ПРАКТИКА РЕАЛИЗАЦИИ ТРЕБОВАНИЙ ФЕДЕРАЛЬНОГО ЗАКОНА №187-ФЗ «О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ»

Тарви Игорь

Ведущий архитектор систем безопасности Отдела консалтинга

АО «ДиалогНаука»

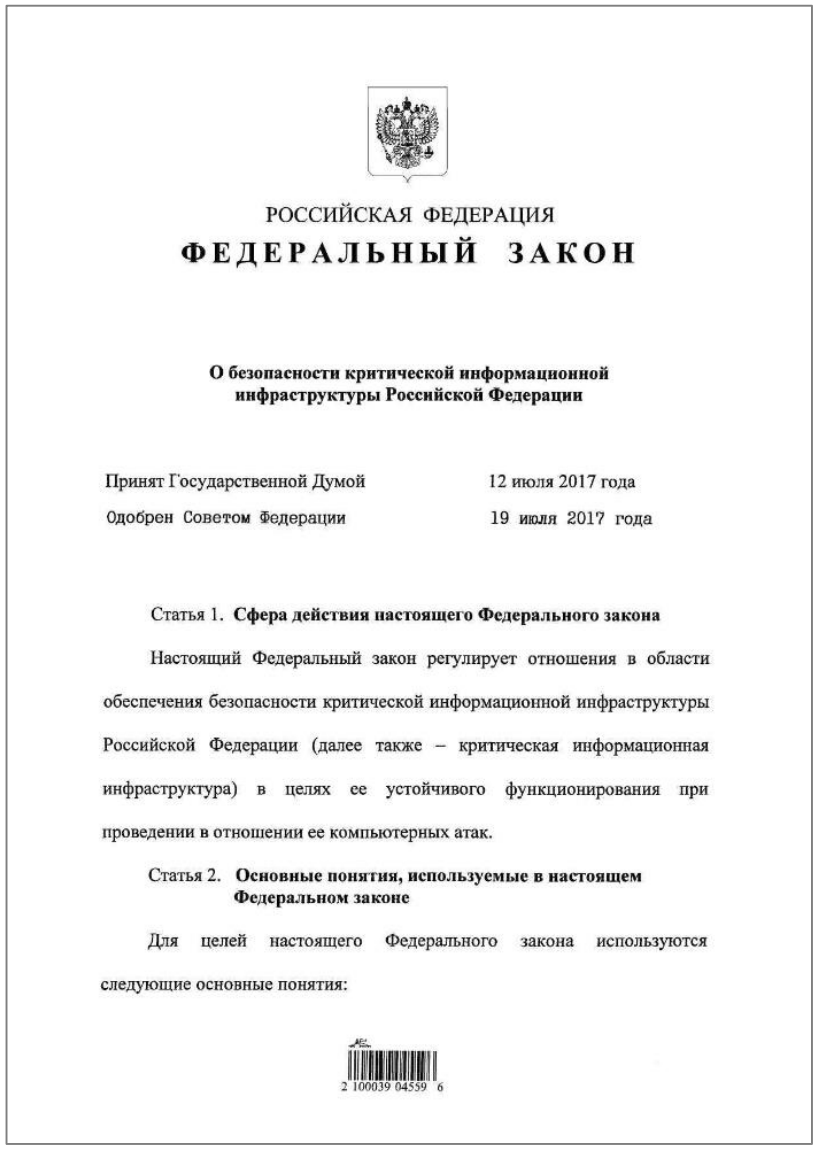
ДиалОгНаука

187-ФЗ «О безопасности КИИ РФ»

Регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры **Российской Федерации** в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак

Критическая информационная инфраструктура (КИИ) - объекты критической информационной инфраструктуры, **а также сети электросвязи, используемые для организации взаимодействия таких объектов**

К объектам КИИ могут относиться ИС/ИТС/АСУ



РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О безопасности критической информационной инфраструктуры Российской Федерации

Принят Государственной Думой 12 июля 2017 года

Одобрен Советом Федерации 19 июля 2017 года

Статья 1. **Сфера действия настоящего Федерального закона**

Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также – критическая информационная инфраструктура) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Статья 2. **Основные понятия, используемые в настоящем Федеральном законе**

Для целей настоящего Федерального закона используются следующие основные понятия:

На что стоит обратить внимание

149-ФЗ

- **ИС** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
- **ИТС** - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники

187-ФЗ

- **АСУ** - комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами

ГОСТ 34.003-90

- АСУ – подмножество АС, включающее в себя персонал
- В зависимости от вида управляемого объекта (процесса) АСУ делят, например, на **АСУ технологическими процессами (АСУТП), АСУ предприятиями (АСУП) и т.д.**

Сферы функционирования объектов КИИ

1. Здравоохранение;
2. Наука;
3. Транспорт;
4. Связь;
5. Энергетика;
6. Банковская сфера и иные сферы финансового рынка;
7. Топливно-энергетический комплекс;
8. Область атомной энергии;
9. Оборонная промышленность;
10. Ракетно-космическая промышленность;
11. Горнодобывающая промышленность;
12. Металлургическая промышленность;
13. Химическая промышленность.

На кого и на что распространяются требования

Надзорный орган

Федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры является **ФСТЭК России.**

Контактные телефоны представителей ФСТЭК России координирующих обеспечения безопасности объектов КИИ **в сферах:**

- оборонного комплекса, ракетно-космического комплекса, горнодобывающей и металлургической промышленности **8(495)605-33-84;**
- науки, связи, транспорта, здравоохранения, банковской сфере и иных сферах финансового рынка **8(499)252-49-68;**
- энергетического комплекса, атомной энергии, химической промышленности **8(499)252-51-01.**

А вы являетесь субъектом КИИ?

Сведения о том, может ли организация являться субъектом КИИ, можно получить в следующих источниках:

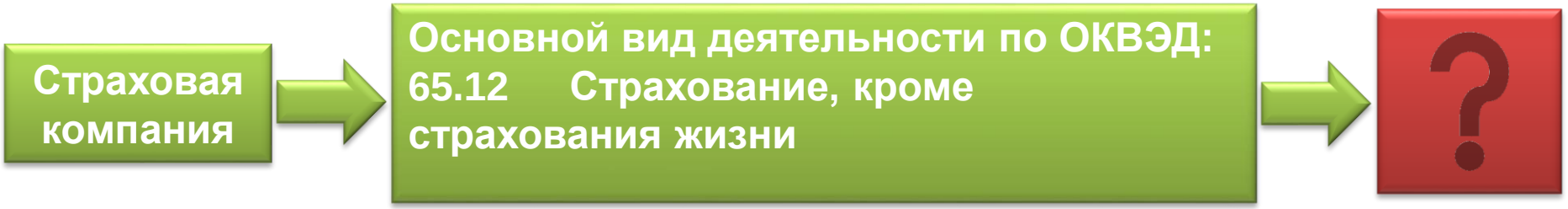
- Общероссийский классификатор видов экономической деятельности (ОКВЭД)

Телеком → **Основной вид деятельности по ОКВЭД: 61.10.1 Деятельность по предоставлению услуг телефонной связи**

- ✗ Здравоохранение
- ✗ Наука
- ✗ Транспорт
- ✓ Связь
- ✗ Энергетика
- ✗ Банковская сфера и иные сферы финансового рынка
- ✗ Топливно-энергетический комплекс
- ✗ Область атомной энергии
- ✗ Оборонная промышленность
- ✗ Ракетно-космическая промышленность
- ✗ Горно-добывающая промышленность
- ✗ Металлургическая промышленность
- ✗ Химическая промышленность

А вы являетесь субъектом КИИ?

- Лицензии и иные разрешительные документы на различные виды деятельности
- Уставы, положения организаций
- Другие источники



Наименование лицензирующего органа, выдавшего или переоформившего лицензии: - Центральный банк Российской Федерации

Федеральный закон «О Центральном банке Российской Федерации (Банке России)» от 10.07.2002 N 86-ФЗ Статья 76.1. Не кредитными финансовыми организациями признаются лица, осуществляющие следующие виды деятельности: … 9) деятельность субъектов страхового дела; …

Даже если субъект КИИ посчитал, что он не является субъектом КИИ и не должен проводить категорирование, ФСТЭК России обладает возможностью направить субъекту КИИ требование о необходимости соблюдения положений пункта 11 статьи 7 закона.

Обязанности субъектов КИИ

- **Первая задача -** категорирование ОКИИ
- **Вторая задача -** подготовить и направить в ФСТЭК России сведения о результатах категорирования ОКИИ
- **Третья задача -** привести систему защиты значимых ОКИИ в соответствие требованиям по обеспечению безопасности таких объектов

Срок подачи перечня ОКИИ в ФСТЭК России

Направить перечни объектов КИИ подлежащих категорированию необходимо было до 1го июня 2019 года!

Постановление
от 13 апреля 2019 г. № 452 «О внесении изменений в постановление Правительства от 8 февраля 2018 г. № 127»

Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Утвердить прилагаемые изменения, которые вносятся в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 "Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений" (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204).

2. Субъектам критической информационной инфраструктуры - государственным органам и государственным учреждениям утвердить до 1 сентября 2019 г. перечень объектов критической информационной инфраструктуры, подлежащих категорированию.

3. Рекомендовать субъектам критической информационной инфраструктуры - российским юридическим лицам и (или) индивидуальным предпринимателям утвердить до 1 сентября 2019 г. перечень объектов критической информационной инфраструктуры, подлежащих категорированию.

Председатель Правительства
Российской Федерации Д.Медведев

Категорирование объектов КИИ

Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127
(с изменениями от 13 апреля 2019 г.)

«Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»

Подготовлено в соответствии с пунктом 1 части 2 статьи 6 187-ФЗ

Утверждает:

1. Правила категорирования ОКИИ РФ
2. Перечень показателей критериев значимости ОКИИ РФ и их значения

ПП127 является подзаконным актом к 187-ФЗ, разъясняющим, как субъекту КИИ выполнить требования 187-ФЗ Статьи 7 «Категорирование объектов критической информационной инфраструктуры»

Методические рекомендации

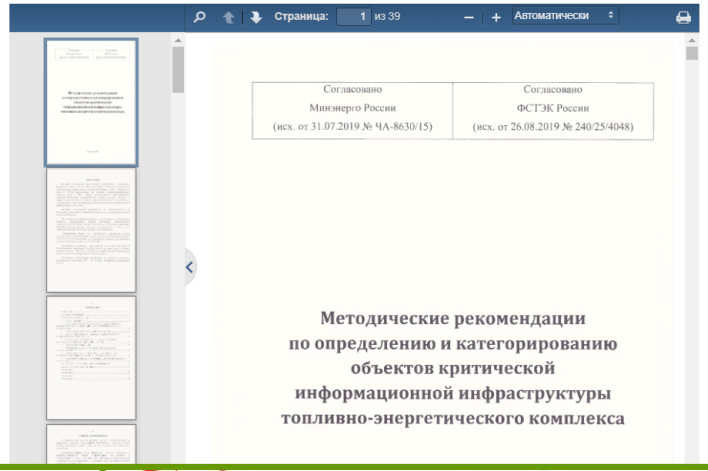
МИНИСТЕРСТВО ЭНЕРГЕТИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Новости и события · Противодействие коррупции · Общественный совет · Открытые данные · Общественная приемная

МИНИСТЕРСТВО ДЕЯТЕЛЬНОСТЬ ОТКРЫТОЕ МИНИСТЕРСТВО СТАТИСТИК

Главная › Методические рекомендации по определению и категорированию объектов критической информационной инфраструктуры топливно-энергетического комплекса.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОПРЕДЕЛЕНИЮ И КАТЕГОРИРОВАНИЮ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА.


Страница: 1 из 39 — Автоматически

Согласовано	Согласовано
Минэнерго России	ФСТЭК России
(исх. от 31.07.2019 № ЧА-8630/15)	(исх. от 26.08.2019 № 240/25/4048)

Методические рекомендации по определению и категорированию объектов критической информационной инфраструктуры топливно-энергетического комплекса

mos.ru Официальный сайт Мэра Москвы — Войти — Обратная связь

Новости Услуги Мэр Власть Карта Мой район β

Коронавирус: официальная информация · Какие лекции, выставки и экскурсии можно посетить не выходя из дома · Получить доступ к электронной медицинской карте · Где и когда появятся новые линии метро · Записаться онлайн на сдачу анализов в поликлинике

Департамент информационных технологий города Москвы

Главная · Деятельность · Руководство · Новости · Документы · Учреждения · Контакты

Документы

Методические рекомендации по определению объектов КИИ и категорий значимости объектов КИИ

Дата публикации: 23.05.2019

Методические рекомендации по определению объектов КИИ и категорий значимости объектов КИИ

[docx / 165.7Kb] Просмотреть файл

"УТВЕРЖДАЮ"
Начальник КГБУЗ ККМИАЦ
[redacted]
"30" ноября 2018 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по категорированию объектов критической информационной инфраструктуры в медицинских организациях Красноярского края

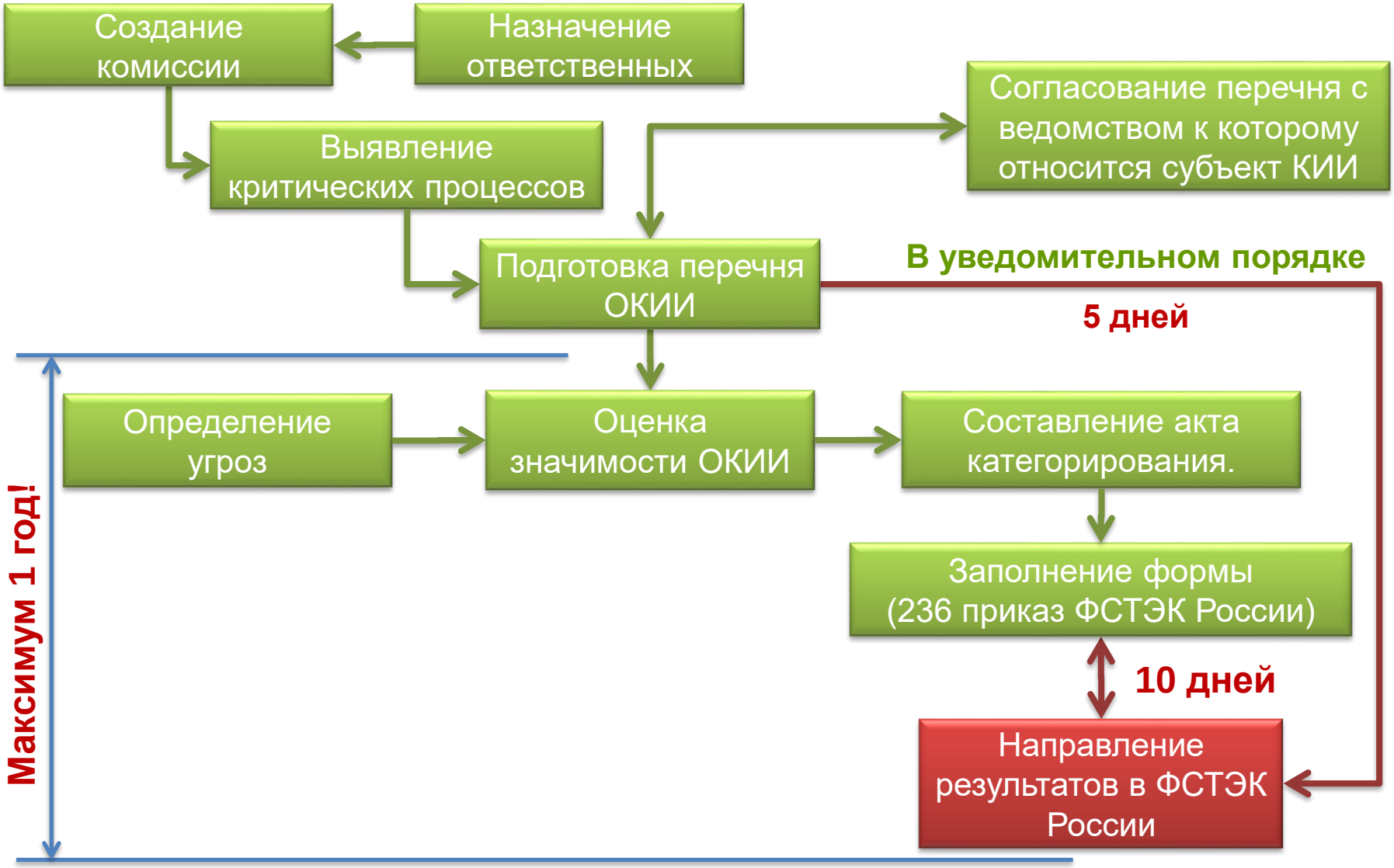
АССОЦИАЦИЯ ДОКУМЕНТАЛЬНОЙ ЭЛЕКТРОСВЯЗИ

АССОЦИАЦИЯ · ЧЛЕНСТВО В АДЭ · ДЕЯТЕЛЬНОСТЬ

Информация для членов АДЭ

Методические рекомендации по категорированию объектов критической информационной инфраструктуры, принадлежащих субъектам критической информационной инфраструктуры, функционирующим в сфере связи

Порядок категорирования



Назначение ответственных

Комиссия сама по себе в организации не появляется!

Кто-то должен:

- ✓ определить персональный состав Комиссии в Организации;
- ✓ разработать документы регламентирующие ее работу;
- ✓ обеспечить утверждение документов;
- ✓ спланировать деятельность Комиссии;
- ✓ подготовить материалы к заседаниям Комиссии.

Создание комиссии

Комиссия по категорированию назначается руководителем субъекта КИИ

Состав комиссии:

1. Руководитель субъекта
2. Работники являющиеся специалистами в области осуществляемых видов деятельности:
   - ✓ специалисты в области ИТ и связи;
   - ✓ специалисты по эксплуатации основного технологического оборудования;
   - ✓ специалисты по технологической (промышленной) безопасности
   - ✓ и т.д.
3. Специалисты по информационной безопасности
4. Работники подразделения по защите государственной тайны
5. Работники по ГО и ЧС

Комиссия может быть назначена отдельно в Филиалах и/или общая в Головном офисе

Определение критических процессов

Критические процессы для бизнеса?
Или
Критические для РФ?

187-ФЗ, статья 1. **Сфера действия настоящего Федерального закона**
Настоящий Федеральный закон регулирует отношения в области **обеспечения безопасности критической информационной инфраструктуры Российской Федерации** (далее также - критическая информационная инфраструктура) **в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.**

Подготовка перечня

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ от о 24 августа 2018 г. N 240/25/3752

По вопросам представления перечней ОКИИ, подлежащих категорированию

Приложение 1
к информационному сообщению
ФСТЭК России
от 24 августа 2018 г. № 240/25/3752

Рекомендуемая форма перечня объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

УТВЕРЖДАЮ

_____
Должность руководителя субъекта критической информационной инфраструктуры Российской Федерации (далее – субъект) или уполномоченного им лица

_____ _____
Подпись руководителя субъекта или уполномоченного им лица | Фамилия, имя, отчество (при наличии) руководителя субъекта или уполномоченного им лица

«____» _____ 20____ г.
Дата утверждения перечня объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

Перечень объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

№ п/п	Наименование объекта	Тип объекта[1]	Сфера (область) деятельности, в которой функционирует объект [2]	Планируемый срок категорирования объекта	Должность, фамилия, имя, отчество (при наличии) представителя, его телефон, адрес электронной почты (при наличии)[3]
1.					
2.					
…					
n.					

*прикладывать электронную копию в форматах docx, xlsx

Оценка значимости

Критерии значимости

1. Социальная
2. Политическая
3. Экономическая
4. Экологическая
5. Значимость для обеспечения обороны страны, безопасности государства и правопорядка

Показатели

14 показателей в 5ти критериях

Значение показателя

3и категории:

1. Первая (наивысшая)
2. Вторая
3. Третья
4. Нет категории

Присвоение категории значимости

Значимым объектом КИИ считается только тот, которому присвоена одна из трех категорий значимости и, только после внесения данных о нем в реестр значимых объектов КИИ.

Акт категорирования

РЕЗУЛЬТАТ РАБОТЫ КОМИССИИ

Акт должен содержать (в соответствии с п.16 ПП 127):

- ✓ сведения об объекте КИИ **(см. п.1 приказа 236 ФСТЭК России);**
- ✓ сведения о присвоенной объекту КИИ категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий **(см. п.8 приказа 236 ФСТЭК России);**

Акт подписывается членами комиссии по категорированию и утверждается руководителем субъекта КИИ.

Допускается **оформление единого акта** по результатам категорирования **нескольких объектов КИИ**, принадлежащих одному субъекту КИИ.

На что стоит обратить внимание

- Для проведения категорирования создается **постоянно** действующая комиссия по категорированию;
- **Филиалы могут создаваться отдельные комиссии** для категорирования объектов КИИ;
- Необходимо **согласовать перечень объектов КИИ с ведомством** к которому относится субъект КИИ;
- Должны рассматриваться **наихудшие сценарии атак** на объект КИИ;
- **Для создаваемых объектов КИИ** категория значимости определяется при формировании требований заказчиком, техническим заказчиком;
- Если объект КИИ по одному из показателей **отнесен к 1ой категории**, расчет **по остальным показателям может не проводиться;**
- Допускается **оформление единого акта** по результатам категорирования **нескольких объектов КИИ** одного субъекта;
- **После утверждения акта** необходимо **в течении 10 дней направить** в ФСТЭК России заполненную **форму по объектам КИИ**.

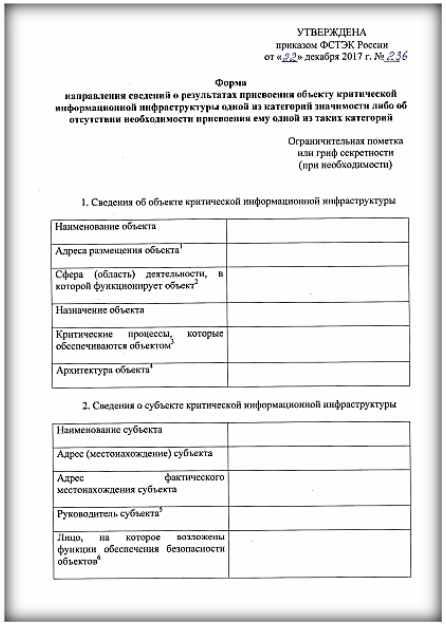
Направление сведений об объектах КИИ

Приказ ФСТЭК России
от 22 декабря 2017 г. № 236
(в ред. от 21 марта 2019 г.)

«Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»

Подготовлен в соответствии с пунктом 3 части 3 статьи 6 Федерального закона № 187-ФЗ

Определяет какие сведения и в какой форме направляются во ФСТЭК России по результатам категорирования ОКИИ



УТВЕРЖДЕНА
приказом ФСТЭК России
от «22» декабря 2017 г. № 236

Форма
направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

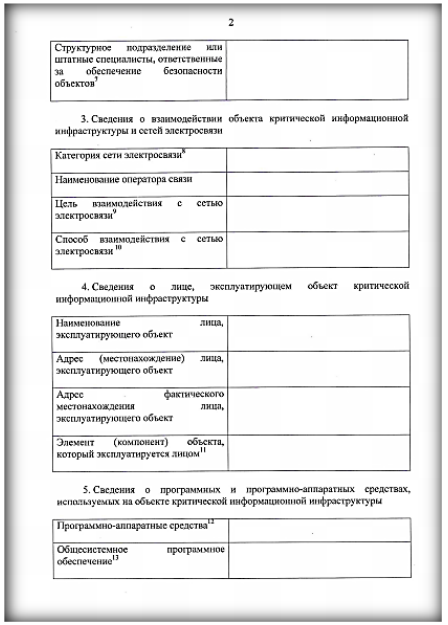
Ограничительная пометка
или гриф секретности
(при необходимости)

1. Сведения об объекте критической информационной инфраструктуры

Наименование объекта	
Адреса размещения объекта[1]	
Сфера (область) деятельности, в которой функционирует объект[2]	
Назначение объекта	
Критические процессы, которые обеспечиваются объектом[3]	
Архитектура объекта[4]	

2. Сведения о субъекте критической информационной инфраструктуры

Наименование субъекта	
Адрес (местонахождение) субъекта	
Адрес фактического местонахождения субъекта	
Руководитель субъекта[5]	
Лицо, на которое возложены функции обеспечения безопасности объектов[6]	



2

Структурное подразделение или штатные специалисты, ответственные за обеспечение безопасности объектов[7]	

3. Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи

Категория сети электросвязи[8]	
Наименование оператора связи	
Цель взаимодействия с сетью электросвязи[9]	
Способ взаимодействия с сетью электросвязи[10]	

4. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

Наименование лица, эксплуатирующего объект	
Адрес (местонахождение) лица, эксплуатирующего объект	
Адрес фактического местонахождения лица, эксплуатирующего объект	
Элемент (компонент) объекта, который эксплуатируется лицом[11]	

5. Сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры

Программно-аппаратные средства[12]	
Общесистемное программное обеспечение[13]	

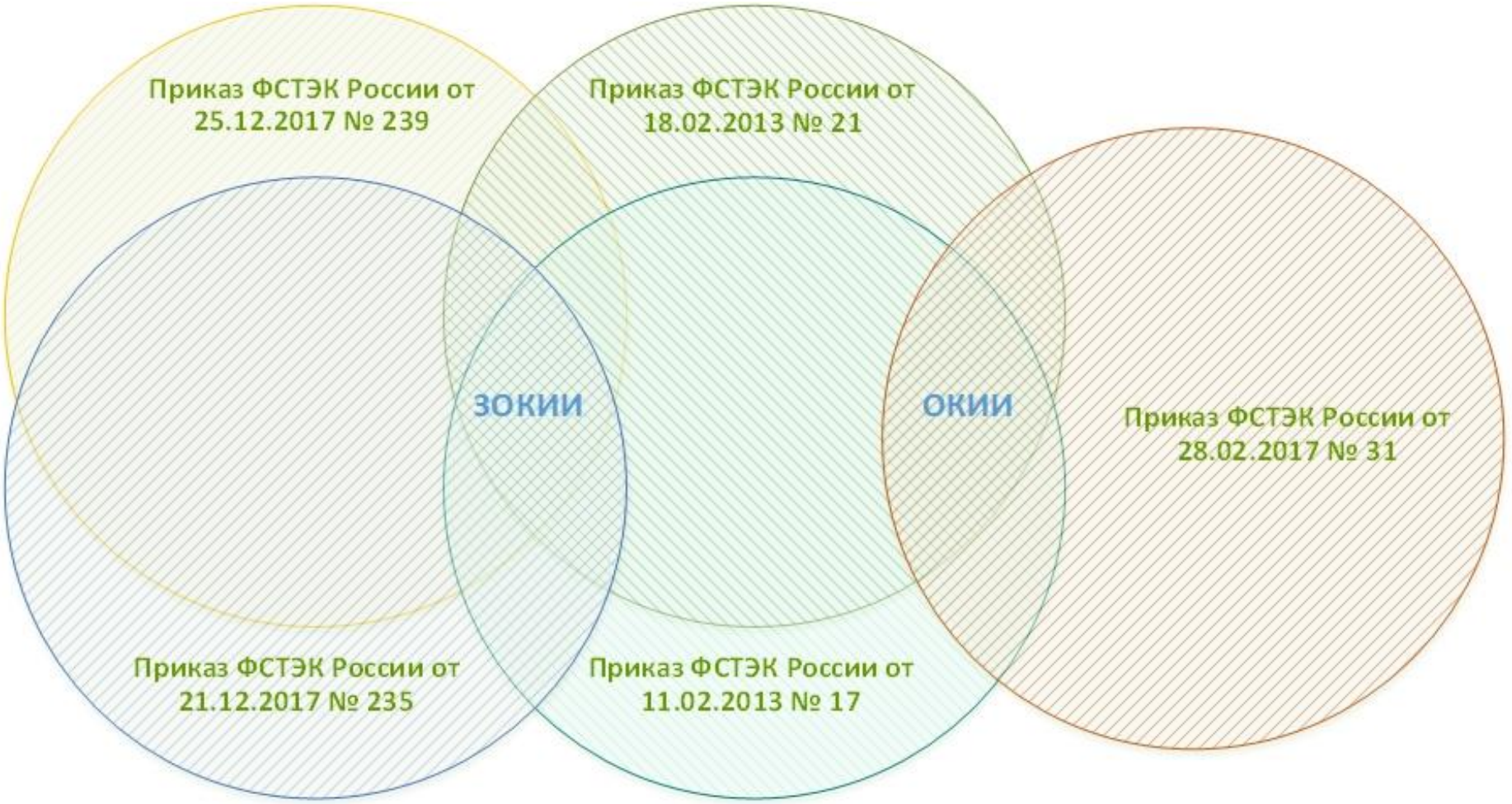
*Направляется в ФСТЭК России в течение 10 дней со дня утверждения акта

На что стоит обратить внимание

- Сведения о результатах направляются в ФСТЭК России в бумажном виде с приложением электронных копий в формате файлов электронных таблиц .ods;
- Данные об изменении категории также должны направляться в ФСТЭК России, в случае если:
  1. объект перестал соответствовать критериям значимости и показателям их значений;
  2. субъект КИИ был реорганизован, ликвидирован или произошли изменения в его организационно-правовой форме;
  3. по решению ФСТЭК России по результатам проверки;
  4. субъект КИИ не реже чем один раз в 5 лет осуществляет пересмотр категории значимости и сообщает об изменениях в ФСТЭК России.

Надзорная деятельность

Меры по обеспечению безопасности ОКИИ



Основные этапы создания системы безопасности

Основными этапами в ходе создания (модернизации) системы безопасности ЗОКИИ является:

1. Назначение ответственных
2. Установление требований к обеспечению безопасности ЗОКИИ
3. Разработка организационно-технических мер по обеспечению безопасности ЗОКИИ
4. Внедрение организационно-технических мер по обеспечению безопасности ЗОКИИ

Приказ №235

Приказ ФСТЭК России
от 21 декабря 2017 г. № 235

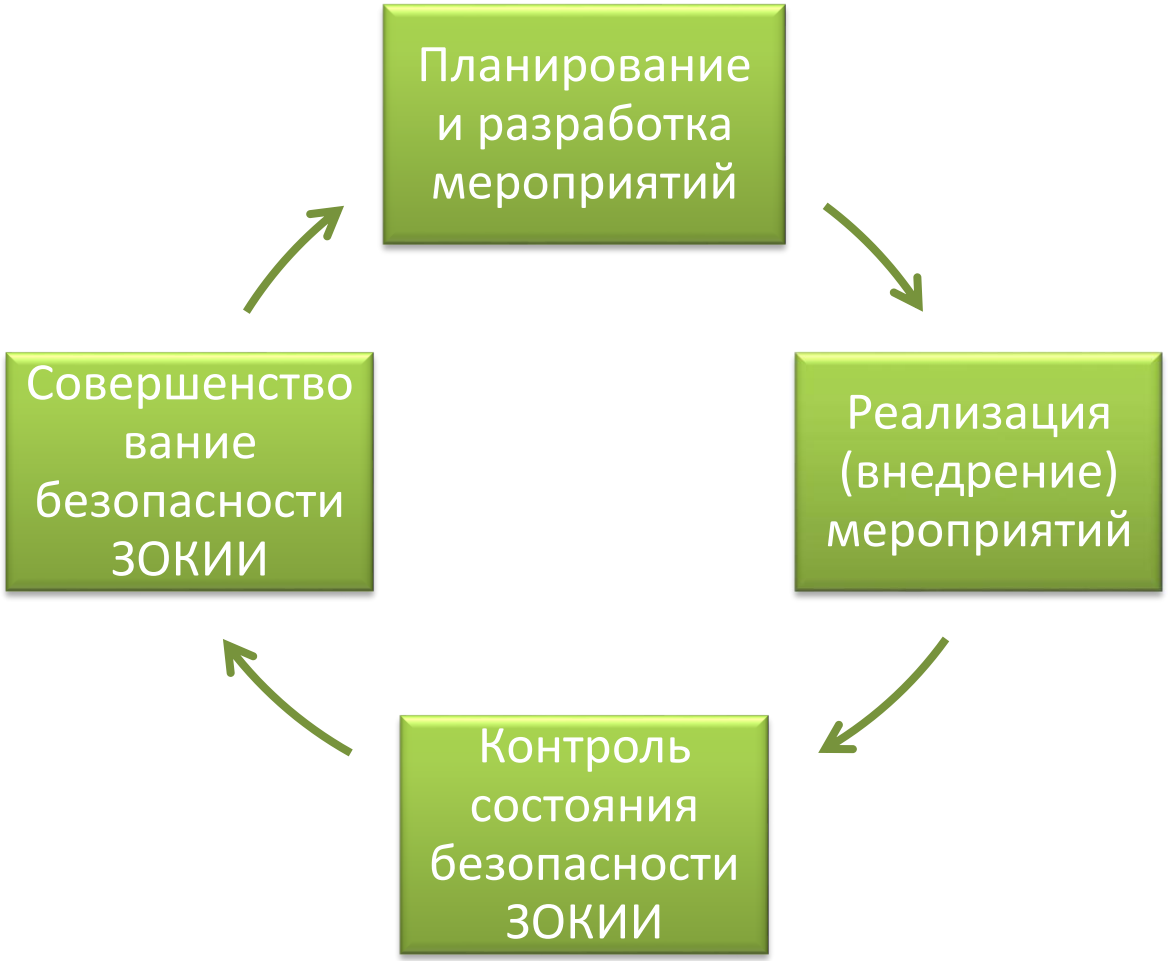
«Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»

Документ определяет требования к:

- силам и средствам обеспечения безопасности ЗОКИИ;
- организационно-распорядительной документации;
- функционированию системы безопасности в части организации работ по обеспечению безопасности ЗОКИИ

Функционирование системы безопасности

ФСТЭК России выделяет 4 этапа функционирования системы безопасности



Система безопасности может создаваться как для одного ЗОКИИ, так и их совокупности.

Назначение ответственных

Руководитель субъекта КИИ

(или уполномоченное лицо)

Определяет:

- ✓ структурное подразделение ответственное за безопасность ЗОКИИ;
- ✓ состав и структуру системы безопасности;
- ✓ функции ее участников.

Ответственные за обеспечение безопасности ЗОКИИ

Должны осуществлять следующие функции:

- ✓ разрабатывать предложения по совершенствованию ОРД;
- ✓ проводить анализ угроз
- ✓ обеспечивать реализацию требований к системе защиты;
- ✓ осуществлять реагирование на компьютерные инциденты;
- ✓ организовывать проведение оценки соответствия;
- ✓ готовить предложения по совершенствованию системы защиты

Ответственным за обеспечение безопасности ЗОКИИ должно быть отдельное подразделение (работники), совмещение ролей не допускается.

Изменения в приказ №235

С 1 января 2021 года устанавливаются дополнительные требования к стажу и образованию руководителей и штатных работников структурных подразделений по безопасности

Руководитель структурного подразделения по безопасности должен:

- ✓ иметь высшее профессиональное образование по направлению в области ИБ;
- ✓ или иное высшее профессиональное образование и пройти обучение по программам профессиональной переподготовки по направлению «Информационная безопасность» (со сроком обучения не менее 360 часов).
- ✓ иметь стаж работы в сфере ИБ не менее 3 лет.

Штатные работники структурного подразделения по безопасности должны:

- ✓ иметь высшее профессиональное образование по направлению в области ИБ
- ✓ или иное высшее профессиональное образование и пройти обучение по программам повышения квалификации по направлению «Информационная безопасность» (со сроком обучения не менее 72 часов).

Субъект КИИ должен организовывать **не реже 1 раза в 5 лет** обучение по программам повышения квалификации по направлению **«Информационная безопасность»** работников структурного подразделения по безопасности.

Приказ №239

Приказ ФСТЭК России
от 25 декабря 2017 г. № 239

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

Требования документа распространяются на все стадии жизненного цикла системы безопасности: создание, эксплуатация, вывод из эксплуатации.

Данные требования распространяются как на действующие ЗОКИИ, так и на создаваемые.

Разработка и внедрение технических мер

РАЗРАБОТКА:

1. Определение требований к системе защиты информации
2. Разработка организационно-распорядительной документации
3. Проектирование системы защиты
4. Разработка рабочей и эксплуатационной документации

ВНЕДРЕНИЕ:

1. Установка и настройка средств защиты
2. Предварительные испытания
3. Опытная эксплуатация
4. Приемочные испытания

Организационно-распорядительная документация

Политики, положения, приказы

Регламенты, инструкции

Документы планирования, порядок проведения испытаний, приемки, взаимодействия подразделений и т.д

Особенности моделирования угроз

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ от 4 мая 2018 г. N 240/22/2339

Для моделирования УБИ для ЗОКИИ **могут** применяться:

- Базовая модель угроз безопасности информации в КСИИ, утвержденная ФСТЭК России 18 мая 2007 г.
- Методика определения актуальных угроз безопасности информации в КСИИ, утвержденная ФСТЭК России 18 мая 2007 г.

Не официальная точка зрения ФСТЭК России:

- выше указанные документы рекомендуется использовать в случае если ЗОКИИ является **АСУ;**
- если ЗОКИИ является **ИСПДн,** то логично использовать базовую модель и методику для ПДн;
- если ЗОКИИ является **ГИС,** то методика для ГИС;
- допустимо применять адаптированные методики или полностью разработанные самостоятельно.

Отраслевые методики должны в обязательном порядке согласовываться с ФСТЭК России.

Допускается разрабатывать одну модель угроз для группы ЗОКИИ, имеющих одинаковые цели создания и архитектуру, а также типовые УБИ.

Установление требований

1. Определение базового набора мер в соответствии с категорией значимости ОКИИ
2. Адаптация базового набора мер защиты
3. Дополнение адаптированного набора мер защиты
4. Разработка технического задания

Состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости

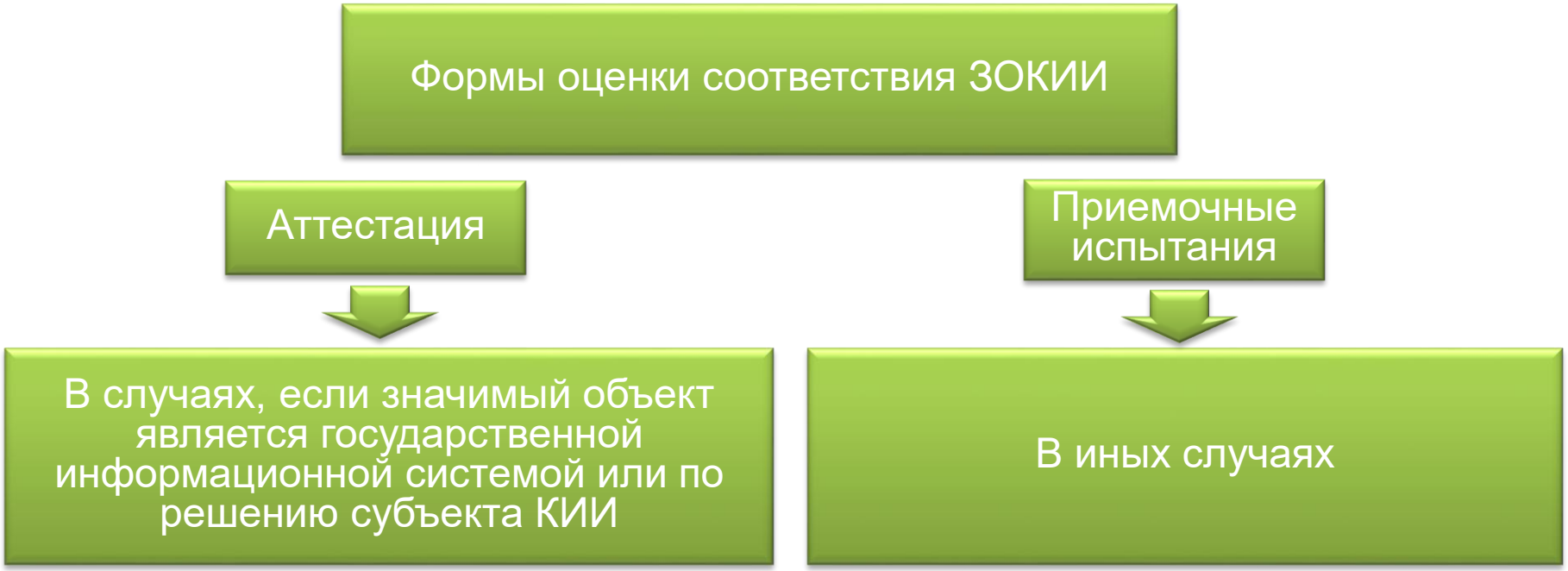
Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости		
		3	2	1
I. Идентификация и аутентификация (ИАФ)				
ИАФ.0	Разработка политики идентификации и аутентификации	+	+	+
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+	+	+
ИАФ.2	Идентификация и аутентификация устройств	+	+	+
ИАФ.3	Управление идентификаторами	+	+	+
ИАФ.4	Управление средствами аутентификации	+	+	+
ИАФ.5	Идентификация и аутентификация внешних пользователей	+	+	+
ИАФ.6	Двусторонняя аутентификация			
ИАФ.7	Защита аутентификационной информации при передаче	+	+	+
II. Управление доступом (УПД)				
УПД.0	Разработка политики управления доступом	+	+	+
УПД.1	Управление учетными записями пользователей	+	+	+
УПД.2	Реализация политик управления доступом	+	+	+
УПД.3	Доверенная загрузка		+	+
УПД.4	Разделение полномочий (ролей) пользователей	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий	+	+	+
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+	+	+
УПД.7	Предупреждение пользователя при его доступе к информационным ресурсам			
УПД.8	Оповещение пользователя при успешном входе о предыдущем доступе к информационной (автоматизированной) системе			+
УПД.9	Ограничение числа параллельных сеансов доступа			+

На что стоит обратить внимание

- Для создаваемых ЗОКИИ в ТЗ должны включаться требования к составу и содержанию разрабатываемой документации.
- Категория значимости может быть уточнена в процессе проектирования ЗОКИИ.
- По результатам опытной эксплуатации принимается решение о возможности (или невозможности) проведения приемочных испытаний ЗОКИИ.
- В ТЗ на создание ЗОКИИ должны включаться требования по документации.
- Изменен базовый набор мер защиты.

Средства защиты информации

Оценка соответствия ЗОКИИ



Информирование о компьютерных инцидентах

Субъект КИИ должен информировать ФСБ России обо всех компьютерных инцидентах, связанных с функционированием принадлежащих ему объектов КИИ, не позднее 24 часов с момента обнаружения компьютерного инцидента!

Данные передаются через Национальный координационный центр по компьютерным инцидентам (НКЦКИ) одним из следующих образов:

- с использованием технической инфраструктуры НКЦКИ
- по телефону
- по факсу
- с сайта cert.gov.ru

Приказ ФСБ России «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах»:

- в случае, если компьютерный инцидент связан с функционированием объекта КИИ, принадлежащего субъекту КИИ, который осуществляет деятельность в банковской сфере и в иных сферах финансового рынка, одновременно с информированием ФСБ России о таком компьютерном инциденте также информируется Центральный банк РФ

Вопросы

Спасибо за внимание!

117105, г. Москва, ул. Нагатинская, д. 1

Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru
e-mail: itarvi@DialogNauka.ru