Реализация Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»

ТОРБЕНКО Елена Борисовна
Заместитель начальника управления ФСТЭК России

ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Федеральный закон от 26 июля 2017 г. № 187-ФЗ
«О безопасности критической информационной инфраструктуры Российской Федерации»

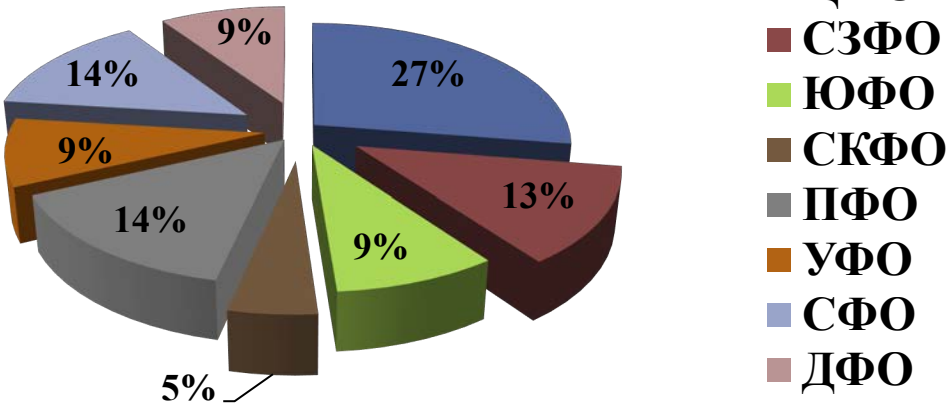
Действует более 22 месяцев или более 670 дней


Сфера здравоохранения
Банковская сфера и иные сферы финансового рынка
Сфера горнодобывающей промышленности
Сфера науки
Сфера энергетики и топливно-энергетического комплекса
Сфера металлургической промышленности

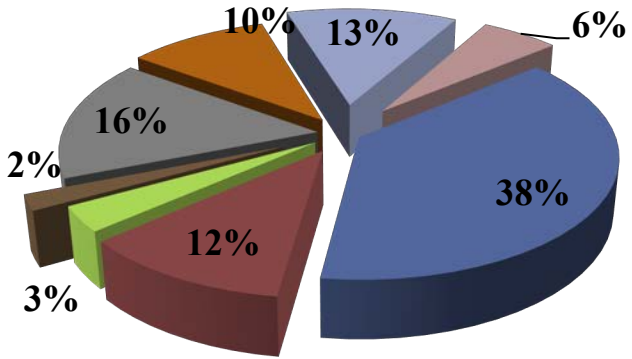
Сфера транспорта
Сфера химической промышленности
Сфера связи
Сфера ракетно-космической промышленности
Сфера оборонной промышленности

Перечни объектов КИИ, представленные в ФСТЭК России

Количество субъектов КИИ



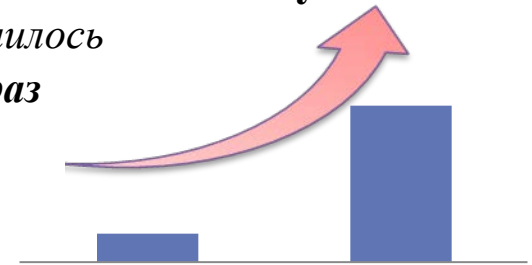
Количество объектов КИИ



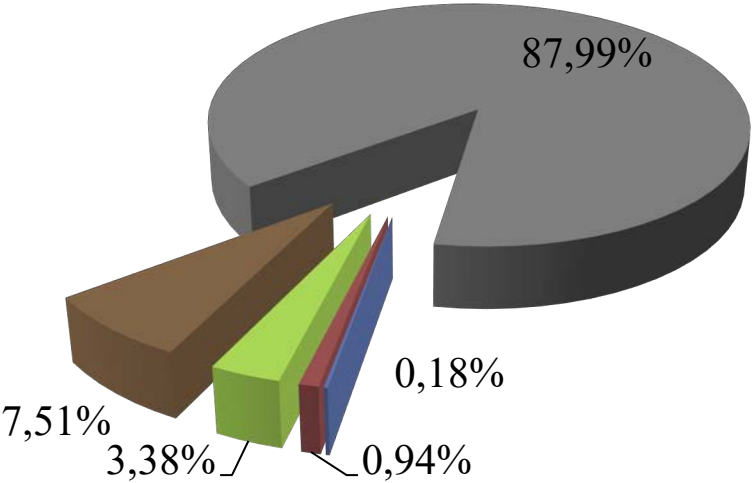
Количество субъектов

увеличилось

в 5.6 раз



Объекты КИИ, представленные в ФСТЭК России

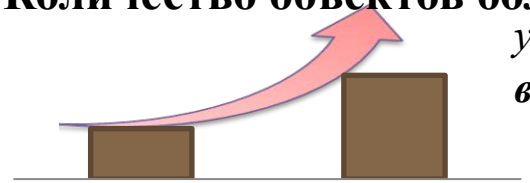


- 1 кат.
- 2 кат.
- 3 кат.
- Без кат.
- Не завершено

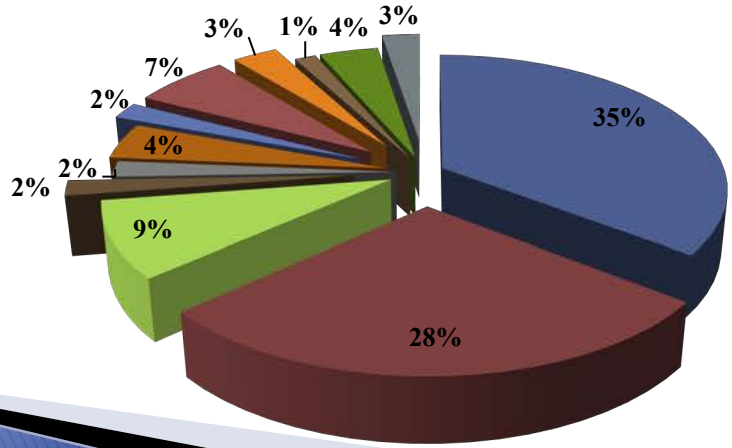
Количество объектов более 45 000

увеличилось

в 2 раза

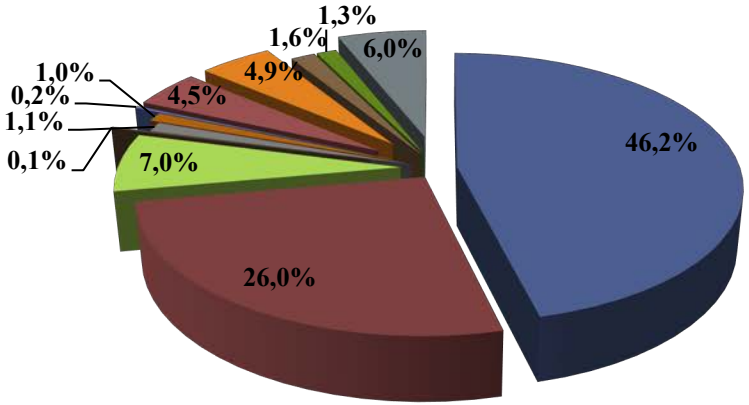


октябрь 2018 г. ноябрь 2019 г.



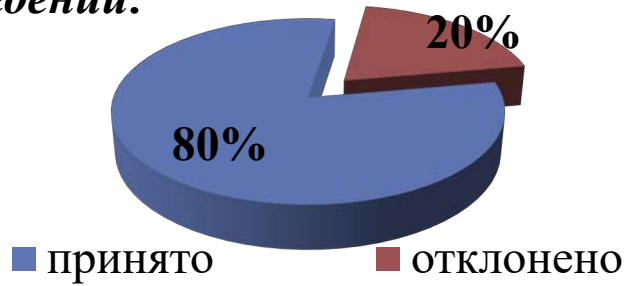
- Энергетика и топливно-энергетический комплекс
- Здравоохранение
- Связь
- Наука
- Транспорт
- Банковская сфера и иные сферы финансового рынка
- Атомная энергия
- Оборонная промышленность
- Ракетно-космическая промышленность
- Горнодобывающая промышленность
- Металлургическая промышленность
- Химическая промышленность

Значимые объекты КИИ



- Энергетика и топливно-энергетический комплекс
- Здравоохранение
- Связь
- Наука
- Транспорт
- Банковская сфера и иные сферы финансового рынка
- Атомная энергия
- Оборонная промышленность
- Ракетно-космическая промышленность
- Горнодобывающая промышленность
- Металлургическая промышленность
- Химическая промышленность

По результатам рассмотрения сведений:



Нормативные правовые акты в области обеспечения безопасности КИИ, разработанные ФСТЭК России

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

Постановление Правительства Российской Федерации от 17 февраля 2018 г. № 162

Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры

Приказ ФСТЭК России от 25 декабря 2017 г. № 239

Об утверждении требований по обеспечению безопасности значимых объектов КИИ

(зарегистрирован Минюстом России 26 марта 2018 г., рег. № 50524)

Приказ ФСТЭК России от 11 декабря 2017 г. № 229

Об утверждении формы акта проверки

(зарегистрирован Минюстом России 28 декабря 2017 г., рег. № 49500)

Приказ ФСТЭК России от 6 декабря 2017 г. № 227

Об утверждении порядка ведения реестра значимых объектов КИИ

(зарегистрирован Минюстом России 8 февраля 2018 г., рег. № 49966)

Приказ ФСТЭК России от 21 декабря 2017 г. № 235

Об утверждении требований к созданию систем безопасности значимых объектов КИИ

(зарегистрирован Минюстом России 22 февраля 2018 г., рег. № 50118)

Приказ ФСТЭК России от 22 декабря 2017 г. № 236

Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости

(зарегистрирован Минюстом России 13 апреля 2018 г., рег. № 50753)

Меры по обеспечению безопасности критической информационной инфраструктуры

ФЕДЕРАЛЬНЫЙ ЗАКОН

от 26 июля 2017 г. № 187-ФЗ

«О безопасности критической информационной инфраструктуры Российской Федерации»

Разработка перечней объектов, подлежащих категорированию

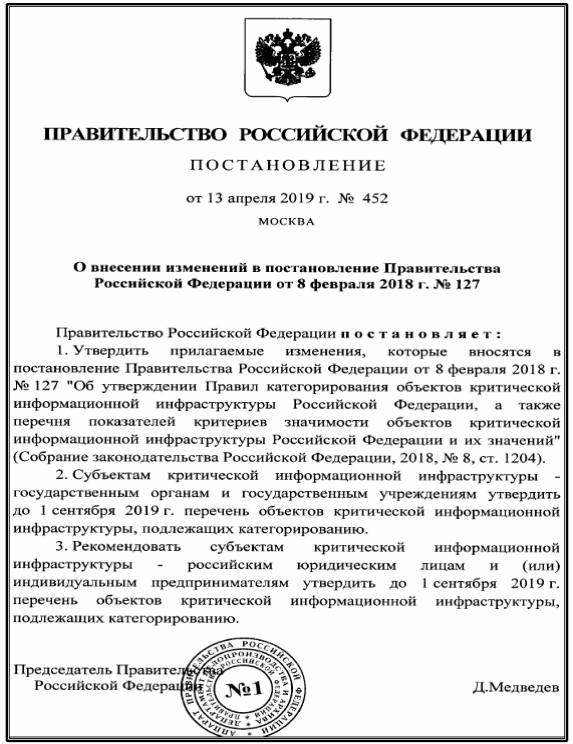
Категорирование объектов КИИ

Осуществление взаимодействия с ГосСОПКА

Создание и обеспечение функционирования систем безопасности объектов КИИ

Принятие мер по обеспечению безопасности объектов КИИ

Изменения в Правила категорирования объектов КИИ



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 13 апреля 2019 г. № 452

МОСКВА

О внесении изменений в постановление Правительства Российской Федерации 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

срок утверждения перечней объектов, подлежащих категорированию – 1 сентября 2019 г.

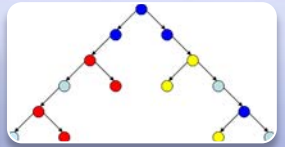
- Категорирование объектов КИИ 1-го уровня значимости
- Категорирование вновь создаваемых объектов КИИ
- Вопросы создания и функционирования комиссии по категорированию
- Рассмотрение наихудших сценариев атак на объект КИИ
- Категорирование связанных объектов КИИ
- Срок утверждения перечня объектов, подлежащих категорированию, Изменение / дополнение перечней
- Оформление 1 акта категорирования на все объекты КИИ, принадлежащие субъекту КИИ
- Значения показателей критериев значимости

Что видим в поступивших сведениях?

- Занижение значимости объектов КИИ
- Игнорирование сроков реализации ФЗ
- Сокрытие объектов КИИ
- Привлечение к категорированию сторонних организаций

О чем забывают при анализе своих ОКИИ?

Многие объекты эксплуатируются множеством организаций



Многие объекты являются территориально распределенными

Применение СЗИ, не прошедших оценку соответствия

Не рассматриваются угрозы, реализуемые внешним нарушителем

Не рассматривается возможность реализации компьютерных инцидентов

На что еще обратить внимание?

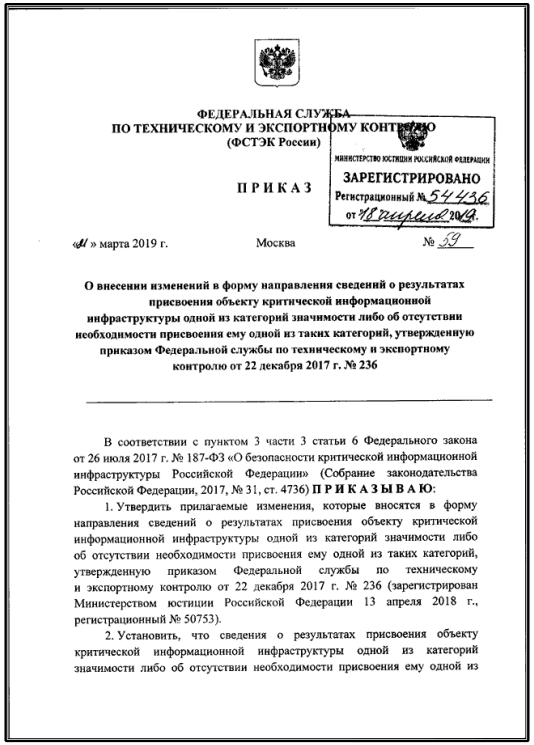
Импортное ПО и оборудование

Связи с внешними сетями

Замедление автоматизируемого процесса

Не учитывается зависимость одного ОКИИ (процесса) от другого ОКИИ (процесса)

Изменения в Форму представления сведений



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 54436
от 18 апреля 2019

П Р И К А З

«11» марта 2019 г. Москва № 59

О внесении изменений в форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденную приказом Федеральной службы по техническому и экспортному контролю от 22 декабря 2017 г. № 236

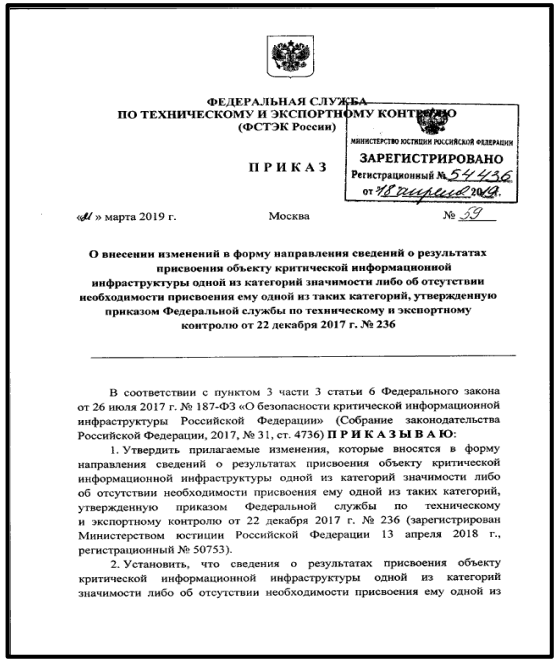
В соответствии с пунктом 3 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) **П Р И К А З Ы В А Ю**:

1. Утвердить прилагаемые изменения, которые вносятся в форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденную приказом Федеральной службы по техническому и экспортному контролю от 22 декабря 2017 г. № 236 (зарегистрирован Министерством юстиции Российской Федерации 13 апреля 2018 г., регистрационный № 50753).

2. Установить, что сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из

- **Введена обязанность представления сведений в формате .ods**
- **Добавлены поля, содержащие сведения для идентификации субъекта КИИ**
- **Добавлено отдельное поле для обоснования полученных значений по категориям значимости объектов**
- **Добавлено поле для идентификации типа объекта**

Ошибки при заполнении Формы представления сведений



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 54436
от 18 апреля 2019

ПРИКАЗ

«21» марта 2019 г. Москва № 59

О внесении изменений в форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденную приказом Федеральной службы по техническому и экспортному контролю от 22 декабря 2017 г. № 236

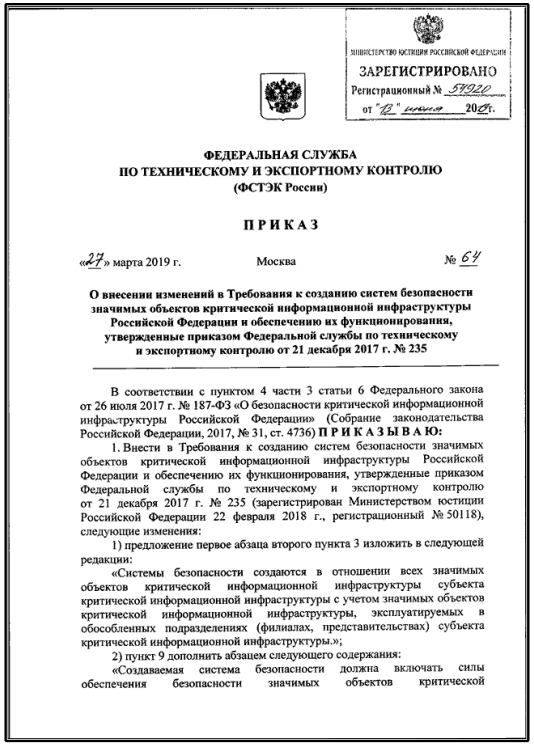
В соответствии с пунктом 3 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) **П Р И К А З Ы В А Ю**:

1. Утвердить прилагаемые изменения, которые вносятся в форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденную приказом Федеральной службы по техническому и экспортному контролю от 22 декабря 2017 г. № 236 (зарегистрирован Министерством юстиции Российской Федерации 13 апреля 2018 г., регистрационный № 50753).

2. Установить, что сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из

- **представлены Сведения без учета изменений, внесенных приказом ФСТЭК России от 21 марта 2019 г. № 59**
- **в представленных Сведениях заполнены не все поля**
- **представлены Акты категорирования объектов критической информационной инфраструктуры**
- **в представленных Сведениях содержится противоречивая информация**
- **несоответствие содержания подпунктов Сведений**

Изменения в Требования к созданию систем обеспечения безопасности ЗО КИИ



МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 53920
от "2" июля 2019 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«27» марта 2019 г. Москва № 64

О внесении изменений в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235

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:**

1. Внести в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235 (зарегистрирован Министерством юстиции Российской Федерации 22 февраля 2018 г., регистрационный № 50118), следующие изменения:

1) предложение первое абзаца второго пункта 3 изложить в следующей редакции:

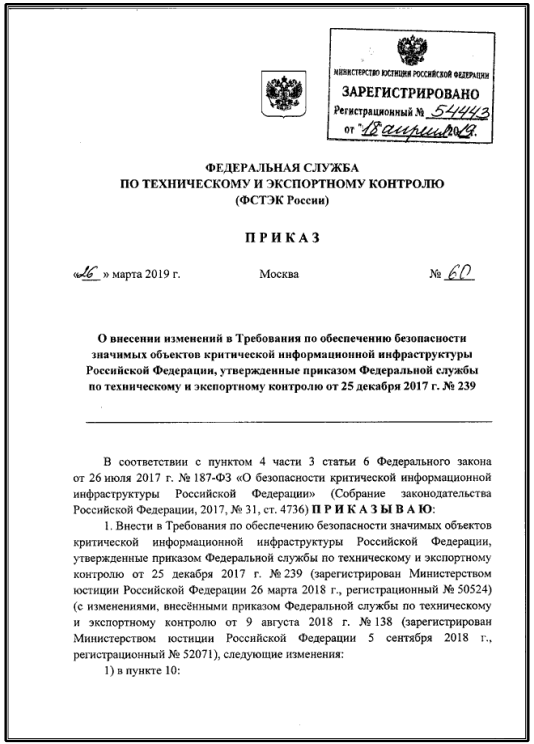
«Системы безопасности создаются в отношении всех значимых объектов критической информационной инфраструктуры субъекта критической информационной инфраструктуры с учетом значимых объектов критической информационной инфраструктуры, эксплуатируемых в обособленных подразделениях (филиалах, представительствах) субъекта критической информационной инфраструктуры.»;

2) пункт 9 дополнить абзацем следующего содержания:

«Создаваемая система безопасности должна включать силы обеспечения безопасности значимых объектов критической

- **Уточнен порядок создания систем безопасности в филиалах (представительствах) и подчиненных организациях интегрированных структур**
- **Установлены требования к квалификации специалистов по безопасности значимых объектов КИИ**
- **Вступление в силу требований к квалификации с 1 января 2021 г.**

Изменения в Требования по обеспечению безопасности ЗО КИИ



МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 54443
от 18 апреля 2019

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«16» марта 2019 г. Москва № 60

О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239

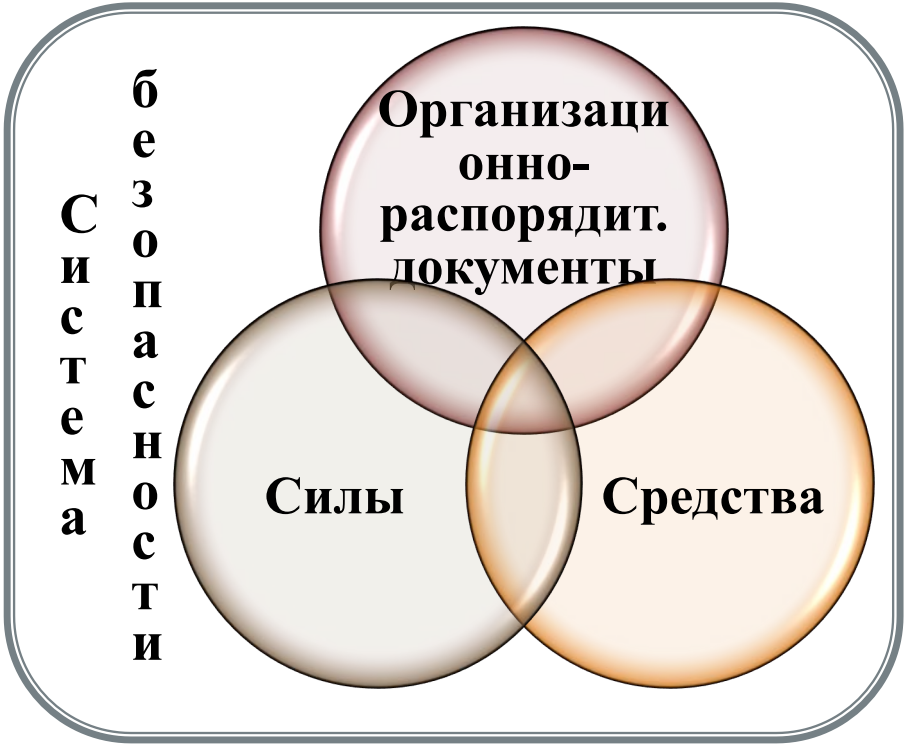
В соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) **П Р И К А З Ы В А Ю**:

1. Внести в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 (зарегистрирован Министерством юстиции Российской Федерации 26 марта 2018 г., регистрационный № 50524) (с изменениями, внесёнными приказом Федеральной службы по техническому и экспортному контролю от 9 августа 2018 г. № 138 (зарегистрирован Министерством юстиции Российской Федерации 5 сентября 2018 г., регистрационный № 52071), следующие изменения:

1) в пункте 10:

- **Уточнен состав организационных и технических мер в базовых наборах**
- **Установлены требования в части уровней доверия применяемых сертифицированных СЗИ**
- **Установлено требование о применении сертифицированных маршрутизаторов**
- **Установлено требование о размещении компонентов значимых объектов КИИ на территории РФ**

Создание системы обеспечения безопасности ЗО КИИ



Создание/определение штатных служб или подразделений по обеспечению безопасности объектов КИИ

Проведение инвентаризация ПО и оборудования, входящих в состав объектов КИИ

Разработка/доработка организационно-распорядительных документов, регламентирующих защиту значимых объектов КИИ

усиление мер по защите периметра АСУ ТП

принятие мер по поддержанию безопасного состояния систем

постоянный мониторинг безопасности систем

управление инцидентами информационной безопасности

Создание системы обеспечения безопасности ЗО КИИ

организация – лицензиат (ТЗИ или ТЗКИ)

руководитель субъекта КИИ

уполномоченное лицо

Обособленное подразделение (филиал, представительство)

Взаимодействие!!!!

подразделения, эксплуатирующие значимые объекты

подразделения, обеспечивающие функционирование значимых объектов

подразделение, ответственное за обеспечение безопасности значимых объектов

Создание системы обеспечения безопасности ЗО КИИ для дочерних обществ, являющихся субъектами КИИ

Требования к силам обеспечения безопасности

Функции и обязанности структурного подразделения по безопасности

- ✓ **разработка предложений по совершенствованию организационно-распорядительных**
- ✓ **обеспечение в соответствии с требованиями по обеспечению безопасности значимых**
- ✓ **подготовка предложений по совершенствованию функционирования систем безопасности, а также по повышению уровня безопасности значимых объектов;**

Не допускается возложение на структурное подразделение (специалистов) по безопасности функций, не связанных с обеспечением безопасности ЗО КИИ или ***обеспечением информационной безопасности субъекта КИИ в целом***

Руководитель субъекта КИИ создает или определяет структурное подразделение, ответственное за обеспечение безопасности ЗО КИИ, или назначает отдельных работников, ответственных за обеспечение безопасности ЗО КИИ

Требования к работникам структурного подразделения по безопасности

Руководитель структурного подразделения по безопасности

- высшее профессиональное образование
  - по направлению подготовки в области информационной безопасности
  - иное высшее профессиональное образование и обучение по программе профессиональной переподготовки по направлению "Информационная безопасность" (не менее 360 часов),
- наличие стажа работы в сфере информационной безопасности не менее 3 лет

Штатные работники структурного подразделения по безопасности

- высшее профессиональное образование
  - по направлению подготовки в области информационной безопасности
  - иное высшее профессиональное образование и прохождение обучения по программе повышения квалификации по направлению "Информационная безопасность" (не менее 72 часов)

прохождение не реже одного раза в 5 лет обучения по программам повышения квалификации по направлению "Информационная безопасность»

Вступление в силу с 1 января 2021 г.

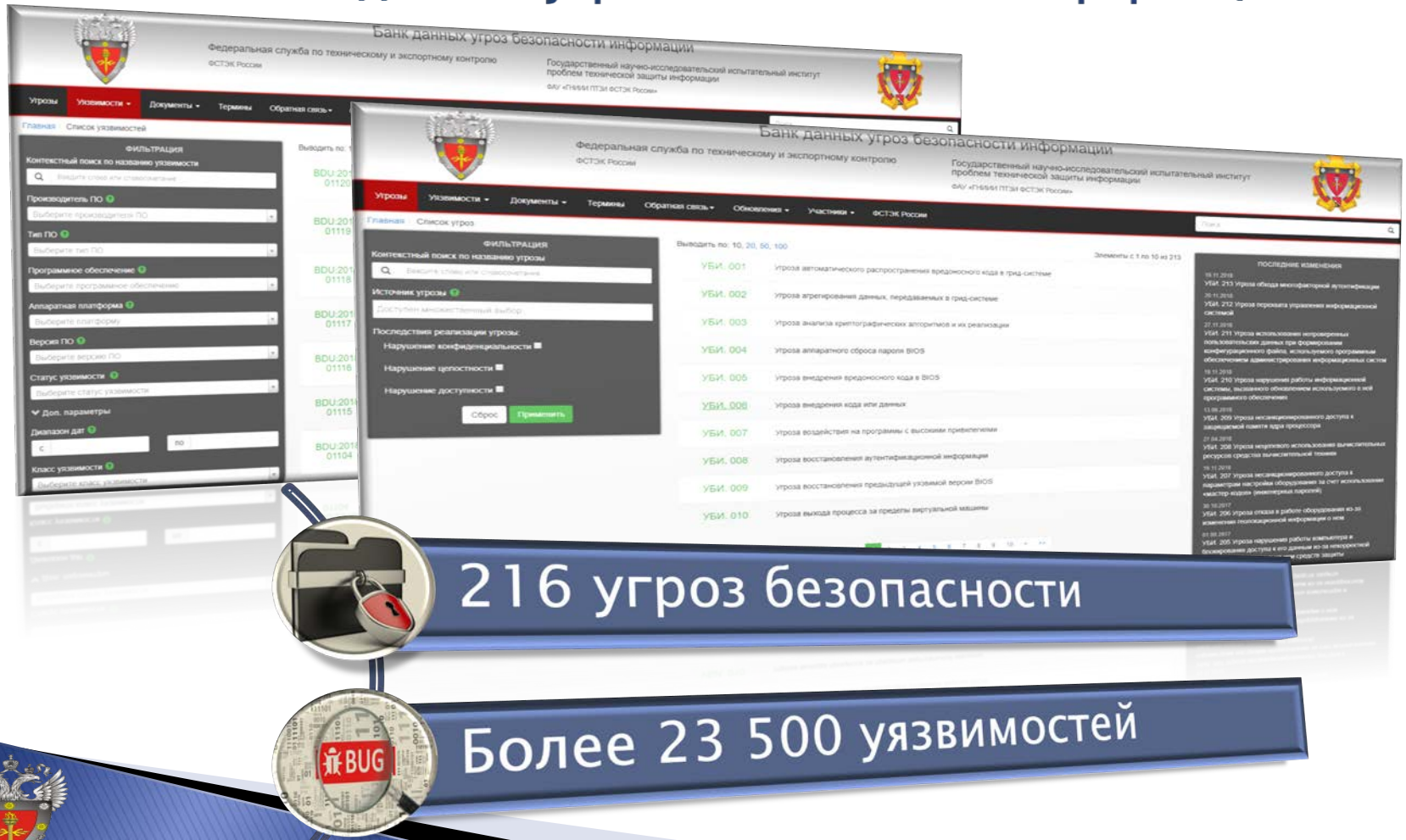
Внедрение мер по обеспечению защиты ЗО КИИ

1. • Формирование требований к обеспечению безопасности значимого объекта
2. • Разработка организационных и технических мер по обеспечению безопасности значимого объекта
3. • Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и его ввод в эксплуатацию
4. • Обеспечение безопасности значимого объекта в ходе его эксплуатации
5. • Обеспечение безопасности значимого объекта при выводе его из эксплуатации

Проблемы при внедрении мер обеспечения безопасности ЗО КИИ

- Требования к системе обеспечения безопасности закладываются на этапе ТЗ
- Нет знаний о защищаемом объекте
- Есть не учтенные подключения к сетям общего пользования
- Оборудование управляется удаленно (по гарантии или нет)
- Неправильно настроены СЗИ
- Не учитываются ограничения на эксплуатацию СЗИ
- Не все объекты защиты учитываются при построении системы обеспечения безопасности

Банк данных угроз безопасности информации



216 угроз безопасности

Более 23 500 уязвимостей

СПАСИБО ЗА ВНИМАНИЕ!

ТОРБЕНКО Елена Борисовна
Заместитель начальника управления ФСТЭК России