

**Нормативные правовые акты
Российской Федерации, разработанные
в рамках реализации требований
Федерального закона
от 26 июля 2017 г. № 187-ФЗ
«О безопасности критической информационной
инфраструктуры Российской Федерации»»**

Система нормативных правовых актов РФ в области обеспечения безопасности КИИ РФ

! **Федеральный закон от 26.07.2017 № 187-ФЗ**
«О безопасности критической информационной
инфраструктуры Российской Федерации»

➤ **ФЗ от 26 июля 2017 г. № 193-ФЗ**
«О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»

➤ **ФЗ от 26 июля 2017 г. № 194-ФЗ**
«О внесении изменений в Уголовный кодекс Российской Федерации и в статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»

Система нормативных правовых актов РФ в области обеспечения безопасности КИИ РФ

Нормативные правовые акты Президента Российской Федерации



- **Указ Президента РФ от 25 ноября 2017 г. № 569**
«О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085»

- **Указ Президента РФ «О внесении изменений в Указ Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации компьютерных атак»**

- **Указ Президента РФ от 2 марта 2018 г. № 98**
«О внесении изменений в перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203»

Система нормативных правовых актов РФ в области обеспечения безопасности КИИ РФ

Нормативные правовые акты Правительства Российской Федерации



- **Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденные постановлением Правительства РФ от 8 февраля 2018 г. No. 127**
- **Правила осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные постановлением Правительства РФ от 17 февраля 2018 г. No. 162**
- **Проект постановления Правительства РФ «Об утверждении порядка подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов КИИ»**

Система нормативных правовых актов РФ в области обеспечения безопасности КИИ РФ

Нормативные правовые акты ФСТЭК России



➤ **Приказ ФСТЭК России от 11 декабря 2017 г. № 229 «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»**

➤ **Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденный приказом ФСТЭК России от 6 декабря 2017 г. № 227**

➤ **Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом ФСТЭК России от 21 декабря 2017 г. № 235**

➤ **Форма сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденная приказом ФСТЭК России от 22 декабря 2017 г. № 236**

➤ **Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239 (+ изменения, внесенными приказом ФСТЭК России от 9 августа 2018 г. № 138)**

Система нормативных правовых актов РФ в области обеспечения безопасности КИИ РФ



Нормативные правовые акты ФСБ России

- **Приказ ФСБ России от 24 июля 2018 № 366** «О Национальном координационном центре по компьютерным инцидентам» (зарегистрирован Министерством юстиции Российской Федерации 6 сентября 2018 г.)
- **Приказ ФСБ России от 24 июля 2018 г. № 367** «Об утверждении Перечня информации, представляемой в ГосСОПКА, Порядка предоставления информации в ГосСОПКА» (зарегистрирован Министерством юстиции Российской Федерации 6 сентября 2018 г.)
- **Приказ ФСБ России от 24 июля 2018 г. № 368** «Об утверждении порядка обмена информацией о компьютерных инцидентах между объектами критической информационной инфраструктуры Российской Федерации...» (зарегистрирован Министерством юстиции Российской Федерации 6 сентября 2018 г.)
- **Приказ ФСБ России**
«Об утверждении порядка информирования ФСБ России о компьютерных инцидентах и реагирования на них»
- **Приказ ФСБ России**
«Об утверждении порядка технических условий, установки и эксплуатации средств обнаружения, предупреждения и ликвидации компьютерных атак»

Нормативные правовые акты Минкомсвязи России



- **Приказ Минкомсвязи России** «Об утверждении порядка, технических условий, установки и эксплуатации средств обнаружения, предупреждения и ликвидации компьютерных атак на сетях связи»

Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ



ФСТЭК России

Реализация
государственной политики

Организация
межведомственной
координации и взаимодействия

Специальные и контрольные
функции в области
государственной безопасности

по вопросам обеспечения безопасности
критической информационной
инфраструктуры Российской Федерации

25 ноября 2017 года

N 569

УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О ВНЕСЕНИИ ИЗМЕНЕНИЙ В ПОЛОЖЕНИЕ О ФЕДЕРАЛЬНОЙ СЛУЖБЕ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ, УТВЕРЖДЕННОЕ УКАЗОМ ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ ОТ 16 АВГУСТА 2004 Г. N 1085

1. Внести в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. N 1085 "Вопросы Федеральной службы по техническому и экспортному контролю" (Собрание законодательства Российской Федерации, 2004, N 34, ст. 3541; 2006, N 49, ст. 5192; 2008, N 43, ст. 4921; N 47, ст. 5431; 2012, N 7, ст. 818; 2013, N 26, ст. 3314; N 52, ст. 7137; 2014, N 36, ст. 4833; N 44, ст. 6041; 2015, N 4, ст. 641; 2016, N 1, ст. 211), следующие изменения:

а) подпункт 1 пункта 1 изложить в следующей редакции:

"1) обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура);";

б) абзац первый пункта 2 изложить в следующей редакции:

"2. ФСТЭК России является федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, а также специально уполномоченным органом в области экспортного контроля.";

в) в пункте 4:

в подпункте 1 слова "обеспечения безопасности информации в ключевых системах информационной инфраструктуры" заменить словами "обеспечения безопасности значимых объектов критической информационной инфраструктуры";

абзац второй подпункта 4 изложить в следующей редакции:

"обеспечения безопасности значимых объектов критической информационной инфраструктуры";

в подпункте 5 слова "безопасности информации в ключевых системах информационной инфраструктуры" заменить словами "безопасности значимых объектов критической информационной инфраструктуры";

из подпункта 9 слова "по обеспечению безопасности информации в ключевых системах информационной инфраструктуры," исключить;

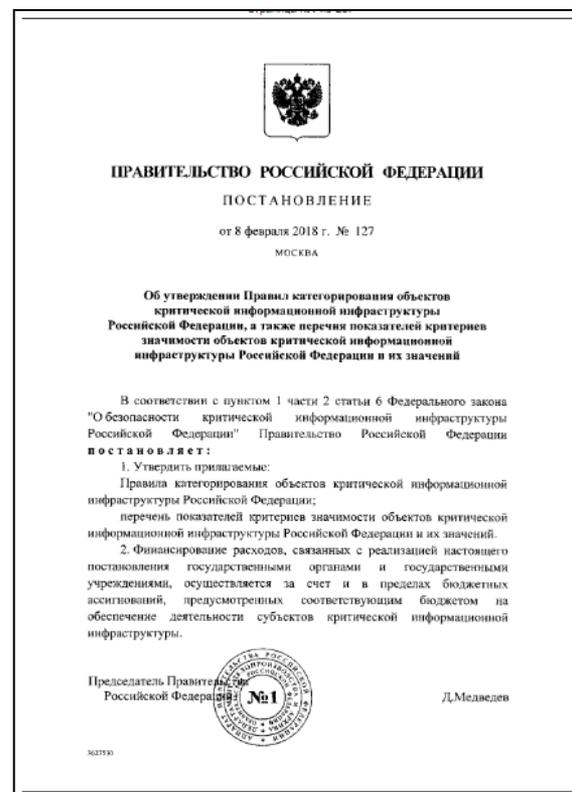
дополнить подпунктом 9.1 следующего содержания:

Правила категорирования объектов критической информационной инфраструктуры Российской Федерации

Утвержденные постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127

Определяет:

- порядок категорирования
- этапы категорирования
- кто должен и может входить в состав комиссии
- как оформляются результаты категорирования



Категорирование объектов КИИ Российской Федерации

Основные этапы Субъект КИИ



**Комиссия
по категорированию**

Определяет процессы

**Выявляет наличия
критических процессов**

Выявляет объекты КИИ

Категорирование объектов КИИ Российской Федерации

Основные этапы (продолжение)

Формирует перечень
объектов КИИ

Согласовывает Перечень

Субъект КИИ
утверждает Перечень

Перечень направляется
в ФСТЭК России

≤ 5 раб. дней



Рекомендуемая форма перечня объектов КИИ

Приведена в информационном сообщении ФСТЭК России от 24 августа 2018 г. № 240/25/3752

Утверждаю
Генеральный директор (*руководитель*) _____
(наименование организации)

А.Петров

«___» _____ 2018г.

Перечень
объектов критической информационной инфраструктуры, подлежащих категорированию

| № п/п | Наименование организации | Сфера деятельности | Наименование объекта | Планируемый срок категорирования | Контакты организации. |
|-------|--------------------------|---|--|----------------------------------|---|
| 1 | 2 | 3 | 4 | 5 | 8 |
| 1. | | транспорт (здравоохранение, связь, наука, банковская сфера, топливно-энергетический комплекс, область атомной энергии, область оборонной промышленности, область металлургической промышленности и т.п.) | 1. Информационные системы: 2. Информационно-телекоммуникационные сети: 3. Автоматизированные системы управления: (производством, производственным процессом и т.п.) | декабрь 2018 г. | Указать контакты должностных лиц, которые могут дать пояснения по информационным системам, включенным в Перечень (Ф.И.О, номер телефона, адрес электронной почты) |

Заместитель руководителя организации, *ответственный за обеспечение безопасности информации или начальник отдела (штатный специалист) по обеспечению безопасности КИИ*

А.Сидоров

«___» _____ 2018 г.

Категорирование объектов КИИ Российской Федерации

В течение 1 года с момента утверждения Перечня объектов КИИ



Рассматриваются возможные
источники УБИ

Анализируются УБИ и уязвимости

Оценивается масштаб возможных
последствий

Устанавливается одна
из категории значимости

Принятие решения
об отсутствии
необходимости присвоения
категории значимости

АКТ категорирования

Категорирование объектов КИИ Российской Федерации

Основные этапы (продолжение)



Категорирование объектов КИИ Российской Федерации

Основные этапы (продолжение)



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

Утверждена приказом ФСТЭК России от 22 декабря 2017 г. № 236

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

ПРИКАЗ

«22» декабря 2017 г. Москва № 236

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

В соответствии с пунктом 3 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 прилагаемую форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.Селин В.СЕЛИН

1. Сведения об объекте КИИ

2. Сведения о субъекте КИИ

3. Сведения о взаимодействии объекта КИИ и сетей электросвязи

4. Сведения о лице, эксплуатирующем объект КИИ

5. Сведения о программных и ПАС, используемых на объекте КИИ

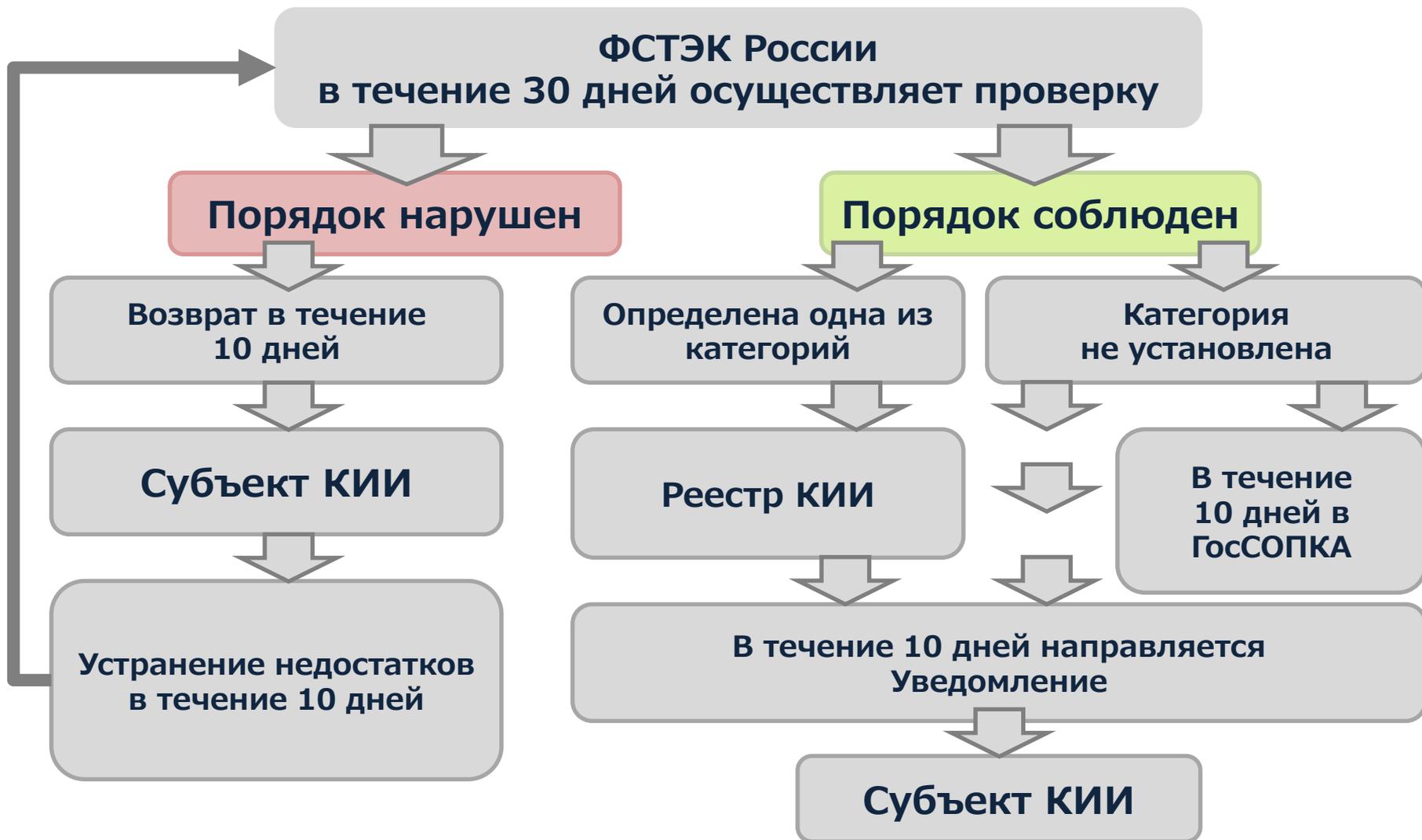
6. Сведения об УБИ и категориях нарушителей в отношении объекта КИИ

7. Возможные последствия в случае возникновения компьютерных инцидентов

8. Категория значимости, которая присвоена объекту КИИ

9. Орг. и тех. меры, применяемые для обеспечения безопасности значимого объекта КИИ

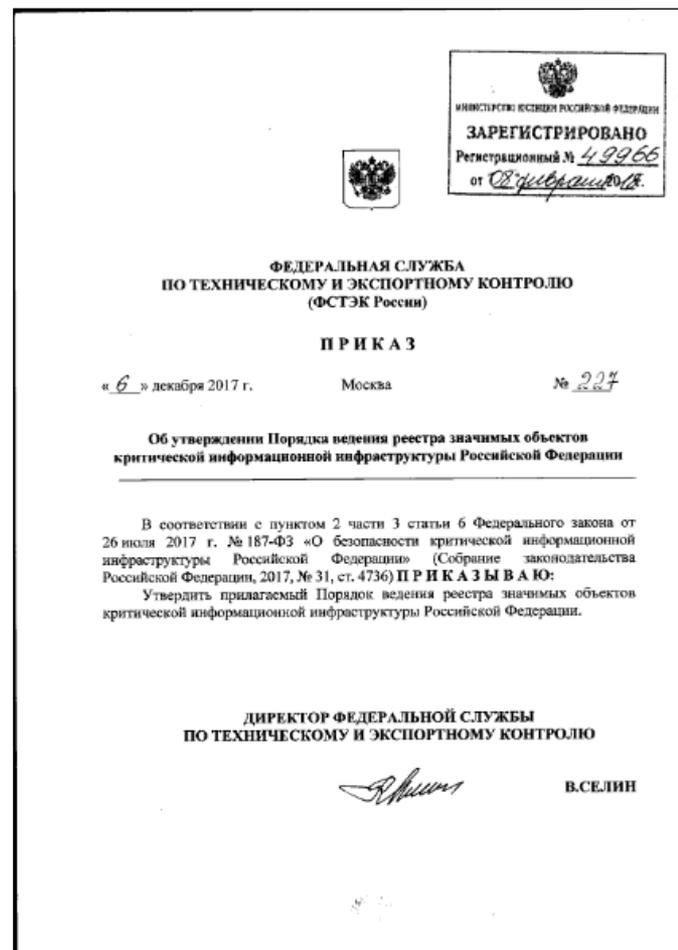
Категорирование объектов КИИ Российской Федерации



Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации

Утвержден приказом ФСТЭК России от 6 декабря 2017 г. № 227

- Реестр формируется и ведется ФСТЭК России
- Субъекты КИИ должны обеспечивать достоверность и актуальность предоставляемых сведений
- Решение о включении в Реестр принимается в течение 30 дней



Правила осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

Утверждены постановлением Правительства Российской Федерации от 17 февраля 2018 г. № 162



Устанавливают сроки проведения проверки



Определяют основания для осуществления проверки



Приведен порядок оформления результатов проверки



Правила осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации



Государственный контроль, осуществляемый ФСТЭК России

Плановый

Истечение 3-х лет со дня последней плановой проверки

Истечение 3-х лет со дня внесения сведений об объекте в Реестр

Приказ руководителя ФСТЭК России (по поручению президента РФ/ Правительства РФ/ требований прокурора)

Внеплановый

Возникновение компьютерного инцидента, повлекшего негативные последствия

Истечение срока выполнения предписания об устранении выявленного нарушения

Выявлены нарушения

Нет нарушений

Предписание об устранении

Акт проверки



Форма акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

Утверждена приказом ФСТЭК России от 11 декабря 2017 г. № 229


ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

« 11 » декабря 2017 г. Москва № 229

Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

В соответствии с пунктом 5 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 прилагаемую форму акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ


В.СЕЛИН


МИНИСТЕРСТВО ИСТОРΙΑ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 48500
от 28 декабря 2017 г.

Приложение
к приказу ФСТЭК России
от « 11 » декабря 2017 г. № 229

Форма

Гриф секретности
или
ограничительная пометка
Экз. № _____

(наименование органа государственного контроля)

АКТ ПРОВЕРКИ
по итогам проведения государственного контроля
в области обеспечения безопасности значимых объектов
критической информационной инфраструктуры
Российской Федерации

« ____ » _____ 20 ____ г. _____
(дата составления акта проверки) (место составления акта проверки)

На основании _____
(дата и номер приказа органа государственного контроля)

в период с « ____ » _____ 20 ____ г. по « ____ » _____ 20 ____ г. была проведена _____
(с указанием даты проведения)

выявленная проверка общей продолжительностью _____ рабочих дней в отношении _____
(наименование субъекта критической информационной инфраструктуры и принадлежащего (принадлежащего) ему значимого объекта (значимых объектов) критической информационной инфраструктуры Российской Федерации (далее – критическая информационная инфраструктура) _____)

_____ (наименование и категория значимости значимого объекта критической информационной инфраструктуры)

Эксплуатацию значимого объекта (значимых объектов) критической информационной инфраструктуры осуществляет: _____

_____ (наименование лица, эксплуатирующего значимый объект критической информационной инфраструктуры)

Место проведения проверки: _____
Должностное лицо (должностные лица) органа государственного контроля, проводившее (проводившие) проверку: _____
(фамилия, имя, отчество (последнее – при наличии) и должность)

С копией приказа о проведении проверки ознакомлен _____
(фамилия, имя, отчество)

При проведении проверки присутствовал: _____
(фамилия, имя, отчество (последнее – при наличии))

и должность руководителя субъекта критической информационной инфраструктуры (его филиала, представительства или иного обособленного структурного подразделения) или уполномоченного им должностного лица _____

2

В ходе проведения проверки установлено: _____
(указывается описание в выполнении субъектом критической информационной инфраструктуры требований, установленных Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» и прилагаемых в соответствии с ним нормативным правовым актами (далее – требования по обеспечению безопасности))

_____ (указывается описание о результатах контрольных мероприятий, проведенных на объекте критической информационной инфраструктуры с использованием специализированных по требованиям безопасности информации программных и программно-аппаратных средств измерения)

В ходе проведения проверки:
выявлены нарушения требований по обеспечению безопасности: _____
(с указанием выявленных нарушений)

выявлены факты невыполнения предписания органа государственного контроля об устранении выявленного нарушения требований по обеспечению безопасности (с указанием реквизитов выданного предписания): _____

выявлены нарушения требований по обеспечению безопасности или факты, явившиеся причиной возникновения компьютерного инцидента, повлекшего негативные последствия, на значимом объекте критической информационной инфраструктуры: _____

_____ (указывается перечень нарушений требований по обеспечению безопасности не выявлено)

Рекомендации: _____

Запись в Журнал учета проверок внесена: _____
(подпись должностного лица, проводившего проверку)

Журнал учета проверок отсутствует: _____
(подпись должностного лица, проводившего проверку)

Прилагаемые к акту документы: _____

Подпись (подписи) должностного лица (должностных лиц) органа государственного контроля, проводившего (проводивших) проверку: _____

С актом проверки ознакомлен(а), акт проверки со всеми приложениями получен(а): _____
(фамилия, имя, отчество (последнее – при наличии) и должность руководителя субъекта критической информационной инфраструктуры или уполномоченного им должностного лица)

« ____ » _____ 20 ____ г. _____
(подпись)

Пометка об отказе ознакомления с актом проверки: _____
(подпись, должностное лицо органа государственного контроля, проводившего проверку)

Требования к созданию системы безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования

Утверждены приказом ФСТЭК России от 21 декабря 2017 г. № 235

1. Общие положения

2. Требования к силам обеспечения безопасности значимых объектов КИИ

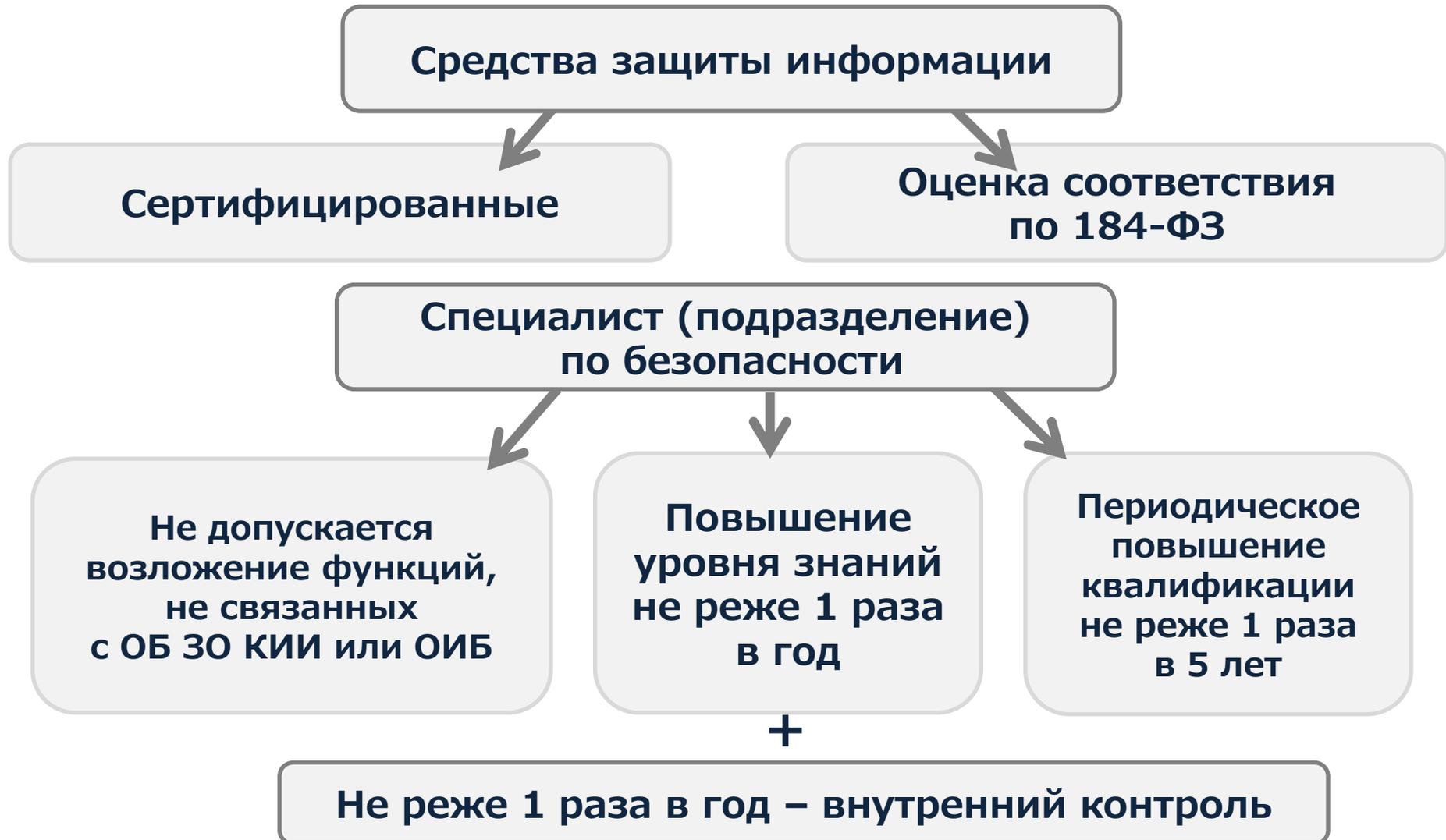
3. Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ

4. Требования к организационно-распорядительным документам по безопасности значимых объектов

5. Требования к функционированию системы безопасности в части организации работ по обеспечению безопасности значимых объектов КИИ



Требования к созданию системы безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования



Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

Утверждены приказом ФСТЭК России от 25 декабря 2017 г. № 239

1. Общие положения

2. Требования по обеспечению безопасности в ходе создания, эксплуатации и вывода из эксплуатации значимых объектов

3. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов

Приложение к Требованиям: Состав мер по обеспечению безопасности значимого объекта соответствующей категории значимости

МИНИСТЕРСТВО КОМПЬЮТЕРНОЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 50524
от 25.12.2017 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.С.ЕЛИН В.С.ЕЛИН

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

Разработка ТЗ (ЧТЗ)

**Модель угроз (основа - БДУ
ФСТЭК России)**

Проектная документация

**Рабочая (эксплуатационная
документация)**

**Организационно-распорядительная
документация**



Меры по обеспечению безопасности значимого объекта критической информационной инфраструктуры

Аудит безопасности

Реагирование на инциденты информационной безопасности

Управление конфигурацией

Управление обновлениями программного обеспечения

Планирование мероприятий по обеспечению безопасности

Обеспечение действий в нештатных (непредвиденных) ситуациях

Информирование и обучение персонала

Идентификация и аутентификация

Управление доступом

Ограничение программной среды

Защита машинных носителей информации

Антивирусная защита

Предотвращение вторжений (компьютерных атак)

Обеспечение целостности

Обеспечение доступности

Защита технических средств и систем

Защита информационной (автоматизированной) системы (сети) и ее компонентов