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

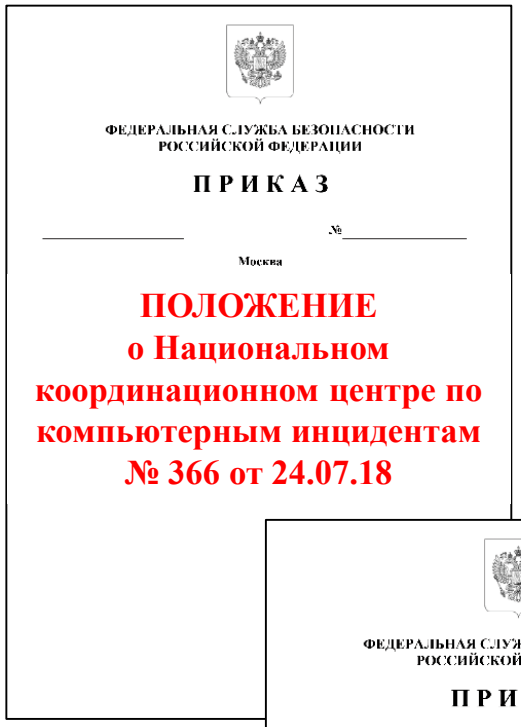
ГОССОПКА

Силы ГосСОПКА:

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

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
№ 366 от 24.07.18


ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

П Р И К А З

Москва

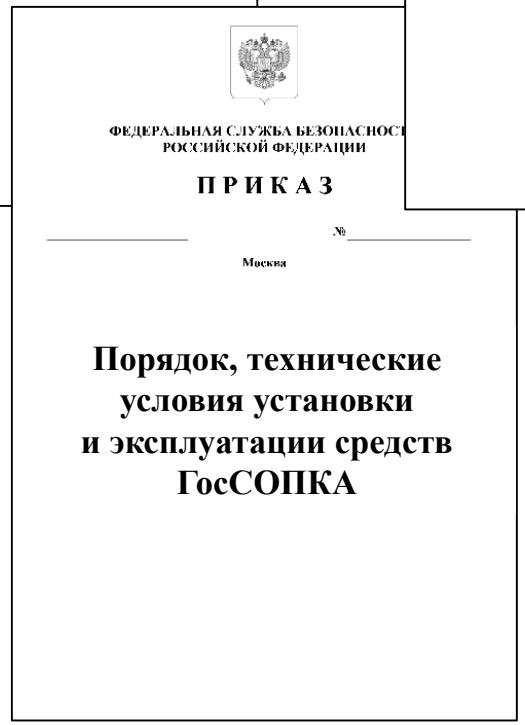
Перечень информации, предоставляемой в ГосСОПКА
№ 367 от 24.07.2018


ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

П Р И К А З

Москва

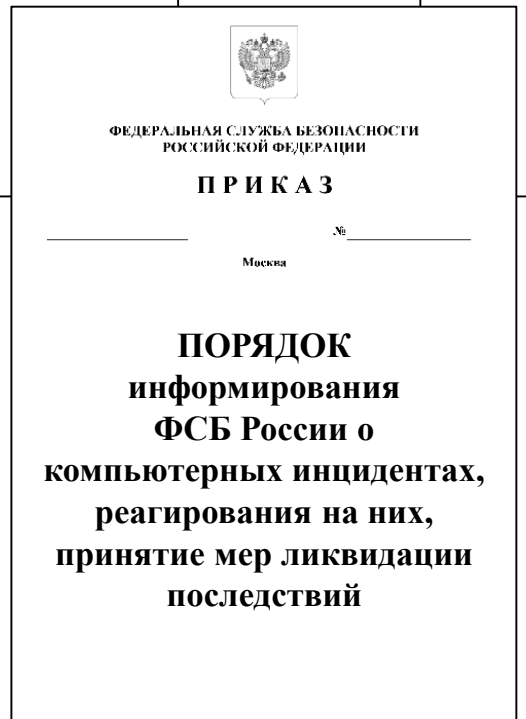
ПОРЯДОК
обмена информацией о компьютерных инцидентах
№ 368 от 24.07.2018


ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТ
РОССИЙСКОЙ ФЕДЕРАЦИИ

П Р И К А З

Москва

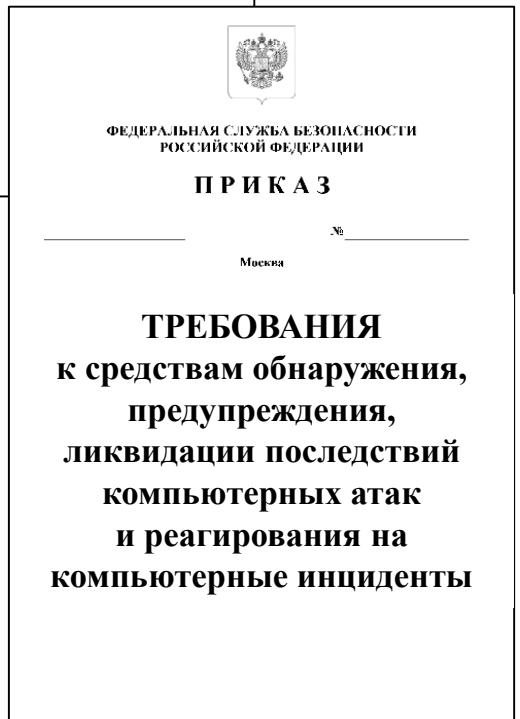
Порядок, технические условия установки и эксплуатации средств ГосСОПКА


ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

П Р И К А З

Москва

ПОРЯДОК
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

ОСНОВНАЯ ЗАДАЧА НКЦКИ – КООРДИНАЦИЯ ДЕЯТЕЛЬНОСТИ СУБЪЕКТОВ КИИ

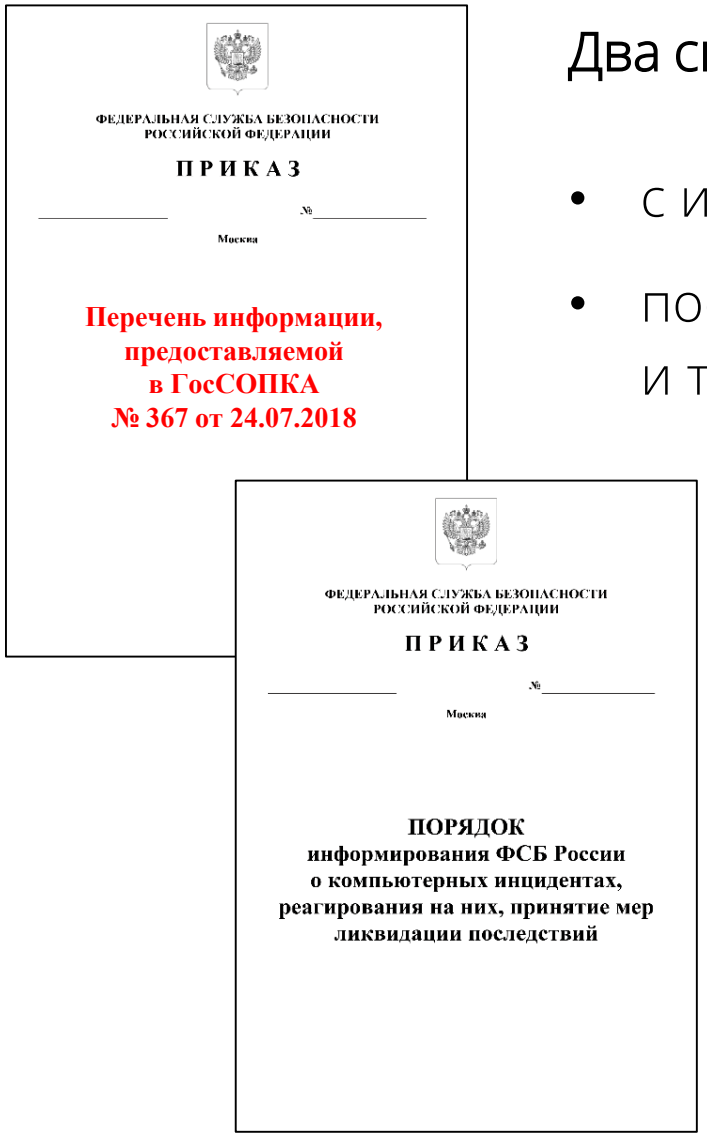
ГОССОПКА

Проекты приказов предусматривают:

- взаимодействие между НКЦКИ и субъектами КИИ
- обмен информацией о компьютерных инцидентах с уполномоченными органами иностранных государств
- рассылку подготовленных НКЦКИ уведомлений об угрозах и способах противодействия

ИНФРАСТРУКТУРА ОБМЕНА С НКЦКИ

ГОССОПКА



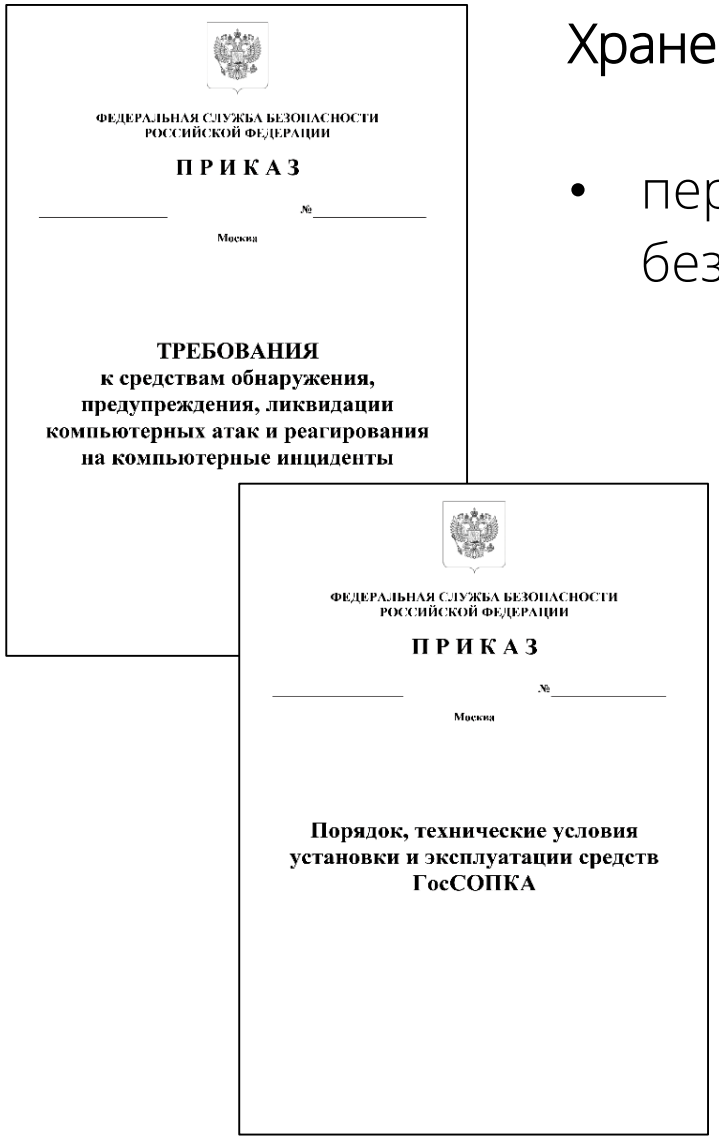
Два способа предоставления информации в НКЦКИ:

- 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

МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ ГОССОПКА

ГОССОПКА

Требования к подразделениям и должностным лицам субъекта ГосСОПКА*

Регламент информационного взаимодействия

Методические рекомендации по обнаружению КА на информационные ресурсы*

Методические рекомендации по установлению причин и ликвидации последствий компьютерных инцидентов*

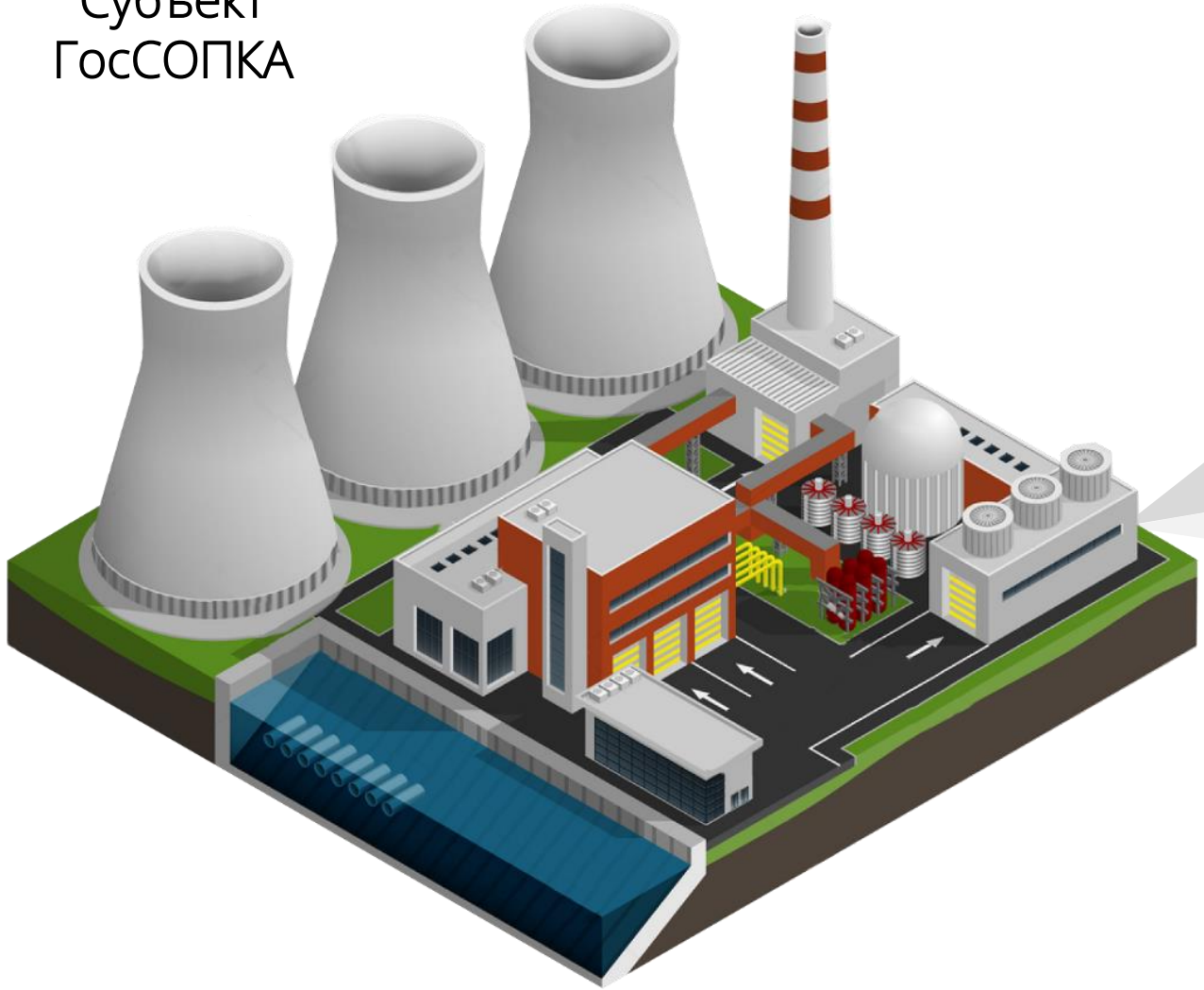
Методические рекомендации по проведению мероприятий по оценке степени защищенности от компьютерных атак

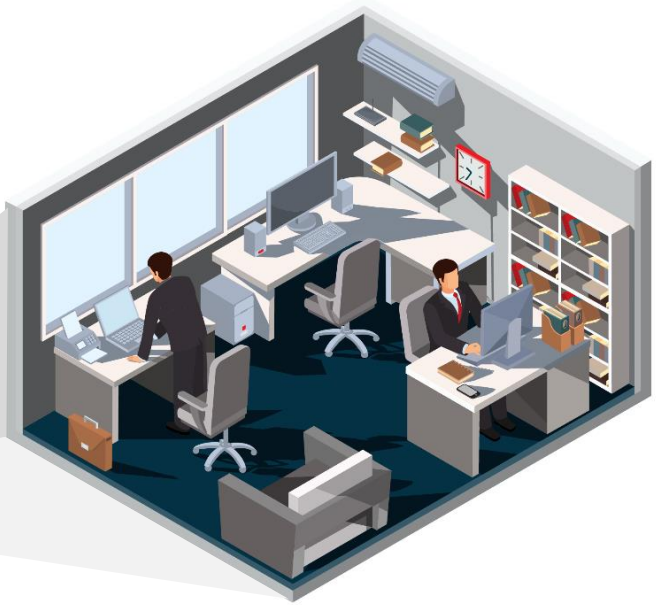
Варианты организации защищенного канала

СУБЪЕКТЫ ГОССОПКА

ГОССОПКА

Субъект ГосСОПКА





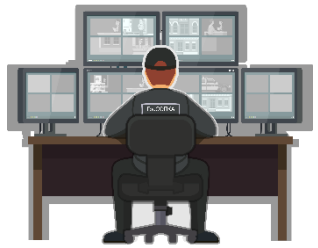
Центр ГосСОПКА
(подразделения, должностные лица субъекта ГосСОПКА)

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

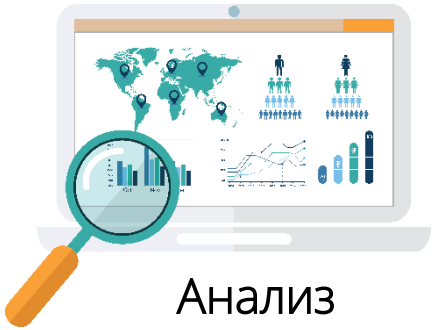
Направление производителю информации об ошибках

Разработка документов

ФУНКЦИИ ЦЕНТРА ГОССОПКА ПО ОБНАРУЖЕНИЮ

ГОССОПКА

Центр ГосСОПКА



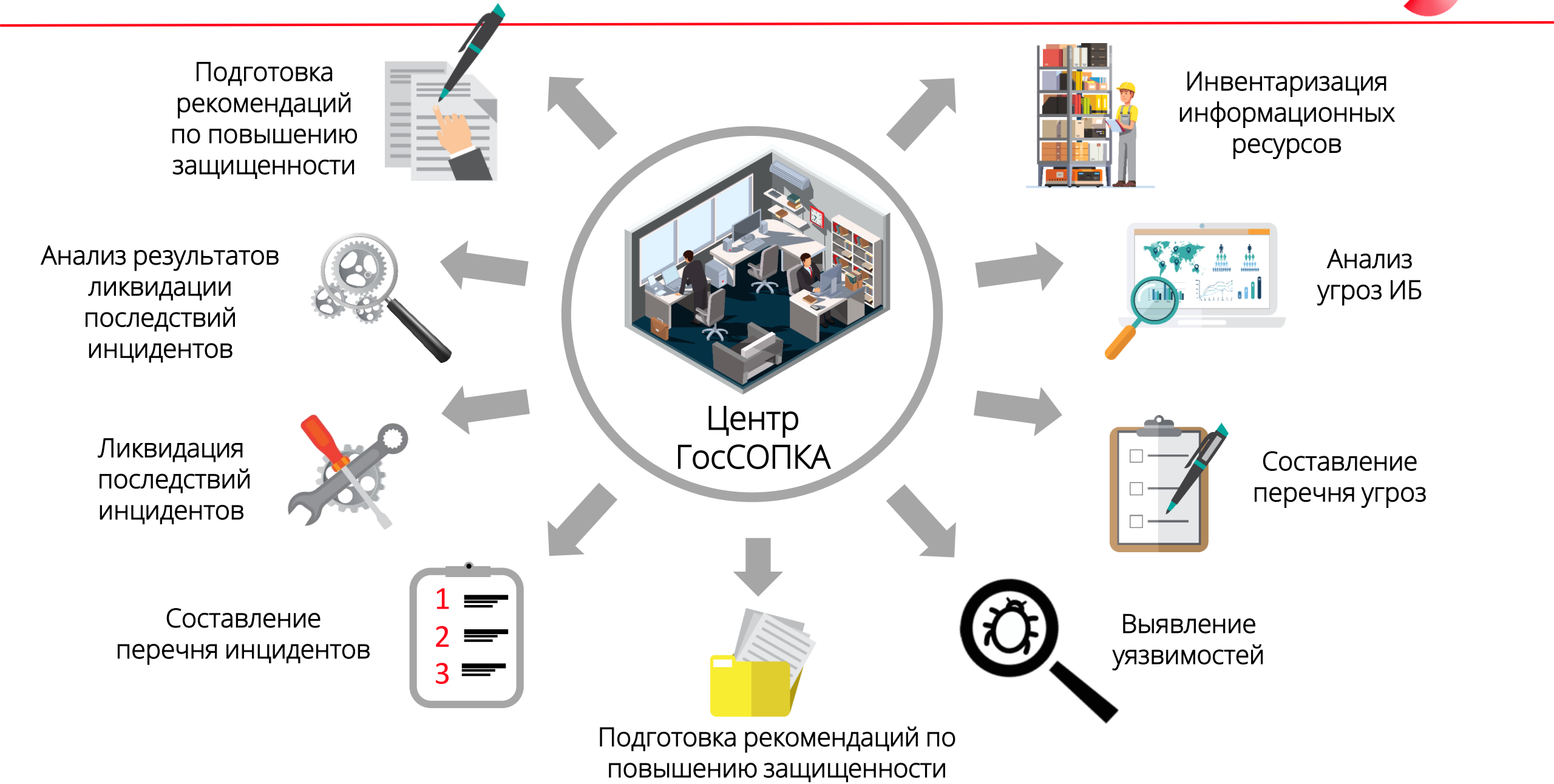
Анализ событий ИБ

Прием сообщений об инцидентах

Регистрация инцидентов

ФУНКЦИИ ЦЕНТРА ГОССОПКА ПО ПРЕДУПРЕЖДЕНИЮ И ЛИКВИДАЦИИ

ГОССОПКА



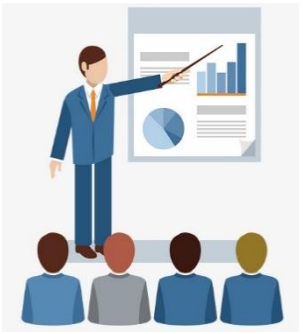
ФУНКЦИИ ЦЕНТРА ГОССОПКА ПО РАЗВИТИЮ СИЛ И СРЕДСТВ

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

ПРИНЦИПЫ РАБОТЫ СО СПЕЦИАЛИСТАМИ

ГОССОПКА

Специалисты первой линии

Специалист по взаимодействию с персоналом и пользователями

- Прием сообщений персонала и пользователей
- Подготовка информации для предоставления в НКЦКИ
- Взаимодействие с НКЦКИ

Специалист по обнаружению компьютерных атак и инцидентов

- Анализ событий информационной безопасности
- Регистрация компьютерных атак и инцидентов

Специалист по обслуживанию средств центра ГосСОПКА

- Обеспечение функционирования средств, размещаемых в центре ГосСОПКА, а также дополнительных средств защиты информационных систем

ПРИНЦИПЫ РАБОТЫ СО СПЕЦИАЛИСТАМИ

ГОССОПКА

Специалисты второй линии

Специалист по оценке защищенности

- Проведение инвентаризации информационных ресурсов
- Выявление уязвимостей
- Сбор и анализ выявленных уязвимостей и угроз
- Установление соответствия требований по информационной безопасности принимаемым мерам

Специалист по ликвидации последствий компьютерных инцидентов

- Координация действий при реагировании на компьютерные инциденты и приведение в штатный режим работы
- Взаимодействие с НКЦКИ

Специалист по установлению причин компьютерных инцидентов

- Установление причин компьютерных инцидентов
- Анализ последствий инцидентов и подготовка перечня компьютерных инцидентов
- Взаимодействие с НКЦКИ

ПРИНЦИПЫ РАБОТЫ СО СПЕЦИАЛИСТАМИ

ГОССОПКА

Специалисты третьей линии

Аналитик

- Анализ информации, предоставляемой специалистами 1-й и 2-й линий
- Выявление и анализ угроз информационной безопасности
- Прогнозирование развития угроз
- Разработка рекомендаций по доработке нормативных и методических документов

Технический эксперт

- Экспертная поддержка в соответствии со специализацией (ВПО, настройка средств защиты, применение специализированных технических средств, оценка защищенности и т.п.)
- Формирование предложений по повышению уровня защищенности

Специалист

- Нормативно-правовое и методическое сопровождение деятельности центра ГосСОПКА

Руководитель

- Управление деятельностью центра ГосСОПКА
- Взаимодействие с НКЦКИ

ДОКУМЕНТЫ, НЕОБХОДИМЫЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ДЕЯТЕЛЬНОСТИ

ГОССОПКА

Положение о Центре ГосСОПКА

Регламент деятельности центра ГосСОПКА

Штатное расписание центра ГосСОПКА

Лицензии

Соглашение о взаимодействии с ФСБ России

НКЦКИ СОБИРАЕТ

ГОССОПКА

Сведения об атаках и инцидентах

Сведения об объектах

Сведения о программном обеспечении

Сведения об угрозах

НКЦКИ ПРЕДОСТАВЛЯЕТ

Сведения о признаках компьютерных инцидентов

Сведения об уязвимостях ПО

Сведения об угрозах безопасности

Индикаторы вредоносной активности

ВАРИАНТЫ ПОДКЛЮЧЕНИЯ К ТЕХНИЧЕСКОЙ ИНФРАСТРУКТУРЕ НКЦКИ

ГОССОПКА

1 вариант

Иметь лицензию на ПО ViPNet Client с классом защиты КС3 в существующую сеть ViPNet с номером 10976

Установить ПО ViPNet Client

Направить запрос на email: gov-cert@gov-cert.ru в котором указать необходимую информацию для подготовки файла с настройками

ВАРИАНТЫ ПОДКЛЮЧЕНИЯ К ТЕХНИЧЕСКОЙ ИНФРАСТРУКТУРЕ НКЦКИ

ГОССОПКА

2 вариант

Иметь лицензию на ПО или ПАК ViPNet Coordinator с классом защиты КС3 в существующую сеть ViPNet с номером 10976

Установить ViPNet Coordinator

Направить запрос на email: gov-cert@gov-cert.ru и rea@gov-cert.ru, в котором указать необходимую информацию для подготовки файла с настройками для ViPNet Coordinator

При такой схеме подключения возможно будет организовать взаимодействие с использованием средств автоматизации (API)

ВАРИАНТЫ ПОДКЛЮЧЕНИЯ К ТЕХНИЧЕСКОЙ ИНФРАСТРУКТУРЕ НКЦКИ

ГОССОПКА

3 вариант

Посредством использования уже действующей (собственной) сети ViPNet

Направить запрос на email: gov-cert@gov-cert.ru и rea@gov-cert.ru, в котором указать необходимую информацию для подготовки файла с межсетевой информацией

Доступ к странице авторизации личного кабинета осуществляется по адресу: https://portal.cert.local

КОНТАКТЫ ДЛЯ ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ

ГОССОПКА

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

gov-cert@gov-cert.ru

+7 (916) 901-07-42

ГОССОПКА

Благодарю за внимание!