ГОССОПКА

Организация и координация взаимодействия субъектов критической информационной инфраструктуры Российской Федерации при решении задач обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты

СОВЕРШЕНСТВОВАНИЕ НОРМАТИВНОЙ ПРАВОВОЙ БАЗЫ

ГОССОПКА

Федеральный закон

- регулирует отношения в области обеспечения безопасности КИИ в целях ее устойчивого функционирования при проведении в отношении нее компьютерных атак
- определяет полномочия госорганов в области обеспечения безопасности КИИ
- определяет права, обязанности и ответственность лиц, владеющих на праве собственности или ином законном основании объектами КИИ

УЧАСТНИКИ ВЗАИМОДЕЙСТВИЯ В РАМКАХ ГОССОПКА

ГОССОПКА

Силы ГосСОПКА:

- Подразделения и должностные лица ФСБ России
- Национальный координационный центр по компьютерным инцидентам (НКЦКИ)
- Подразделения и должностные лица субъектов КИИ

ОСНОВНАЯ ЗАДАЧА НКЦКИ – КООРДИНАЦИЯ ДЕЯТЕЛЬНОСТИ СУБЪЕКТОВ КИИ

ГОССОПКА

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ №_____

Москва

ПОЛОЖЕНИЕ
о Национальном координационном центре по компьютерным инцидентам
№ 366 от24.07.18

Задачи и функции:

- Координация деятельности субъектов КИИ
- Взаимодействие между НКЦКИ субъектами КИИ и иными органами и организациями не КИИ
- Обмен информацией о компьютерных инцидентах с уполномоченными органами иностранных государств
- Рассылку подготовленных НКЦКИ уведомлений об угрозах и способах противодействия
- Определяет форматы взаимодействия
- Сбор и анализ информации
- Заключает соглашения о сотрудничестве
- Создавать РГ с субъектами КИИ

ОПРЕДЕЛЯЕТ ПРАВИЛА ОБМЕНА ИНФОРМАЦИЕЙ О КОМПЬЮТЕРНЫХ ИНЦИДЕНТАХ ГОССОПКА

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ №_____

Москва

ПОРЯДОК
обмена информацией
о компьютерных
инцидентах и
ПОРЯДОК получения
информации
субъектами КИИ
№ 368 от 24.07.2018

Порядок обмена:

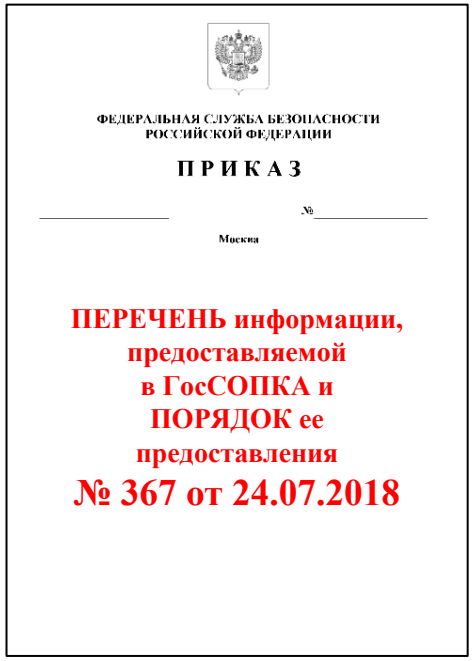
- Субъекты КИИ обмениваются информацией с НКЦКИ и другими субъектами КИИ (об этом информируют НКЦКИ)
- Обмен – в соответствии с форматами и составом технических параметров КИ
- Уведомления и запросы – техническая инфраструктура НКЦКИ, электронная, факсимильная, телефонная связь
- При получении инициативной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

Порядок получения:

- Субъекты КИИ получают информацию о средствах и способах проведения КА и о методах их предупреждения
- Направляют запрос в НКЦКИ

ИНФРАСТРУКТУРА ОБМЕНА С НКЦКИ

ГОССОПКА



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ №_____

Москва

ПЕРЕЧЕНЬ информации, предоставляемой в ГосСОПКА и ПОРЯДОК ее предоставления
№ 367 от 24.07.2018

Предоставляется в НКЦКИ в соответствии с его форматами

Способы предоставления информации в НКЦКИ:

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

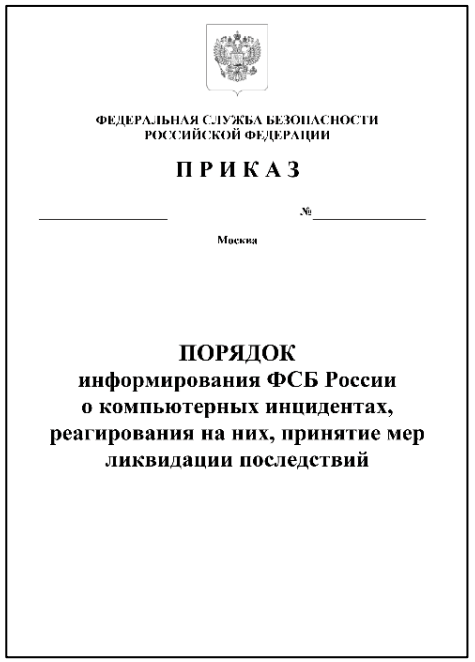
Предоставляемая информация:

- Дата, время, место нахождения объекта КИИ
- Наличие причинно-следственной связи между КИ и КА
- Связь с другими КИ (при наличии)
- Состав технических параметров КИ
- Последствия КИ
- Иная информация

Информация направляется не позднее **24 часов** с момента обнаружения КИ

ИНФРАСТРУКТУРА ОБМЕНА С НКЦКИ

ГОССОПКА



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ №_____

Москва

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

План

- Состав значимых объектов
- События, при которых осуществляется ввод Плана
- Проводимые мероприятия входе реагирования
- Ответственные и привлекаемые силы

Субъекты КИИ:

- Информируют НКЦКИ обо всех КИ, связанных с функционированием объектов КИИ

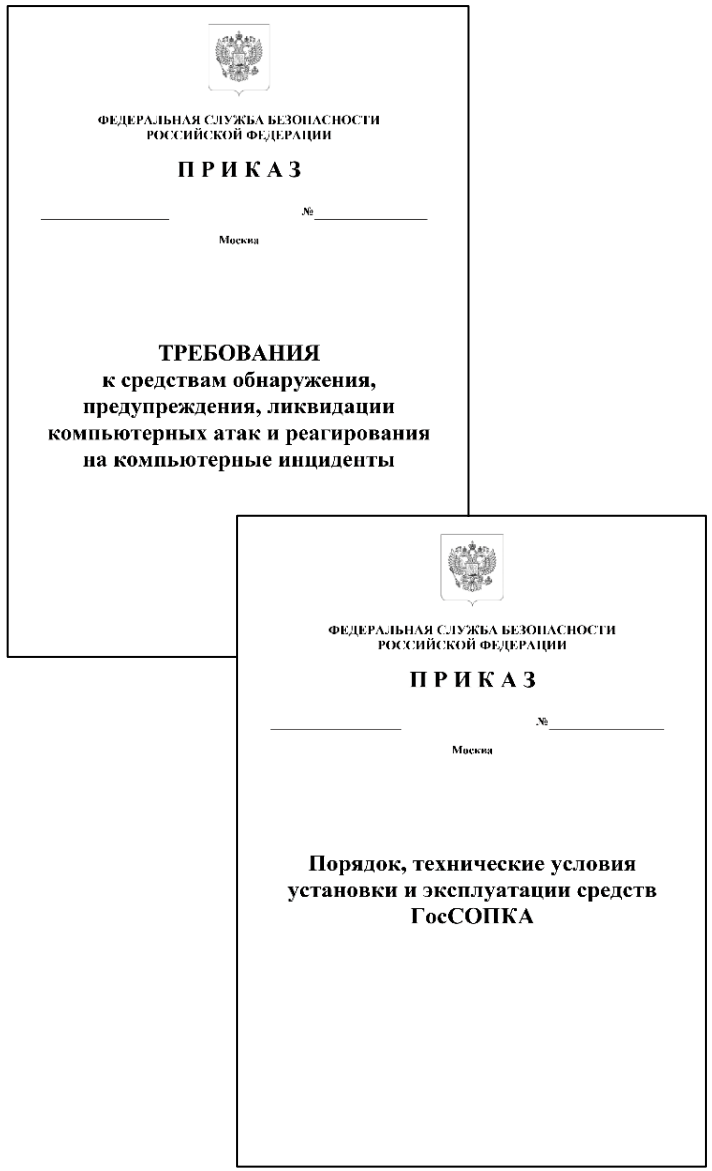
Значимый объект КИИ: Не более 3 часов с момента обнаружения КИ

Объект КИИ: в срок не более 24 часов с момента обнаружения КИ

Субъекты КИИ:

- Осуществляют реагирование на компьютерные инциденты с задействованием собственных сил и средств
- В праве обращаться в ФСБ России для получения практической помощи – Разрабатывается Регламент
- В целях подготовки разрабатывается План реагирования
- О результатах реагирования информируется НКЦКИ в срок не более 48 часов

ТРЕБОВАНИЯ К СРЕДСТВАМ ГОССОПКА


ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ №_____

Москва

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

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

_____ №_____

Москва

Порядок, технические условия установки и эксплуатации средств ГосСОПКА

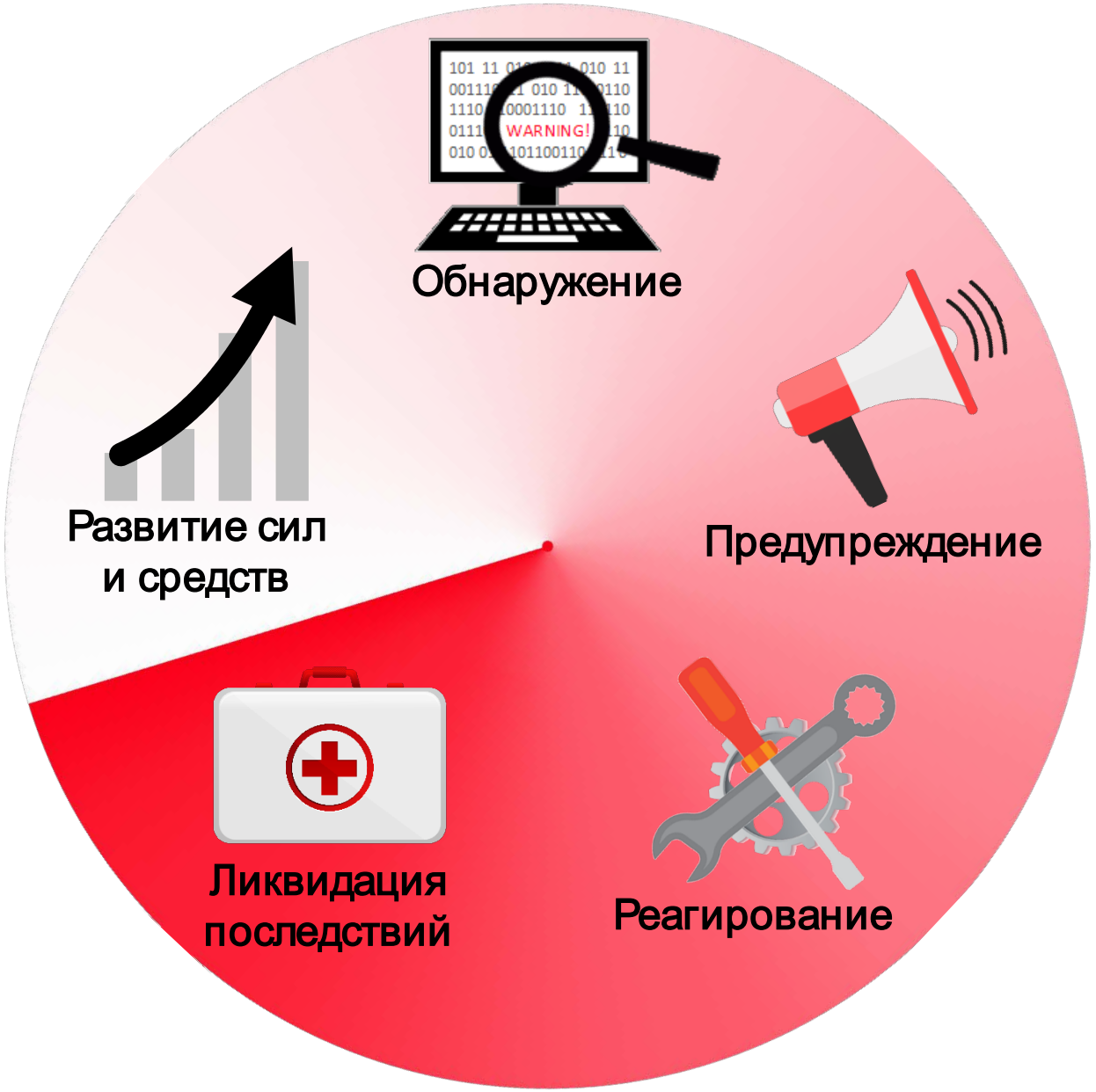
- Отсутствие возможности принудительного обновления или удаленного управления со стороны лиц, не являющихся сотрудниками субъекта КИИ и (или) привлекаемыми работниками организации-лицензиата
- Отсутствие возможности бесконтрольной передачи информации в том числе лицами, осуществляющим техподдержку, ремонт, техобслуживание
- Модернизация, техподдержка российскими организациями

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

ОСНОВНЫЕ ЗАДАЧИ СУБЪЕКТА (ЦЕНТРА) ГОССОПКА

ГОССОПКА



ФУНКЦИИ ЦЕНТРА ГОССОПКА

ГОССОПКА

Центр ГосСОПКА

Обнаружение КА и выявление КИ

Предупреждение и ликвидация

Эксплуатация средств ГосСОПКА

Направление производителю информации об ошибках и в НКЦКИ предложений по совершенствованию средств

Разработка документов

Взаимодействие с НКЦКИ

Развитие сил и средств

Для понимания какие объекты защищать, а также где и как реагировать, необходимо провести инвентаризацию информационных ресурсов (активов) органа, организации, предприятия.