Основные вопросы организации взаимодействия с НКЦКИ
Обзор приказов ФСБ России

ГОССОПКА

13 областей КИИ

ГОССОПКА

Субъекты КИИ обязаны информировать НКЦКИ

Основные задачи НКЦКИ

ГОССОПКА

Координация деятельности субъектов КИИ,
а также органов и организаций
не являющихся таковыми

Практическая помощь в реагировании на
компьютерные инциденты

Адресное информирование об уязвимостях
ПО и актуальных угрозах

Рассылка индикаторов вредоносной активности
для автоматизированного выявления КИ

Силы ГосСОПКА

ГОССОПКА

Подразделения
и должностные лица
ФСБ России

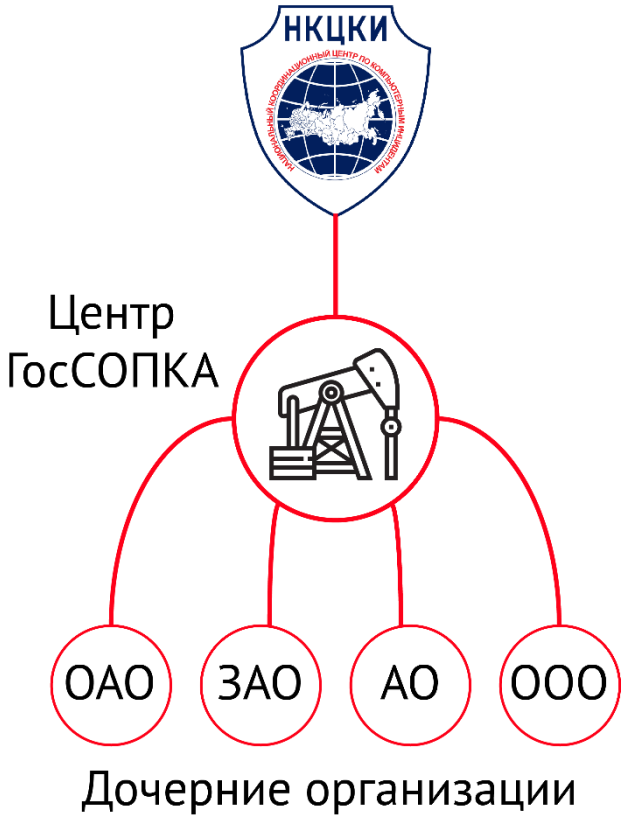
Национальный
координационный центр
по компьютерным
инцидентам

Подразделения и должностные
лица субъектов КИИ и иных
органов и организаций
(Центры ГосСОПКА)

Основные виды информирования НКЦКИ

ГОССОПКА

Информирование НКЦКИ через Центр ГосСОПКА

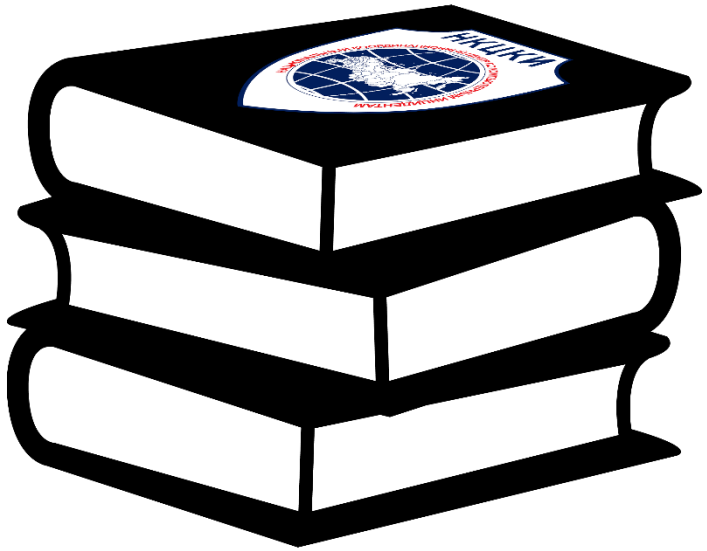


Информирование НКЦКИ напрямую

Перечень методических документов НКЦКИ

ГОССОПКА

- Требования к подразделениям и должностным лицам субъекта ГосСОПКА
- Методические рекомендации по созданию ведомственных и корпоративных центров
- Типовой Регламент информационного взаимодействия
- Методические рекомендации по обнаружению компьютерных атак на информационные ресурсы
- Методические рекомендации по установлению причин и ликвидации последствий компьютерных инцидентов
- Методические рекомендации по проведению мероприятий по оценке степени защищённости от компьютерных атак



Требования к Центрам ГосСОПКА

ГОССОПКА

ТРЕБОВАНИЯ
к подразделениям и должностным лицам субъектов ГосСОПКА

Субъект ГосСОПКА

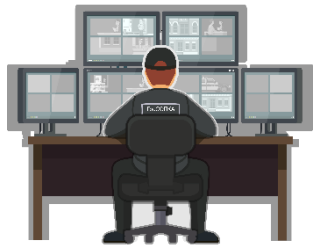
Центр ГосСОПКА
(подразделения, должностные лица субъекта ГосСОПКА)

Основные задачи Субъекта (Центра) ГосСОПКА

ГОССОПКА

Общие функции центра ГосСОПКА

ГОССОПКА

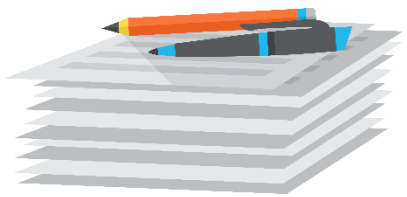


Эксплуатация средств ГосСОПКА

Центр ГосСОПКА

НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Взаимодействие с НКЦКИ



Разработка документации

Функции центра ГосСОПКА по обнаружению

ГОССОПКА

Центр ГосСОПКА

Анализ событий ИБ

Прием сообщений об инцидентах

Регистрация инцидентов

Общие функции центра ГосСОПКА по предупреждению и ликвидации

ГОССОПКА

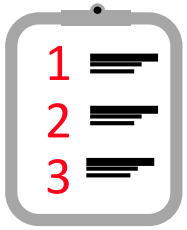
Центр ГосСОПКА

Подготовка рекомендаций по повышению защищенности

Анализ результатов ликвидации последствий инцидентов

Ликвидация последствий инцидентов

Составление перечня инцидентов

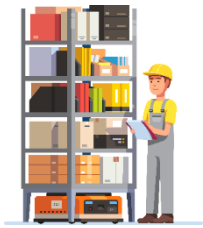


Подготовка рекомендаций по повышению защищенности

Выявление уязвимостей

Составление перечня угроз

Анализ угроз ИБ



Инвентаризация информационных ресурсов

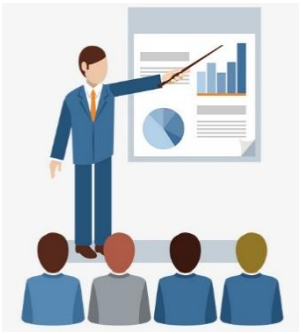
Общие функции центра ГосСОПКА по развитию сил и средств

ГОССОПКА

Центр ГосСОПКА

НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Направление в НКЦКИ информации по совершенствованию средств



Обучение и переподготовка персонала

Направление производителю средств информации об ошибках

Документы центра ГосСОПКА

ГОССОПКА

Положение о Центре ГосСОПКА

Регламент деятельности центра ГосСОПКА

Штатное расписание центра ГосСОПКА

Лицензии ФСБ России ФСТЭК России

Соглашение о взаимодействии с НКЦКИ

Нормативные правовые акты ФСБ России

ГОССОПКА

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

24.07.2018 № 366

Москва

ПОЛОЖЕНИЕ о Национальном координационном центре по компьютерным инцидентам

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

24.07.2018 № 367

Москва

ПЕРЕЧЕНЬ информации, предоставляемой в ГосСОПКА и ПОРЯДОК ее предоставления

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

24.07.2018 № 368

Москва

ПОРЯДОК обмена информацией о компьютерных инцидентах

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

06.05.2019 № 196

Москва

ТРЕБОВАНИЯ к средствам обнаружения, предупреждения и ликвидации последствий компьютерных атак

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

19.06.2019 № 281

Москва

ПОРЯДОК, технические условия установки и эксплуатации средств ГосСОПКА

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

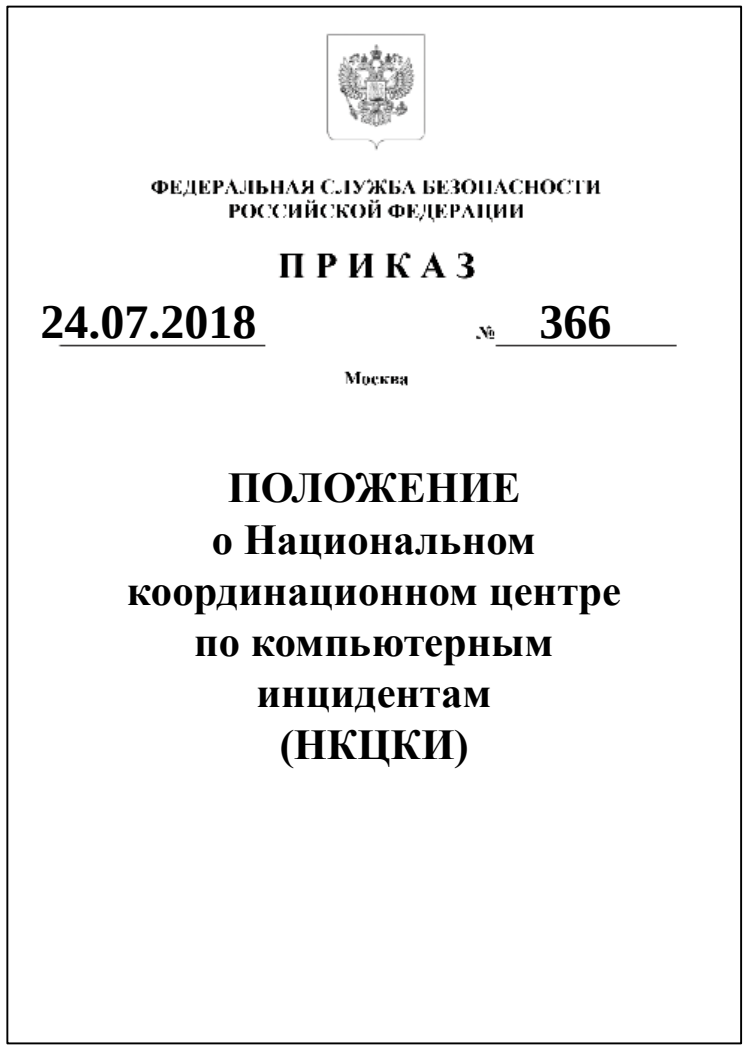
19.06.2019 № 282

Москва

ПОРЯДОК информирования ФСБ России о компьютерных инцидентах, реагирования на них

Положение о НКЦКИ

ГОССОПКА



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

П Р И К А З

24.07.2018 № 366

Москва

ПОЛОЖЕНИЕ
о Национальном координационном центре по компьютерным инцидентам (НКЦКИ)

- Координация мероприятий по реагированию на компьютерные инциденты
- Обмен информацией о компьютерных инцидентах между субъектами КИИ, а также с уполномоченными органами иностранных государств
- Сбор и анализ информации о компьютерных инцидентах
- Рассылку подготовленных НКЦКИ уведомлений об угрозах и способах противодействия, а также методическое сопровождение
- Определяет форматы представления информации и технические параметры компьютерных инцидентов
- Заключает соглашения о сотрудничестве

Направление информации о компьютерных инцидентах

ГОССОПКА

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

П Р И К А З

24.07.2018 № **367**

Москва

ПЕРЕЧЕНЬ информации, предоставляемой в ГосСОПКА и ПОРЯДОК ее предоставления

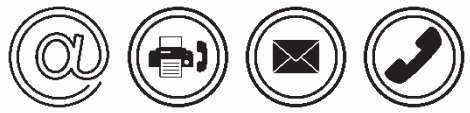
Информация направляется не позднее 24 часов с момента обнаружения КИ

- дата, время, место нахождения (местоположение) объекта КИИ
- наличие причинно-следственной связи между КИ и КА
- связь с другими КИ (при наличии)
- состав технических параметров КИ
- последствия КИ
- иная информация *

*(направляется в сроки, достаточные для проведения мероприятий по обнаружению, предупреждению и ликвидации последствий КА и реагированию на КИ)

Направлять с использованием технической инфраструктуры НКЦКИ

ИЛИ



Порядок обмена и получения информации

ГОССОПКА

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

П Р И К А З

24.07.2018 № 368

Москва

ПОРЯДОК
обмена информацией
о компьютерных инцидентах
и
ПОРЯДОК получения
информации
субъектами КИИ

Порядок обмена информацией

- Субъекты КИИ обмениваются информацией с НКЦКИ и другими субъектами КИИ (об этом информируют НКЦКИ)
- Обмен - в соответствии с форматами и составом технических параметров КИ
- Уведомления и запросы - техническая инфраструктура НКЦКИ, электронная, факсимильная, телефонная связь
- При получении инициативной информации от иностранной организации – субъект направляет её в НКЦКИ не позднее **24** часов с момента получения

Порядок обмена и получения информации

ГОССОПКА

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

П Р И К А З

24.07.2018 № 368

Москва

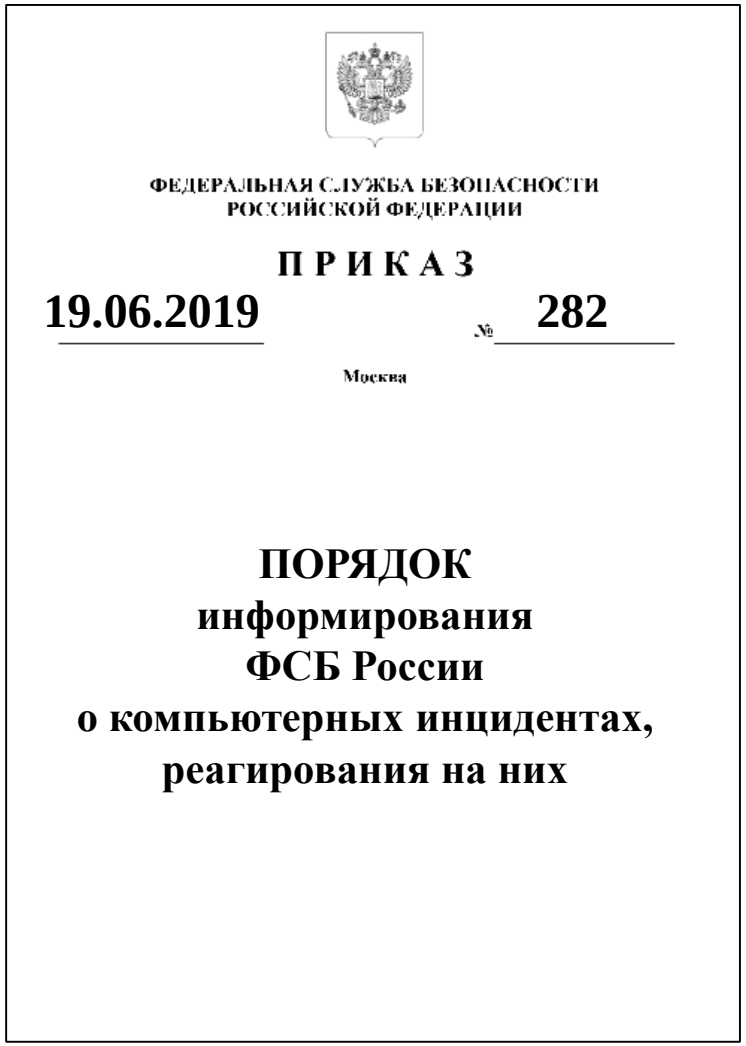
ПОРЯДОК
обмена информацией
о компьютерных инцидентах
и
ПОРЯДОК получения
информации
субъектами КИИ

Порядок получения информации

- Обращение к официальному сайту http://cert.gov.ru
- Направление запроса в НКЦКИ
- Направление обращений в ФСБ России
- Направление запросов другим субъектам КИИ, иностранным (международным) организациям, если запрос не содержит сведений о КИ, связанных с функционированием объектов КИИ

Порядок обмена и получения информации

ГОССОПКА



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

П Р И К А З

19.06.2019 № 282

Москва

ПОРЯДОК
информирования
ФСБ России
о компьютерных инцидентах,
реагирования на них

Субъект КИИ

- Информирует НКЦКИ обо всех КИ, путем направления информации в течение **24 часов** с момента обнаружения КИ, для значимых объектов в течение **3 часов**
(если в банковской сфере, то также уведомляет Банк России)

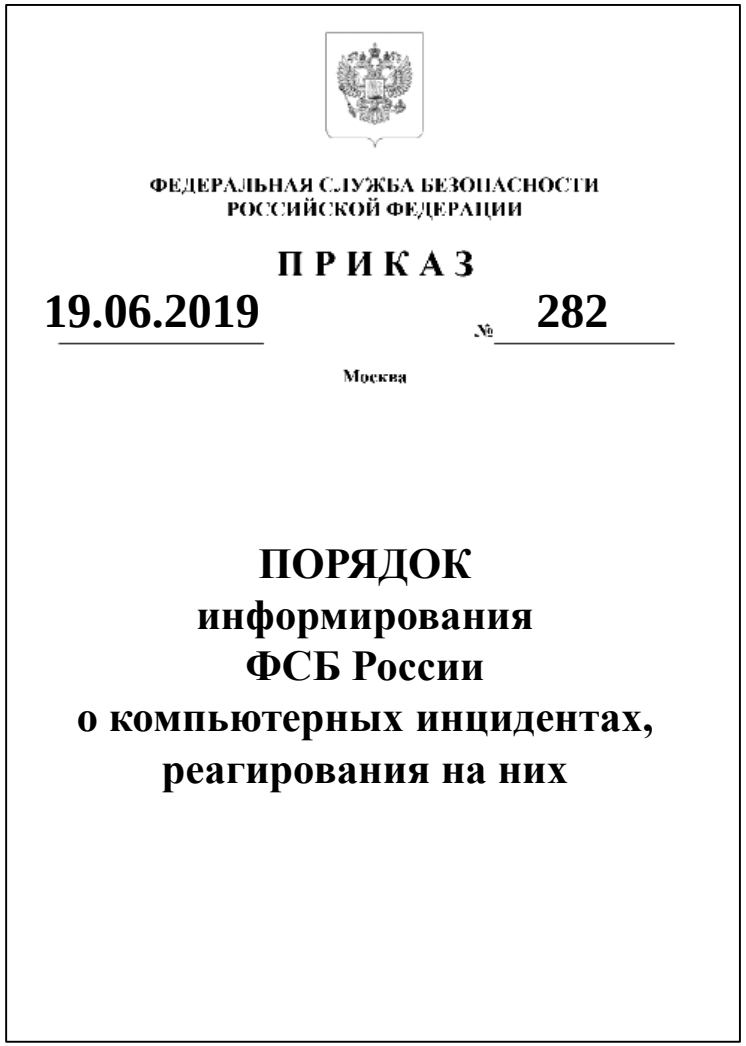
- Разрабатывает в течение **90 дней** с момента включения в реестр значимых объектов КИИ **«План реагирования и принятия мер»** и согласует с ФСБ России

- При необходимости определяет возможность привлечения подразделений и должностных лиц ФСБ России

- После завершения мероприятий по реагированию в течение **48 часов** о результатах информируется НКЦКИ

Порядок обмена и получения информации

ГОССОПКА



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

П Р И К А З

19.06.2019 № 282

Москва

ПОРЯДОК
информирования
ФСБ России
о компьютерных инцидентах,
реагирования на них

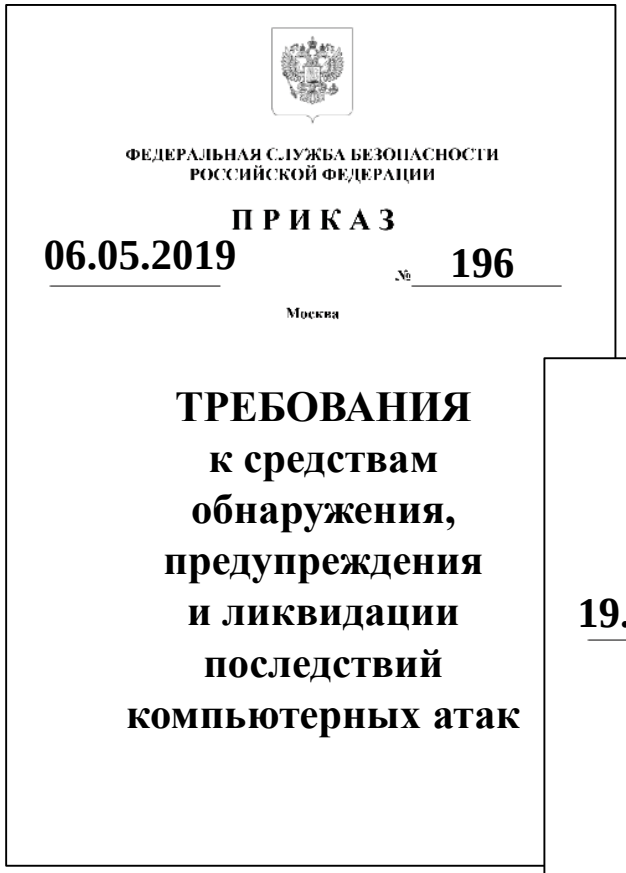
План реагирования и принятия мер

- Технические характеристики и состав значимых объектов КИИ
- События (условия), при наступлении которых начинается реализация предусмотренных планом мероприятий
- Мероприятия, проводимые в ходе реагирования КИ и принятия мер по ликвидации последствий КА, а также время, отводимое на их реализацию
- Описание состава подразделений и должностныъ лиц субъекта КИИ, ответственных за проведение мероприятий по реагированию на КИ

Не реже 1 раза в год субъект КИИ проводит тренировки по отработке Плана

Порядок обмена и получения информации

ГОССОПКА



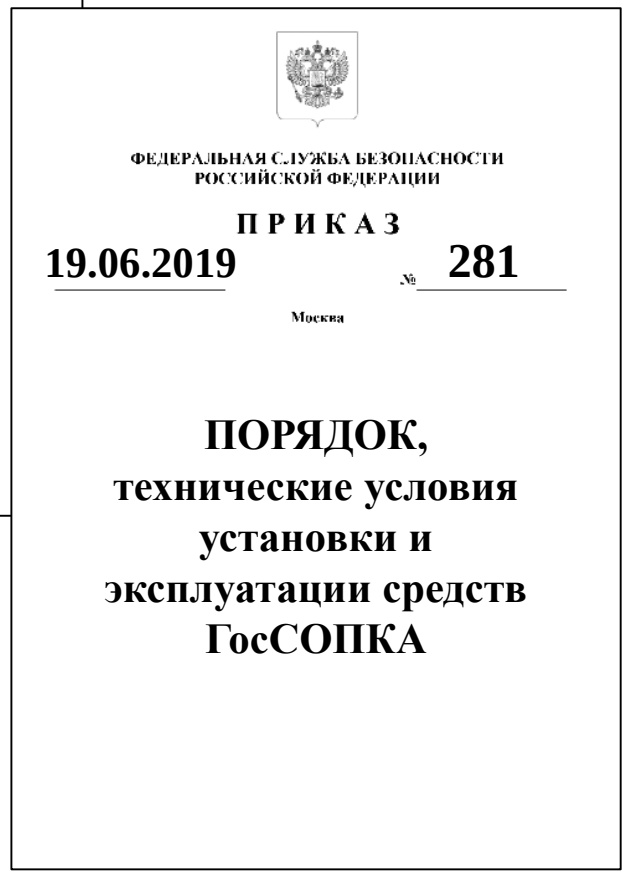
ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

06.05.2019 № 196

Москва

ТРЕБОВАНИЯ
к средствам
обнаружения,
предупреждения
и ликвидации
последствий
компьютерных атак



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

19.06.2019 № 281

Москва

ПОРЯДОК,
технические условия
установки и
эксплуатации средств
ГосСОПКА

Основные моменты

- Определяется перечень функций, которые необходимо реализовать в средствах ГосСОПКА
- Одно средство может выполнять как одну так и несколько функций
- Импортозамещение
- Определяется порядок согласования установки средств ГосСОПКА и описаны технические условия

Методические документы НКЦКИ

ГОССОПКА

Как получить методические документы

Направить письменный запрос на имя Директора НКЦКИ по адресу:

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

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Какие сведения необходимо отразить в запросе:

- информацию об организации
- цель получения документов
- сведения о лицензиях ФСБ России
- предполагаемую зону ответственности

ГОССОПКА

Взаимодействие с НКЦКИ!

Информирование о компьютерном инциденте:

- gov-cert@cert.gov.ru
- тел. +7 (916) 901-07-42
- заполнить соответствующую форму на сайте cert.gov.ru

По организационным вопросам
(соглашение, положение о центре и т.п.):

- gs@cert.gov.ru
- тел. +7 (499) 144-64-69

Спасибо за внимание!

ГОССОПКА