

Практическое значение нормативно-правовых актов для отрасли информационной безопасности



Проверка связи





Если у вас нет звука:

- убедитесь, что на вашем устройстве и на колонках включён звук
- обновите страницу вебинара (или закройте страницу и заново присоединитесь к вебинару)
- откройте вебинар в другом браузере
- перезагрузите компьютер (ноутбук) и заново попытайтесь зайти



Поставьте в чат:

-  если меня видно и слышно
-  если нет

Оксана Докучаева

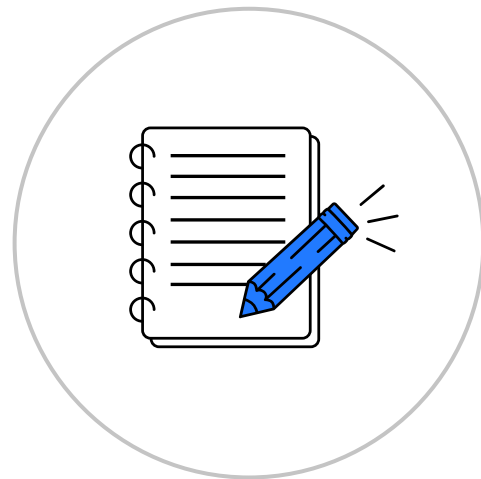
О спикере:

- 13 лет оперативного опыта в Центре информационной безопасности ФСБ России
- Автор публикаций по информационной безопасности и расследованию компьютерных преступлений
- Опыт взаимодействия с Советом Безопасности РФ, правоохранительными органами, спецслужбами, организациями РФ и иностранных государств по вопросам обеспечения информационной безопасности



Правила участия

- 1 Приготовьте блокнот и ручку, чтобы записывать важные мысли и идеи
- 2 Продолжительность вебинара — 80 минут
- 3 Вы можете писать свои вопросы в чате
- 4 Запись вебинара будет доступна в LMS



Вспомним содержание лекции по теме

- 1 Узнали, что такое информационное право: систему, структуру, отдельные элементы
- 2 Дали характеристику информационным правоотношениям и их структуре
- 3 Разобрали, какие документы в области ИБ являются стратегическими, а какие ключевыми
- 4 Рассмотрели особенности применения федеральных нормативно-правовых актов для обеспечения ИБ в РФ

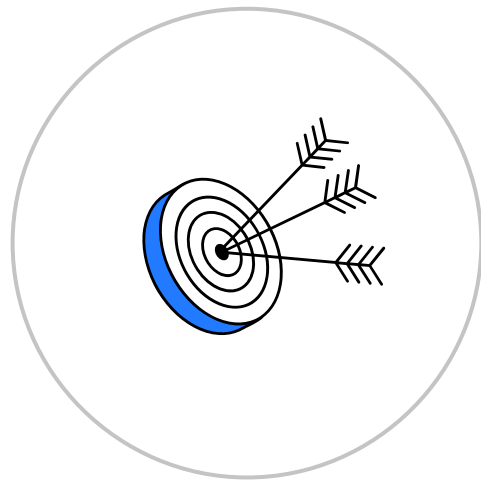




Ваши вопросы?

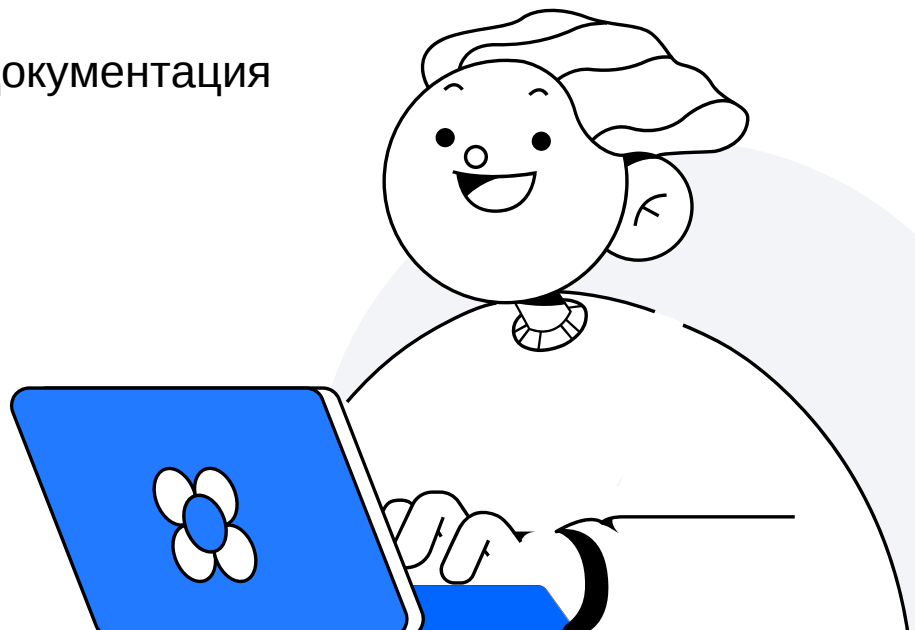
Цели занятия

- Узнать, что такое организационно-распорядительная документация в организации по вопросам ИБ
- Рассмотреть организационно-распорядительные документы для государственных информационных систем
- Рассмотреть организационно-распорядительные документы для критической информационной инфраструктуры



План занятия

- 1 Организационно-распорядительная документация в организации. Общие сведения
- 2 Организационно-распорядительная документация в организации. ГИС
- 3 Организационно-распорядительная документация в организации. КИИ
- 4 Итоги



Организационно-распорядительная документация

Общие сведения



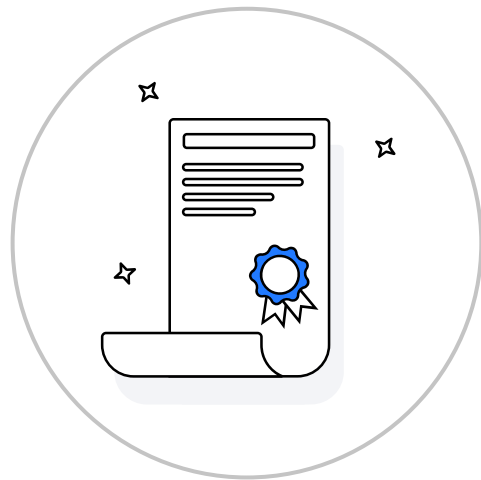
1

Что такое организационно-распорядительная документация (ОРД)

Важная часть системы обеспечения информационной безопасности организации.

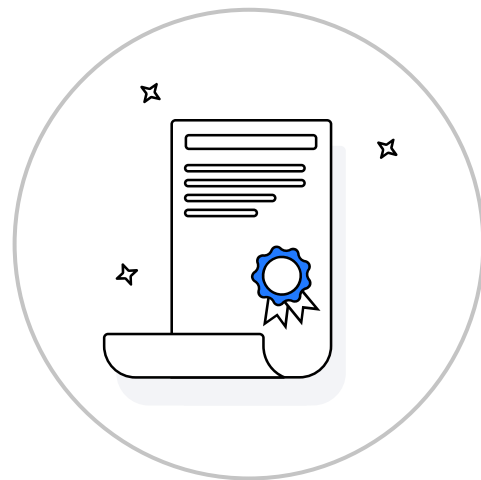
Единого перечня организационно-распорядительной документации (ОРД) в законодательстве нет.

Существует ряд нормативных документов, описывающих отдельные требования по защите конкретных видов информационных систем, отраслевые стандарты и др.



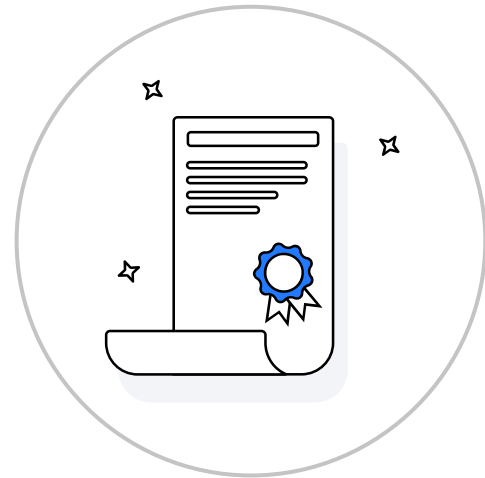
Нормативно-правовые акты, выдвигающие требования к ОРД

- Федеральный закон №152-ФЗ
- Федеральный закон №98-ФЗ
- Федеральный закон №149-ФЗ
- Федеральный закон №395-1
- Приказ ФСБ РФ №416, ФСТЭК РФ №489
- Федеральный закон №187-ФЗ
- Приказ Мининформсвязи РФ от 09.01.2008 №1
- Приказ ФСТЭК России №17
- Методический документ ФСТЭК России от 14.02.2014
«Меры защиты информации в государственных информационных системах»
- Методический документ. Методика оценки угроз безопасности информации
(утв. ФСТЭК России 05.02.2021 г.)



Общий перечень ОРД

- Приказ о назначении ответственных лиц
- Приказ о назначении группы реагирования на инциденты информационной безопасности (ГРИИБ)
- Приказ о контролируемой зоне и положение о контролируемой зоне
- Политика информационной безопасности
- План мероприятий по обеспечению безопасности
- Инструкции ответственных лиц, пользователей, администраторов и пр.
- Журналы и инструкции по их заполнению





**Встречались ли вы
с такими документами
в профессиональной
деятельности?**

Приказ о назначении ответственных лиц

Приказом назначаются: ответственный за организацию обработки персональных данных и администратор безопасности.

Основания: ст. 18.1 ФЗ «О персональных данных» и п. 9 Приказа ФСТЭК №17.

Чтобы обеспечить защиту информации, содержащейся в информационной системе, оператор назначает структурное подразделение или должностное лицо (работника), ответственное за защиту информации.

Во исполнение приказа принимают инструкции для указанных работников

Приказ о назначении группы реагирования на инциденты информационной безопасности

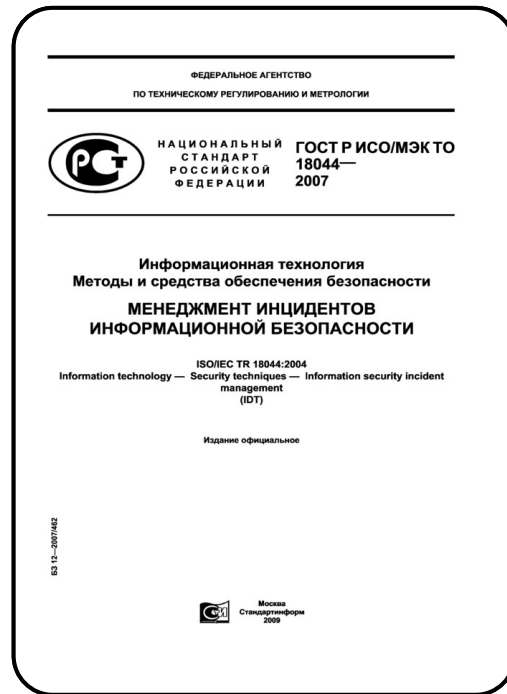
Сокращение (ГРИИБ) введено ГОСТ Р ИСО/МЭК ТО 18044-2007.

Необходимость документа обусловлена ст. 19 закона «О персональных данных», Приказом ФСТЭК №17.

Приказ должен определить лиц, ответственных за выявление инцидентов и реагирование на них.

Реагирование включает:

- обнаружение и идентификацию инцидентов и событий, приводящих к возникновению инцидентов
- своевременное информирование ответственных лиц
- анализ инцидентов
- планирование и принятие мер по устранению инцидентов, предотвращению повторного возникновения инцидентов



[Источник](#)

Приказ о контролируемой зоне и положение о контролируемой зоне

Необходимость этих документов обусловлена требованием ФСТЭК ЗТС.2.

Границы контролируемой зоны устанавливаются в организационно-распорядительных документах по защите информации.

Контролируемая зона — это территория, на которой исключается несанкционированный доступ к элементам информационной системы посторонними лицами.

Для одной информационной системы (её сегментов) может быть организовано несколько контролируемых зон.

Требования ЗТС 2 предъявляют к информационным системам всех классов защищенности



ФСТЭК России
Федеральная служба
по техническому и
экспортному контролю

[Источник](#)

Политика информационной безопасности

Как правило, содержит следующие разделы:

- Общие положения
- Нормативно-правовое обеспечение
- Область применения
- Термины и определения
- Требования в отношении работников
- Требования по защите материалов, содержащих конфиденциальную информацию
- Требования по управлению доступом и регистрацией
- Требования к парольной защите
- Требования к этапам жизненного цикла информационных систем
- Требования к управлению инцидентами информационной безопасности
- Требования к мерам обеспечения непрерывности деятельности
- Требования по обеспечению соответствия законодательству
- Аудит информационной безопасности
- Ответственность

План мероприятий по обеспечению безопасности

Состоит из двух частей:

- список разовых мероприятий
- список периодических мероприятий

План разовых мероприятий содержит мероприятия, которые необходимо осуществить в какой-либо момент времени.

План периодических мероприятий соответствует выполнению требований по постоянному внутреннему контролю информационной безопасности в соответствии с законодательством



План мероприятий по обеспечению безопасности

2 части:

- список разовых мероприятий
- список периодических мероприятий

План разовых мероприятий - мероприятия, которые необходимо осуществить в какой-либо момент времени.

План периодических мероприятий - выполнение требований законодательства по постоянному внутреннему контролю информационной безопасности



Инструкции

Документы, создающиеся во исполнение верхнеуровневых документов и содержащие конкретные перечни действий.

Виды:

- для работников о работе с конфиденциальной информацией
- по безопасной работе в интернете
- для пользователя по обеспечению информационной безопасности на рабочем месте
- по использованию информационных сетевых ресурсов совместного пользования
- по использованию технологий удалённого доступа
- по использованию электронной почты
- по управлению доступом и регистрацией



Журналы

Нужны для ведения различных учётов

В соответствии с требованиями ФСТЭК и ФСБ должны быть журналы учёта носителей информации, причём разные для разных типов носителей.

Также требуются журналы по проведению инструктажей, плановых мероприятий и др.

Правильное ведение журналов позволяет избежать сложностей при проверках регуляторами.

Желательно наличие инструкций по заполнению журналов

(наименование подразделения организации, в ИТ О. индивидуального подразделения,
имеющих лицензию на медицинскую деятельность)

ЖУРНАЛ
УЧЕТА НОСИТЕЛЕЙ ИНФОРМАЦИИ, СОДЕРЖАЩИХ
ПЕРСОНАЛЬНЫЕ ДАННЫЕ

(наименование организации, подразделения)

Начат «__» _____ 20__ г.
Окончен «__» _____ 20__ г.

Ответственный за заполнение _____ Ф.И.О.

Журналы

Нужны для ведения различного учёта.

Журналы учета носителей информации (разные для разных типов носителей) - требование ФСТЭК и ФСБ

Журналы по проведению инструктажей, плановых мероприятий и др.

Правильное ведение журналов позволяет избежать сложностей при проверках регуляторами.

Желательно наличие инструкций по заполнению журналов

(наименование подразделения организации, в И.О. индивидуального подразделения, имеющих лицензию на медицинскую деятельность)

ЖУРНАЛ
УЧЕТА НОСИТЕЛЕЙ ИНФОРМАЦИИ, СОДЕРЖАЩИХ
ПЕРСОНАЛЬНЫЕ ДАННЫЕ

(наименование организации, подразделения)

Начат «__» _____ 20__ г.
Окончен «__» _____ 20__ г.

Ответственный за заполнение _____ Ф.И.О.



**Как вы думаете, без каких
документов в
профессиональной
деятельности можно обойтись?**

Выводы

- 1 В соответствии с НПА в организации должен быть сформирован комплект организационно-распорядительной документации
- 2 В ряде случаев законодательство содержит прямые указания на создание документов
- 3 Отсутствие документов может повлечь санкции со стороны регуляторов





Ваши вопросы?

Организационно-распорядительная документация

Государственная информационная система



2

Подумайте

Вопрос: что такое государственная информационная система?



Подумайте

Вопрос: что такое государственная информационная система?

Ответ: федеральная или региональная информационная система, созданная на основании федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов



Подумайте

Вопрос: какая государственная информационная система самая известная в России?



Подумайте

Вопрос: какая государственная информационная система самая известная в России?

Ответ: Единый портал государственных и муниципальных услуг (ЕПГУ)



НПА, выдвигающие требования к ОРД

- Федеральный закон №149-ФЗ
- Постановление правительства №676
- Приказ ФСТЭК России от №17



Перечень документов. Обеспечение безопасности ГИС

- Приказ необходимости защиты информации
- Приказ о классификации и акт классификации ГИС
- Приказ о вводе в действие ГИС



Приказ необходимости защиты информации

Приказ необходимости защиты информации основывается на требованиях Приказа ФСТЭК №17:

«Принятие решения о необходимости защиты информации, содержащейся в информационной системе».

В приказе отражают:

- необходимость защиты информации
- цели и задачи информационной системы
- цели и задачи защиты информации в системе
- функции ответственных лиц
- этапы создания системы защиты информации



Приказ о классификации ИС и акт классификации

Приказом назначается комиссия по классификации.

Актом комиссия фиксирует параметры информационной системы и присваивает класс защищённости.

В случае обработки в ГИС персональных данных в акте необходимо определить их уровень защищённости



Приказ о вводе в действие

В соответствии с приказом ФСТЭК №17 государственная информационная система может быть введена в действие только на основании аттестата соответствия требованиям по безопасности информации.

Приказ содержит:

- цель создания информационной системы
- сведения об аттестате соответствия
- сведения об организации контроля соответствия системы защиты информации



Выводы

- 1 Для ГИС существует специфичный перечень необходимых документов
- 2 Наличие приказа о необходимости защиты информации, приказа о классификации и акта классификации, приказа о вводе в действие строго обязательно





Ваши вопросы?

Перерыв

5 минут



Организационно-распорядительная документация

Критическая информационная инфраструктура



3

Критическая информационная инфраструктура (КИИ)

- 1 Информационные системы, информационно-телекоммуникационные сети
- 2 Автоматизированные системы управления
- 3 Сети электросвязи, используемые для организации их взаимодействия в следующих сферах:
здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности



[Источник](#)



**Приведите примеры
субъектов КИИ**

НПА, выдвигающие требования к ОРД в сфере критической информационной инфраструктуры

- Федеральный закон №187-ФЗ
- Постановление Правительства №162
- Постановление Правительства №127
- Приказ ФСТЭК России №235
- Приказ ФСТЭК России №239
- Приказ ФСБ России №367
- Приказ ФСБ России №368
- Приказ ФСБ России №281
- Приказ ФСБ России №282
- Приказ ФСБ России №196
- Указ Президента России № 250
- Постановление Правительства РФ от 15 июля 2022 г. N 1272



[Источник](#)

Перечень документов.



Обеспечение безопасности КИИ

- Политика информационной безопасности значимых объектов КИИ
- Положение о системе безопасности значимых объектов КИИ
- Положение о постоянно действующей комиссии по категорированию объектов КИИ
- Положение о структурном подразделении, ответственном за обеспечение безопасности объектов КИИ
- Положение о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации)
- Положение о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)
- Положение о комиссии для проведения контроля состояния защищённости значимых объектов КИИ
- План мероприятий по обеспечению информационной безопасности значимых объектов критической информационной инфраструктуры
- План реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак
- Порядок взаимодействия субъекта с ГосСОПКА РФ
- Модель нарушителя и угроз

Политика информационной безопасности значимых объектов КИИ

Включает:

- цели и задачи обеспечения безопасности
- объекты защиты
- основные угрозы безопасности информации и категории нарушителей
- риски и возможные негативные последствия
- подходы к способам обеспечения безопасности информации и объектов КИИ, выбору средств защиты информации
- ответственность за соблюдение и нарушение требований и правил обеспечения безопасности

 
МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 50.524
от 25 декабря 2017 г.

**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)**


П Р И К А З

«25» декабря 2017 г. Москва № 239

**Об утверждении Требований
по обеспечению безопасности значимых объектов критической
информационной инфраструктуры Российской Федерации**

В соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) **П Р И К А З Ы В А Ю:**
Утвердить прилагаемые Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

**ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ**

 **В.СЕЛИН**

[Источник](#)

Положение о системе безопасности значимых объектов КИИ

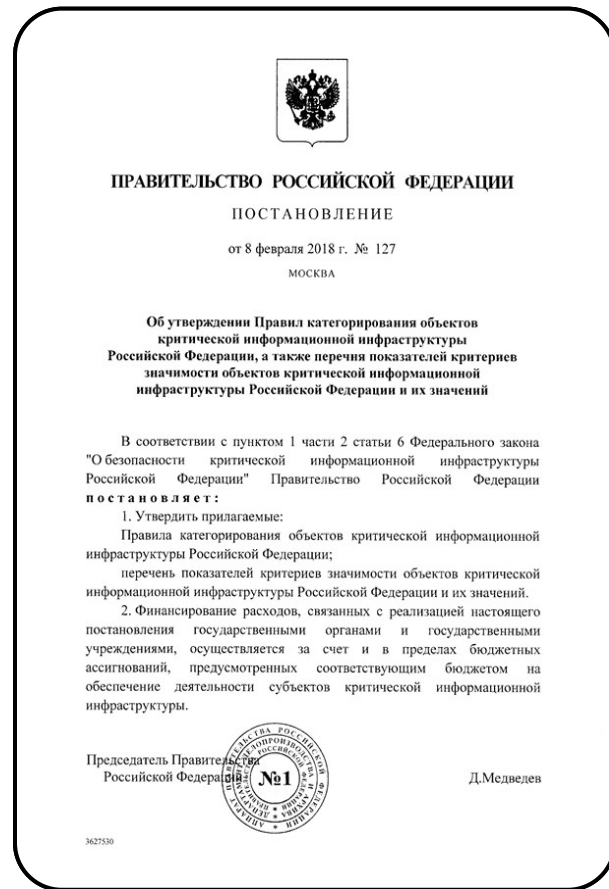
Включает:

- организацию разработки, утверждения и внесения изменений в план мероприятий по обеспечению безопасности значимых объектов КИИ, а также контроля его исполнения и документирования результатов
- организацию реализации мероприятий по обеспечению безопасности значимых объектов КИИ
- управление, обеспечение эксплуатации и контроль функционирования средств защиты информации (СЗИ)
- управление и контроль изменений конфигураций
- контроль физического доступа к объектам КИИ
- анализ угроз и уязвимостей
- мониторинг и контроль состояния безопасности значимых объектов КИИ
- обеспечение безопасности объектов КИИ при возникновении нештатных ситуаций
- совершенствование безопасности значимых объектов КИИ
- информирование, обучение, тренировки и контроль осведомлённости персонала
- сопровождение функционирования системы безопасности, ведения документации
- проведение испытаний, приёмки и оценки соответствия СЗИ требованиям по безопасности

Положение о постоянно действующей комиссии по категорированию объектов КИИ

Издается на основании п. 11 правил, утверждённых Постановлением Правительства РФ №127 и содержит:

- цели и задачи деятельности комиссии
- состав
- структуру
- режим работы
- права и зоны ответственности
- уровни подчинённости
- вопросы взаимодействия с другими подразделениями субъекта КИИ и внешними организациями



[Источник](#)

Положение о структурном подразделении, ответственном за обеспечение безопасности объектов КИИ

содержит 10 требований, утверждённых приказом ФСТЭК №235.

Содержит:

- цели и задачи
- состав и структуру подразделения
- права и зоны ответственности
- уровни подчинённости
- вопросы взаимодействия с другими подразделениями субъекта КИИ и внешними организациями



Положение о заместителе руководителя, ответственного за обеспечение информационной безопасности органа (организации)

Создаётся в соответствии с пп. “а” п. 1 Указа Президента № 250

Содержит:

- полномочия, права и обязанности заместителя руководителя
- квалификационные требования к ответственному лицу
- трудовые (должностные) обязанности ответственного лица
- ответственность ответственного лица

Положение о структурном подразделении, обеспечивающем информационную безопасность органа (организации)

Создаётся в соответствии с пп. “б” п. 1 Указа Президента № 250

Содержит:

- цели, задачи и функции подразделения
- права и зоны ответственности
- взаимоотношения и связи подразделения
- показатели эффективности и результативности подразделения

Положение о комиссии для проведения контроля состояния защищённости значимых объектов КИИ

Положение о комиссии по контролю состояния защищённости значимых объектов КИИ содержит:

- описание состава и структуры комиссии
- порядок и периодичность проведения контроля
- критерии оценки эффективности организации работ по обеспечению безопасности значимых объектов КИИ
- требования к документированию результатов осуществления внутреннего контроля

→ Комиссия может не создаваться, если субъект КИИ принял решение провести внешнюю оценку (аудит)

План мероприятий по обеспечению информационной безопасности значимых объектов КИИ

Основывается на п. 25-б, п. 29, п. 30 требований приказа ФСТЭК №235, п. 13.1-б–13.1-в требований приказа ФСТЭК №239 и содержит:

- перечень мероприятий
- обоснование необходимости проведения
- сроки
- ответственных за проведение
- контроль выполнения

План реагирования на компьютерные инциденты и принятия мер по ликвидации последствий КА

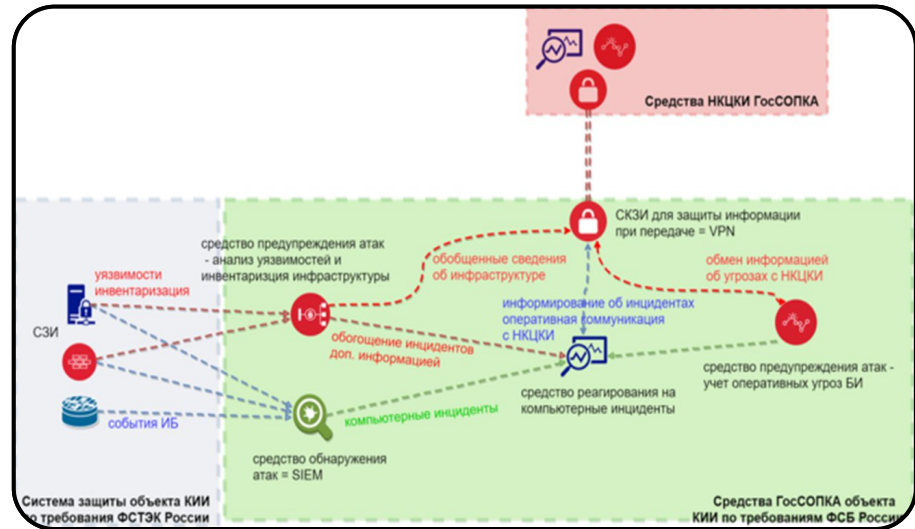
План содержит:

- состав значимых объектов КИИ и их характеристики
- состав подразделений и лиц, ответственных за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак
- их задачи и зоны ответственности
- условия (события) начала и порядка реагирования на компьютерные инциденты, включая регламентное время реагирования
- порядок восстановления функционирования значимых объектов КИИ, включая регламентное время восстановления
- объём, содержание и периодичность проведения тренировок по отработке мероприятий

Порядок взаимодействия с ГосСОПКА

Порядок взаимодействия с ГосСОПКА основывается на п. 25-б требований приказа ФСТЭК №235, п. 2–5 требований приказа №282, приказе ФСБ №368 и содержит:

- порядок информирования о компьютерных инцидентах
- порядок обмена информацией о компьютерных инцидентах
- порядок информирования о результатах мероприятий по реагированию на компьютерные инциденты

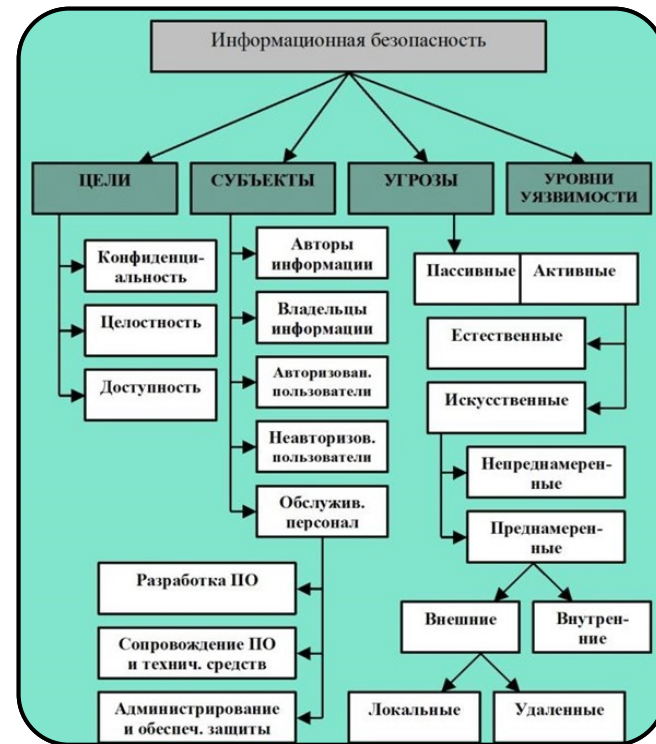


Модель нарушителя и угроз

Модель угроз и нарушителя безопасности информации значимых объектов КИИ основывается на п. 25-б требований приказа ФСТЭК №235, п. 11, п. 11.1 требований приказа ФСТЭК №239 и разрабатывается в соответствии с методическими документами ФСТЭК.

Модель включает:

- краткое описание объектов КИИ
- источники угроз
- уязвимости
- возможные способы реализации угроз
- возможные последствия от реализации угроз





**Как необходимость разработки
этой документация отражается
на деятельность организации?**

Выводы

- 1 Основанные НПА, регулирующие вопросы документации для КИИ — приказы ФСТЭК и ФСБ
- 2 Количество документов значительно
- 3 Наличие перечисленных документов строго обязательно
- 4 Отсутствие документов может повлечь юридическую ответственность





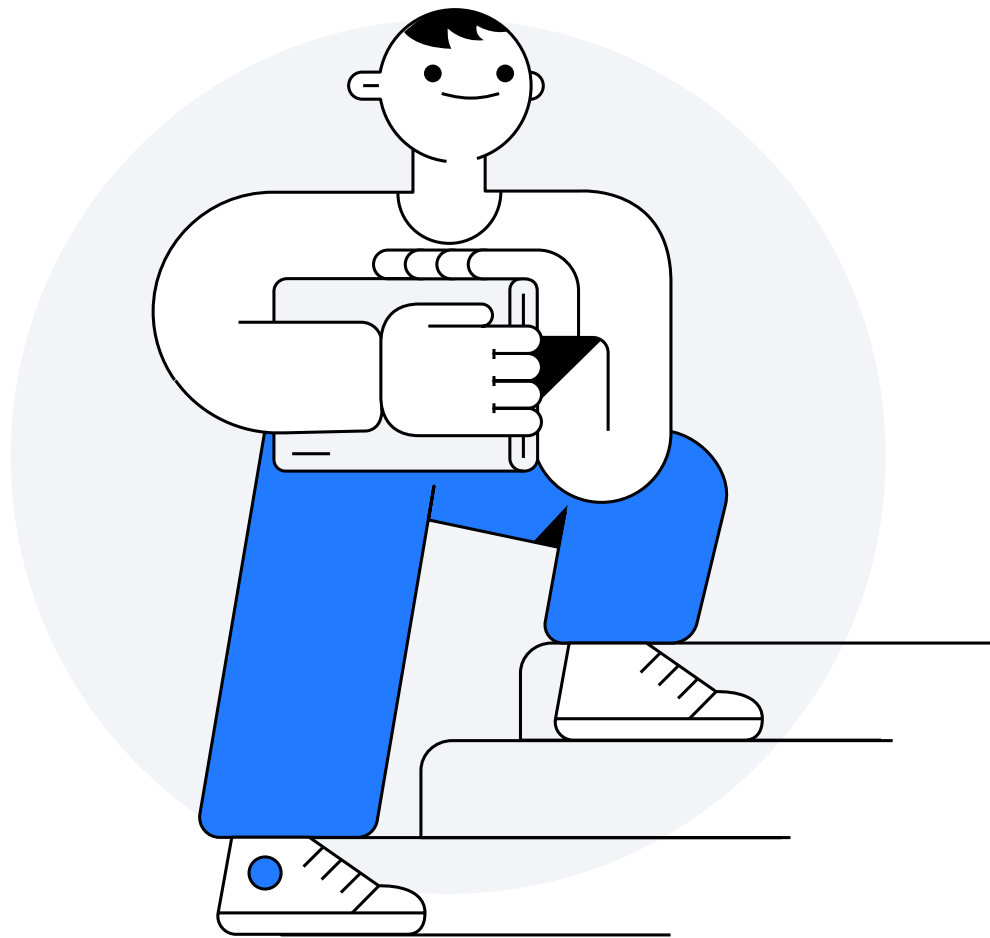
Ваши вопросы?

Итоги

- 1 Узнали, что такое организационно-распорядительная документация в организации по вопросам ИБ
- 2 Рассмотрели организационно-распорядительные документы для государственных информационных систем
- 3 Рассмотрели организационно-распорядительные документы для критической информационной инфраструктуры



Домашнее задание



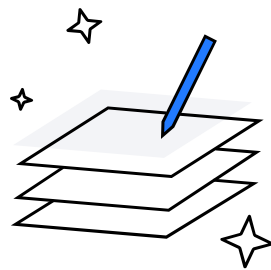
Домашнее задание

Цель: разработка локального организационно-распорядительного документа по вопросам ИБ

Формат выполнения: создание проекта документа в Google Doc

Форма проверки: проверяемое экспертом ДЗ

Результат: документ — краткая инструкция для пользователя по соблюдению правил информационной безопасности на рабочем месте



Дополнительные материалы

- [Шаблоны и примеры документов](https://wikisec.ru/) [https://wikisec.ru/]
- [Шаблоны типовых документов](https://securitypolicy.ru/) по информационной безопасности [SecurityPolicy.ru]



Практическое значение нормативно-правовых актов для отрасли информационной безопасности

