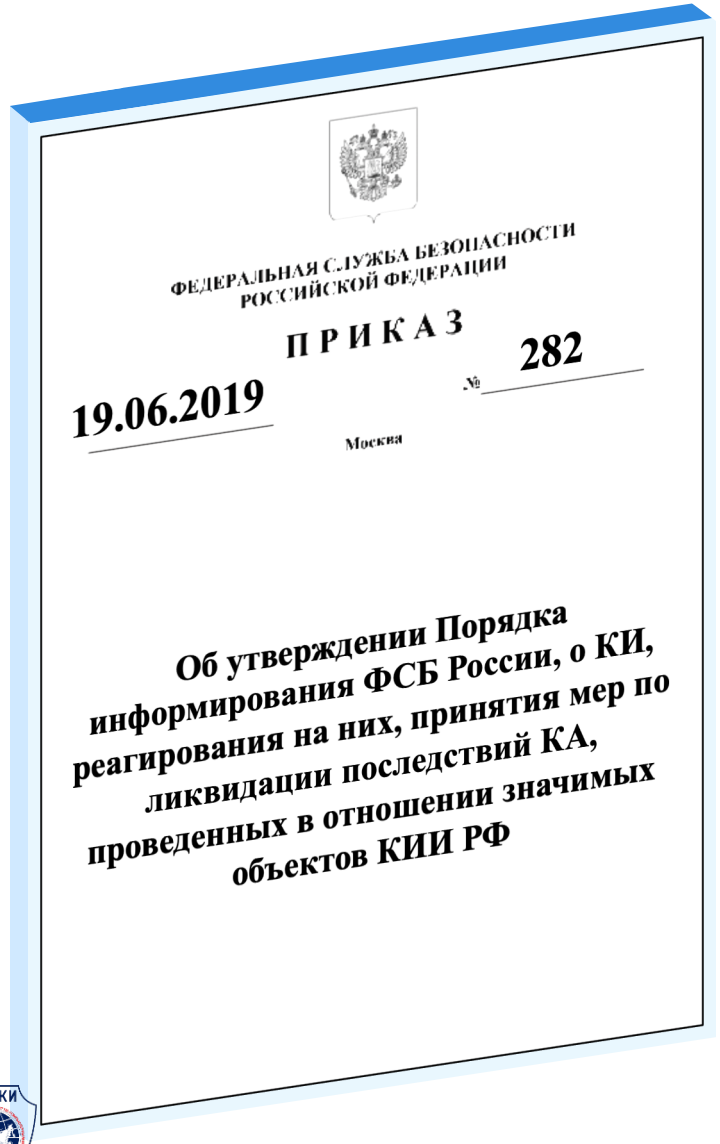
Об утверждении Порядка, технических условий установки и эксплуатации средств ГосСОПКА, за исключением средств предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ РФ

- Субъект КИИ согласовывает установку средств с ФСБ России
- Место установки средств определяется субъектом КИИ самостоятельно
- Установка возможна организацией, осуществляющей лицензируемую деятельность в области защиты информации

Рекомендации потенциальным разработчикам средств ГосСОПКА



Порядок информирования



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

19.06.2019 № 282

Москва

Об утверждении Порядка информирования ФСБ России, о КИ, реагирования на них, принятия мер по ликвидации последствий КА, проведенных в отношении значимых объектов КИИ РФ

- Субъекты КИИ информируют ФСБ России обо всех компьютерных инцидентах на своих объектах КИИ
- Информацию направлять с использованием:

incident@cert.gov.ru

+7 (916) 901-07-42

технической инфраструктуры НКЦКИ

При подключении к ТИ – запрос на info@cert.gov.ru или на 107031 г. Москва, ул. Б. Лубянка, д.1/3

Наиболее распространенные вопросы

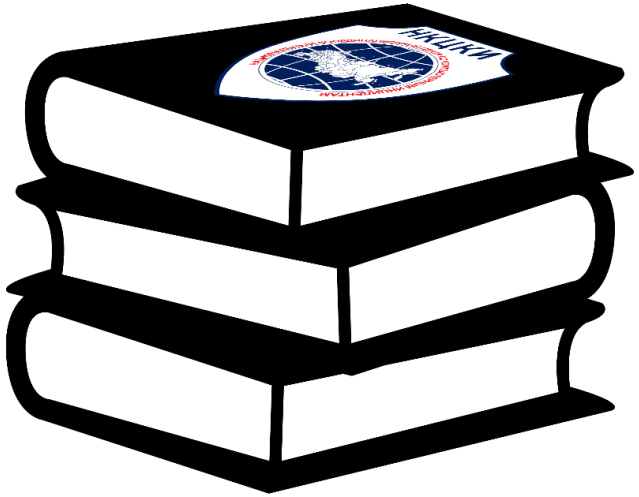
- О какой атаке и каком инциденте вам сообщать?
- Что значит подключиться к ГосСОПКА?

О какой атаке и каком инциденте сообщать

Направляем субъектам ГосСОПКА, заявившим о себе:

- Регламент информационного взаимодействия, где определены состав и форматы сведений о компьютерных инцидентах, которые необходимо направлять в НКЦКИ

- Подробное описание компьютерных инцидентов



Сообщите о себе, чтобы начать взаимодействие

info@cert.gov.ru

107031 г. Москва, ул. Б. Лубянка, д.1/3

С минимальной информацией о себе – наименование субъекта, контактная информация, IP адреса периметра

НКЦКИ

Порядок информирования

Субъект КИИ:

- Регистрирует компьютерные инциденты

НКЦКИ:

- Присваивает каждому КИ идентификационный номер и сообщает его субъекту КИИ

Что значит подключиться к ГосСОПКА?

- Мы установили систему обнаружения атак! Мы в ГосСОПКА?

- Мы заключили соглашение с ФСБ России! Мы в ГосСОПКА?

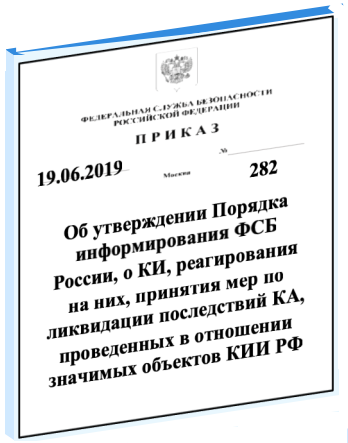
- Мы создали подразделение по реагированию на компьютерные инциденты! Мы в ГосСОПКА?

НКЦКИ

Участник ГосСОПКА решает основные задачи

- Создает систему обеспечения информационной безопасности
- Вносит свой вклад в формирование общей базы знаний о вредоносной активности
- Организует применение в системе защиты тех сведений, которые приходят из ГосСОПКА

Субъект КИИ, имеющий значимые объекты



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

19.06.2019 № 282

Об утверждении Порядка информирования ФСБ России, о КИ, реагирования на них, принятия мер по ликвидации последствий КА, проведенных в отношении значимых объектов КИИ РФ

Разрабатывает «План реагирования на КИ и принятия мер по ликвидации последствий КА»

Проводит тренировки по отработке Плана не реже одного раза в год

После завершения мероприятий по реагированию в течение 48 часов информирует НКЦКИ о результатах

При необходимости к реагированию привлекаются подразделения ФСБ России

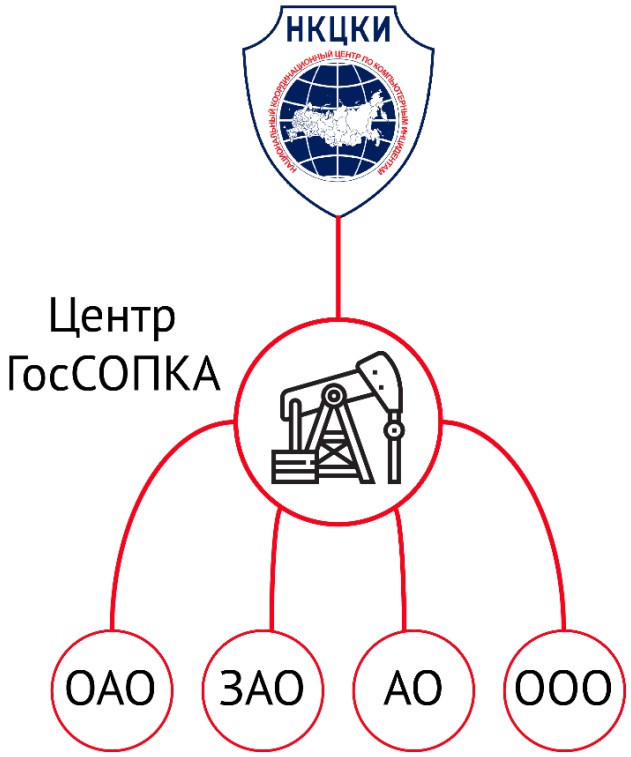
В случае привлечения подразделения ФСБ России

Субъект КИИ сообщает:

- наименование ИР, отнесение ИР к значимому объекту КИИ с указанием категории значимости
- адрес объекта размещения ИР
- контактную информация представителей Субъекта, ответственных за обеспечение функционирования ИР

При возникновении компьютерного инцидента – другие сведения о признаках инцидента или его последствиях

Взаимодействие с НКЦКИ через Центр ГосСОПКА



О достигнутой схеме взаимодействия субъекту КИИ необходимо сообщить в НКЦКИ

Эффективно противодействовать угрозам мы можем только сообща!

Спасибо за внимание!

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ