ФГУП
"НПП "Гамма"

Возникающие сложности при аттестации ЗОКИИ, как следствие ошибок при категорировании

Начальник
Центра аттестации и аудита
ФГУП«НПП«Гамма»
Владимир Ильич Власенко

Указы Президента

УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации

В целях обеспечения технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации п о с т а н о в л я ю:

КАНЦЕЛЯРИЯ

Президент
Российской Федерации В.Путин

Москва, Кремль
30 марта 2022 года
№ 166

УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О дополнительных мерах по обеспечению информационной безопасности Российской Федерации

В целях повышения устойчивости и безопасности функционирования информационных ресурсов Российской Федерации п о с т а н о в л я ю:

КАНЦЕЛЯРИЯ

Президент
Российской Федерации В.Путин

Москва, Кремль
1 мая 2022 года
№ 250

как особое внимание на высшем уровне руководства страны и прорыв в области безопасности КИИ

Правила категорирования

Перед началом категорирования целесообразно провести аудит

Алгоритм категорирования объектов КИИ:

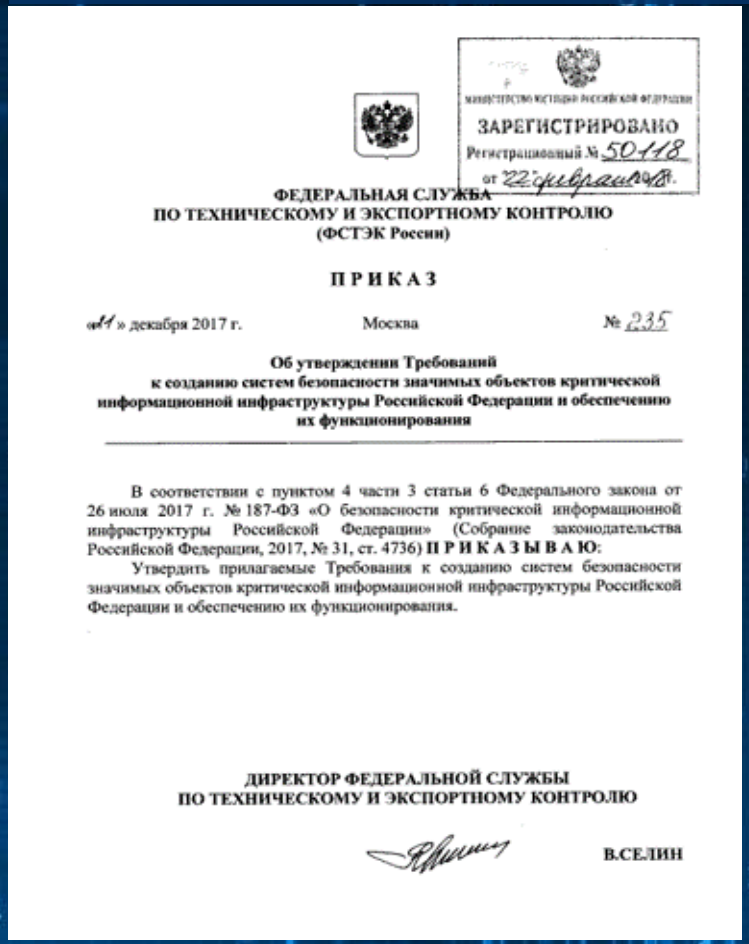
1. Субъект КИИ формирует постоянно действующую комиссию по категорированию.
2. Определяются процессы: управленческие, технологические, производственные, финансово-экономические и (или) иные процессы, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта КИИ.
3. Выявляются критические процессы — управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка.
4. Определяются объекты, которые обрабатывают информацию, необходимую для выполнения критических процессов, и осуществляют управление, контроль или мониторинг критических процессов.
5. Исходя из перечня показателей критериев значимости, и учитывая дополнительные исходные данные, устанавливаются, к какой категории относятся объекты КИИ.
6. Решение комиссии по категорированию оформляется **актом (актами)**, который должен содержать сведения об объекте критической информационной инфраструктуры, сведения о присвоенной объекту критической информационной инфраструктуры категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий
7. Для каждого ОКИИ формируются сведения по форме приказа ФСТЭК России от 22 декабря 2017 г. № 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 ФСТЭК» и эти сведения отправляются во ФСТЭК России.

Результаты Мониторинга КИИ

Актуальность и достоверность сведений

Акт категорирования чаще всего с ошибками

Обеспечение безопасности значимых объектов КИИ



ЗАРЕГИСТРИРОВАНО
Регистрационный № 50118
от 22 февраля 18 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«11» декабря 2017 г. Москва № 235

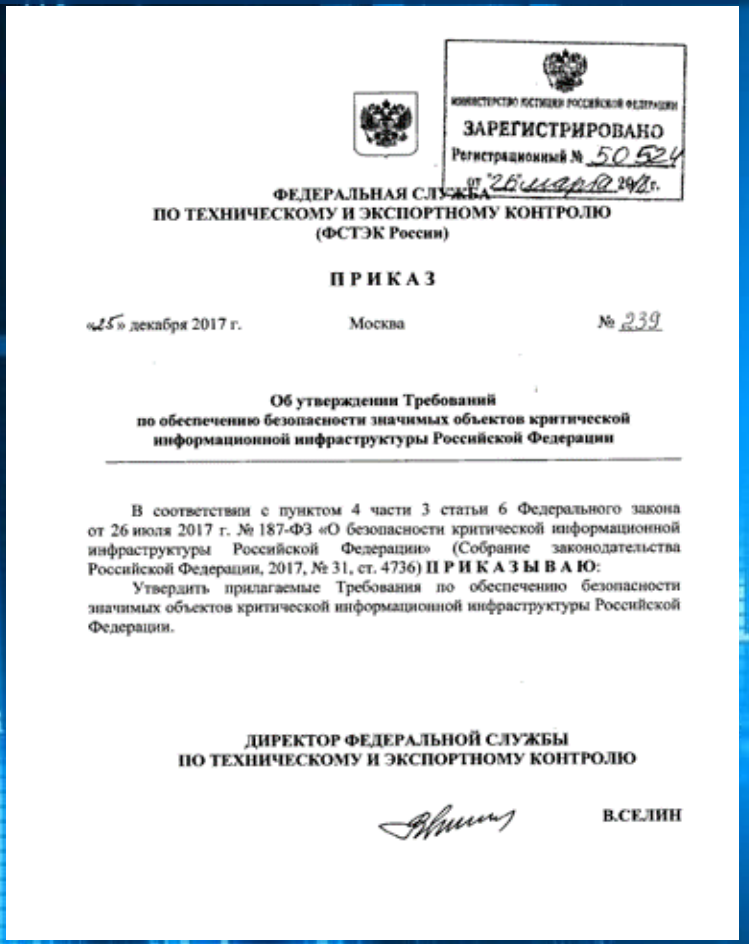
Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования

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 к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН



ЗАРЕГИСТРИРОВАНО
Регистрационный № 50524
от 26 марта 2018 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

Обеспечение безопасности значимых объектов КИИ

Состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости

3 категория	2 категория	1 категория
90 мер	108 мер	117 мер

Аттестация vs Оценка соответствия ЗОКИИ

В каких случаях проводится аттестация ЗОКИИ

- если значимый объект **является ГИС**
- в случае принятия **решения субъектом КИИ**
- в иных случаях, установленных **законодательством Российской Федерации**

При этом оценка значимого объекта и его подсистемы безопасности проводится в форме аттестации ЗОКИИ в соответствии с приказом ФСТЭК России № 17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

Особенности аттестации ЗОКИИ

Новые группы мер защиты в требованиях для ЗОКИИ

1. Реагирование на компьютерные инциденты (ИНЦ)
2. Управление конфигурацией (УКФ)
3. Управление обновлениями программного обеспечения (ОПО)
4. Планирование мероприятий по обеспечению безопасности (ПЛН)
5. Обеспечение действий в нештатных ситуациях (ДНС)
6. Информирование и обучение персонала (ИПО)

3 класс ГИС	3 категория ЗОКИИ
48 мер защиты	90 мер защиты

Особенности аттестации ЗОКИИ

Специфичные требования требованиях для ЗОКИИ

1. Программные и программно-аппаратные средства, в том числе средства защиты информации, применяемые в значимом объекте КИИ, должны быть обеспечены **гарантийной и (или) технической поддержкой.**
2. Должны выполняться требования **по безопасной разработке** программного обеспечения.

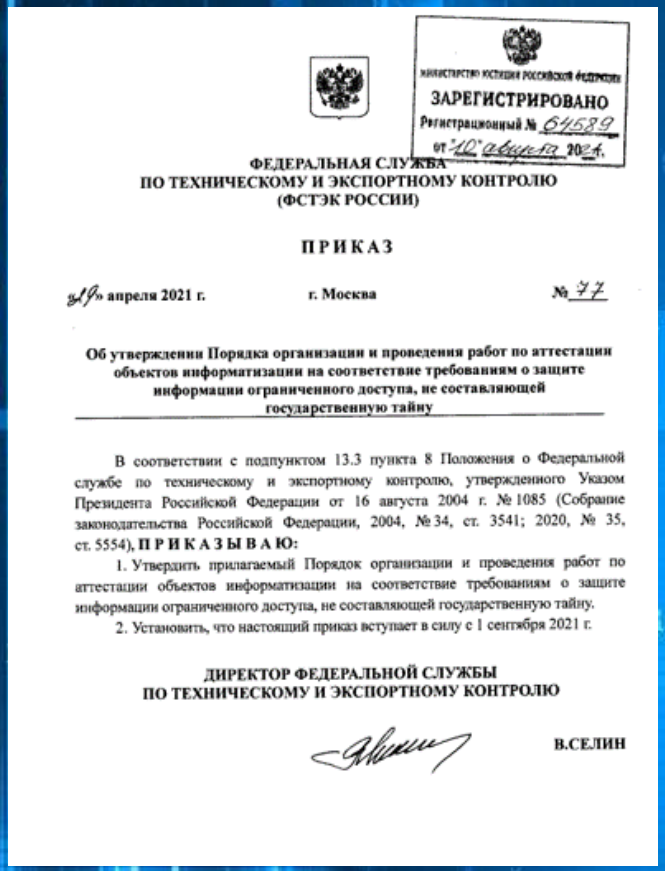
Кто может проводить аттестацию ЗОКИИ

Организация, имеющая лицензию на деятельность по технической защите конфиденциальной информации с пунктом, разрешающим ведение соответствующего вида деятельности (аттестационные испытания и аттестация на соответствие требованиям по защите информации, средств и систем информатизации; помещений), выданную ФСТЭК России в соответствии с постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 «Положение о лицензировании деятельности по технической защите конфиденциальной информации»

Аттестация ЗОКИИ проводится с целью дальнейшего *ввода в эксплуатацию* значимого объекта и его подсистемы информационной безопасности.

Чем регламентирована процедура проведения аттестации и в чем она заключается?

Ввод в эксплуатацию ЗОКИИ и его подсистемы безопасности осуществляется при положительном заключении (выводе) в акте приемки (или в **аттестате соответствия**) о соответствии значимого объекта установленным требованиям по обеспечению безопасности.



Министерство юстиции Российской Федерации
ЗАРЕГИСТРИРОВАНО
Регистрационный № 64539
от “10” августа 2021 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

ПРИКАЗ

«19» апреля 2021 г. г. Москва № 77

Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну

В соответствии с подпунктом 13.3 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2020, № 35, ст. 5554), ПРИКАЗЫВАЮ:

1. Утвердить прилагаемый Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну.

2. Установить, что настоящий приказ вступает в силу с 1 сентября 2021 г.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

Аттестат соответствия

Модернизация (развитие) аттестованного ЗОКИИ

Повторное категорирование

Категория значимости не изменилась и (или) архитектура системы защиты не изменилась

Дополнительные аттестационные испытания

Действие аттестата соответствия не прекращается

Изменение категории значимости и (или) изменению архитектуры системы защиты

Повторная аттестация

Новый аттестат соответствия

Проблемы при аттестации ЗОКИИ

Проблемы

- Категория значимости не пересматриваются и не пересчитываются показатели, даже в связи с изменениями показателей
- Неправильное определение границ значимого объекта КИИ
- Сегментация ЗОКИИ, не приводит к понижению категории значимости, она остается неизменной
- Объединение объектов КИИ может привести к повышению категории значимости
- Несоответствие инфраструктуры требованиям
- Сложность интеграции средств защиты
- Недостаток квалифицированных кадров
- Сложность координации между подразделениями

Вопросы:

Искусство
безопасности,
без опасности

Владимир Ильич
Власенко
Vlasenko.vi@nppgamma.ru

Спасибо
за внимание!