Управление ФСТЭК России

★ по Южному и Северо-Кавказскому федеральным округам ★

г. Ростов-на-Дону

Реализация Федерального закона от 26 июня 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Начальник 1 отдела Управления ФСТЭК России по Южному и Северо-Кавказскому федеральным округам

Чернов Николай Иванович

Телефон: (863) 200-75-25

Вопрос № 1

Обзор практики категорирования объектов критической информационной инфраструктуры

Чернов Николай Иванович
Начальник отдела

СИСТЕМА НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

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

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 от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»**
- **Указ Президента РФ от 2 марта 2018 г. № 98 «О внесении изменений в Перечень сведений, отнесенных к государственной тайне, утвержденный Указом Президента РФ от 30 ноября 1995 г. № 1203»**

Нормативные правовые акты Правительства Российской Федерации

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

Нормативные правовые акты федеральных органов исполнительной власти

- **Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении требований к созданию систем безопасности значимых объектов КИИ»**
- **Приказ ФСТЭК России от 22 декабря 2017 г. № 236 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости»**
- **Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов КИИ»**
- **Приказ ФСТЭК России от 11 декабря 2017 г. № 229 «Об утверждении формы акта проверки»**
- **Приказ ФСТЭК России от 6 декабря 2017 г. № 227 «Об утверждении порядка ведения реестра значимых объектов КИИ»**
- **Приказ ФСБ России от 24 июля 2018 г. № 366 «Об утверждении Положения о Национальном координационном центре по компьютерным инцидентам»**
- **Приказ ФСБ России от 24 июля 2018 г. № 367 «Об утверждении перечня информации, представляемой в ГосСОПКА и порядка ее представления»**
- **Приказ ФСБ России «Об утверждении порядка информирования ФСБ России и компьютерных инцидентах и реагирования на них»**
- **Приказ ФСБ России «Об утверждении порядка, технических условий, установки и эксплуатации средств обнаружения, предупреждения и ликвидации компьютерных атак»**
- **Приказ ФСБ России от 24 июля 2018 г. № 368 «Об утверждении порядка об обмене информации о компьютерных инцидентах между субъектами КИИ»**
- **Приказ Минкомсвязи России «Об утверждении порядка, технических условий, установки и эксплуатации средств обнаружения, предупреждения и ликвидации компьютерных атак на сетях связи»**
- **Приказ ФСБ России «Об утверждении требований к средствам обнаружения, предупреждения и ликвидации компьютерных атак»**

- - вступил в силу
- - готовит ФСТЭК России
- - готовит ФСБ России
- - готовит Минкомсвязи России

ПЕРЕЧЕНЬ
объектов КИИ Северо-Кавказского федерального округа, подлежащих категорированию, по состоянию на 18 апреля 2019 г.

Субъект Российской Федерации	Включено в Перечень объектов КИИ	Сфера деятельности												Всего
		Здравоохранение	Ракетно-космическая промышленность	Горнодобывающая промышленность	Металлургическая промышленность	Банковская сфера и иные сферы финансового рынка	Наука	Транспорт	Связь	Атомная энергия	ТЭК	ОПК	Химическая промышленность	
Республика Дагестан	субъектов КИИ	-	-	-	-	-	-	-	-	-	-	2	-	2
	объектов КИИ	-	-	-	-	-	-	-	-	-	-	5	-	5
Республика Ингушетия	субъектов КИИ	-	-	-	-	-	-	1	1	-	-	-	-	2
	объектов КИИ	-	-	-	-	-	-	3	3	-	-	-	-	6
КБР	субъектов КИИ	-	-	-	-	-	-	-	-	-	-	-	-	-
	объектов КИИ	-	-	-	-	-	-	-	-	-	-	-	-	-
КЧР	субъектов КИИ	-	-	-	-	1	-	-	-	-	-	-	-	1
	объектов КИИ	-	-	-	-	4	-	-	-	-	-	-	-	4
РСО-А	субъектов КИИ	-	-	-	-	-	-	-	-	-	-	-	-	-
	объектов КИИ	-	-	-	-	-	-	-	-	-	-	-	-	-
Чеченская Республика	субъектов КИИ	-	-	-	-	-	-	-	-	-	-	-	-	-
	объектов КИИ	-	-	-	-	-	-	-	-	-	-	-	-	-
Ставропольский край	субъектов КИИ	77	-	-	-	-	-	-	1	-	2/2	1	2	83/2
	объектов КИИ	315	-	-	-	-	-	-	8	-	29/25	1	30	383/25
Всего за СКФО	субъектов КИИ	77	-	-	-	1	-	1	2	-	2/2	3	2	88/2
	объектов КИИ	315	-	-	-	4	-	3	11	-	29/25	6	30	398/25

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»

Подготовлено в соответствии с пунктом 1 части 2 статьи 6 Федерального закона № 187-ФЗ

Утверждает:

- Правила категорирования объектов КИИ РФ
- Перечень показателей критериев значимости объектов КИИ РФ и их значения

К обсуждению привлечены представители более 40 организаций

Согласовано с 12 ФОИВ, ЦБ РФ, ГК «Росатом», ГК «Роскосмос»

ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

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

вступил в силу с 1 января 2018 г.

Сфера здравоохранения

Сфера науки

Сфера транспорта

Сфера связи

Сфера энергетики

Сфера топливно-энергетического комплекса

Банковская сфера и иные сферы финансового рынка

Сфера энергетики и топливно-энергетического комплекса

Сфера атомной энергии

Сфера ракетно-космической промышленности

Сфера горнодобывающей промышленности

Сфера металлургической промышленности

Сфера химической промышленности

Сфера оборонной промышленности

Правила категорирования объектов КИИ РФ

Категорирование – это установление соответствия

Критерии значимости — Объект КИИ

Критерии значимости — Объект КИИ

КАЖДОГО объекта КИИ

критериям значимости и их показателям

Критерии значимости — Объект КИИ

*осуществляется субъектами КИИ в отношении принадлежащих им на праве собственности, аренды или **ином законном основании объектов КИИ***

Правила категорирования объектов КИИ РФ

п. 9 Правил категорирования объектов КИИ РФ: категорирование осуществляется субъектом-владельцем объекта КИИ на основании исходных данных, предоставляемых субъектом-владельцем оборудования

п. 9 Правил категорирования объектов КИИ РФ: категорирование осуществляется субъектом КИИ в том числе на основе данных об угрозах безопасности информации, предоставляемых этими субъектами КИИ.

И в том числе на основе данных о последствиях нарушения или прекращения функционирования указанных программных и (или) программно-аппаратных средств, предоставляемых субъектом КИИ.

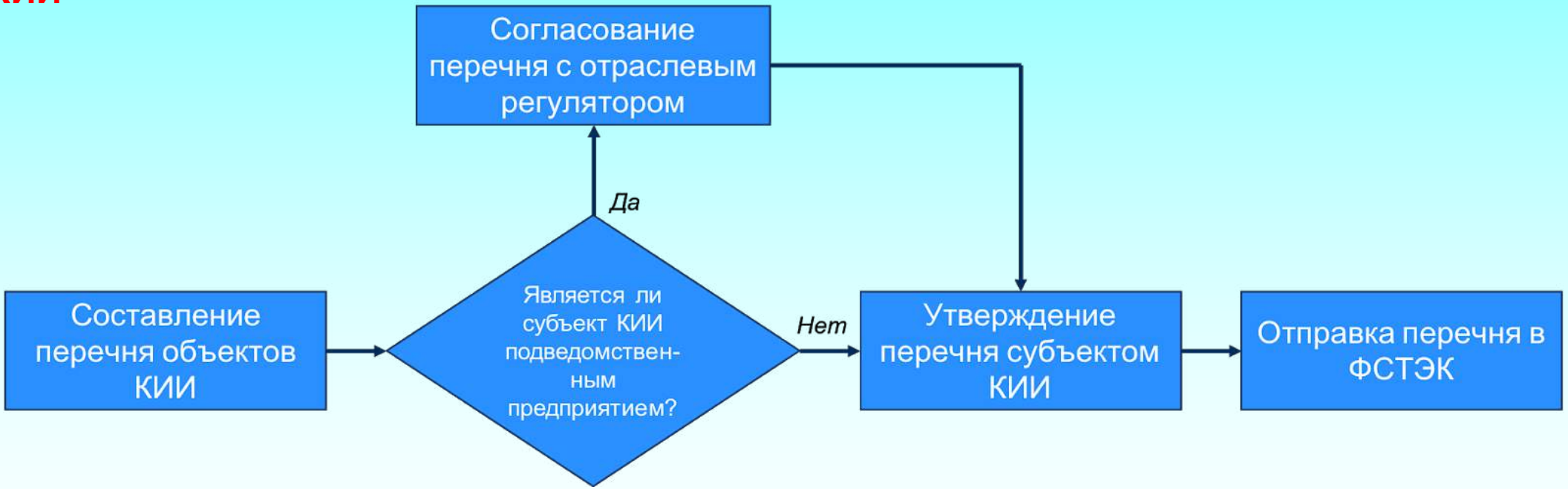
Правила категорирования объектов КИИ РФ

Перечень действующих объектов подлежит Утверждению субъектом КИИ до 1 июня 2019 г.

Максимальный срок категорирования не должен превышать 6 месяцев со дня утверждения субъектом КИИ перечня

Согласование Перечня с государственным органом или российским юридическим лицом, выполняющим функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере в части подведомственных им субъектов КИИ

Перечень объектов до утверждения подлежит согласованию в части подведомственных им субъектов КИИ



Перечень действующих объектов подлежит Утверждению субъектом КИИ до 1 июня 2019 г.

Правила категорирования объектов КИИ РФ

В субъекте КИИ создается
1 комиссия по категорированию

Комиссия по категорированию

Создается решением руководителя субъекта КИИ

п. 11 Правил категорирования

руководитель субъекта КИИ или уполномоченное им лицо
работники субъекта КИИ, являющиеся специалистами в области выполняемых функций, в области информационных технологий, по эксплуатации основного технологического оборудования
работники субъекта КИИ, на которых возложены функции обеспечения безопасности объектов КИИ
работники подразделения по защите государственной тайны субъекта КИИ
работники уполномоченные на решение задач по ГО и ЧС

п. 11 Правил категорирования:
В состав <u>могут</u> включаться представители гос. органов и российских юридических лиц, выполняющих функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию
***в установленной сфере** деятельности, <u>по согласованию с ними</u>.*

п. 11.1. Иные работники, в том числе работники финансово-экономического подразделения.
п. 11.2. Назначение отдельных комиссий в филиалах, представительствах.
п. 11.3. Случаи расформирования комиссии.

Правила категорирования объектов КИИ РФ

Утверждается субъектом КИИ

Перечень объектов КИИ, подлежащих категорированию

Направляется в центральный аппарат ФСТЭК России
Срок: 5 рабочих дней

Обязательное согласование только для организаций, подведомственных (п. 15 Порядка категорирования)

Рекомендация: форма Перечня в информационном сообщении

Рекомендация: указывать планируемые сроки категорирования объектов КИИ

Рекомендация: прилагать электронный вид Перечня

Рекомендуемая форма перечня

Информационное сообщение
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.					

[1] Указывается один из следующих типов объекта: информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть.

[2] Указывается сфера (область) в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации инфраструктуры Российской Федерации».

[3] Указываются должность, фамилия, имя, отчество (при наличии) должностного лица, с которым можно осуществить взаимодействие по вопросам категорирования объекта, его телефон, адрес электронной почты (при наличии). Для нескольких объектов может быть определено одно должностное лицо.

Типовые недостатки при подготовке перечней объектов, подлежащих категорированию

- Вместо наименования объекта указывается место его размещения (или другая информация, в т.ч. наименование субъекта)
- Представляется не утвержденный перечень
- ФСТЭК России не утверждает и не согласует перечни
- Перечень представляется не в центральный аппарат ФСТЭК России
- Перечень представляется не субъектами КИИ (водоканалы, ОМСУ, …)
- В перечне учтены не все критические процессы, учтены не все типы объектов (АСУ, ИС, ИТКС)
- В перечне не учтены объекты, принадлежащие на иных законных основаниях

Перечень показателей критериев значимости объектов КИИ РФ и их значения

(Внесены изменения в Перечень показателей)

I социальная значимость

1.1 | 1.2 | 1.3 | 1.4 | 1.5

II политическая значимость

2.1 | 2.2

III экономическая значимость

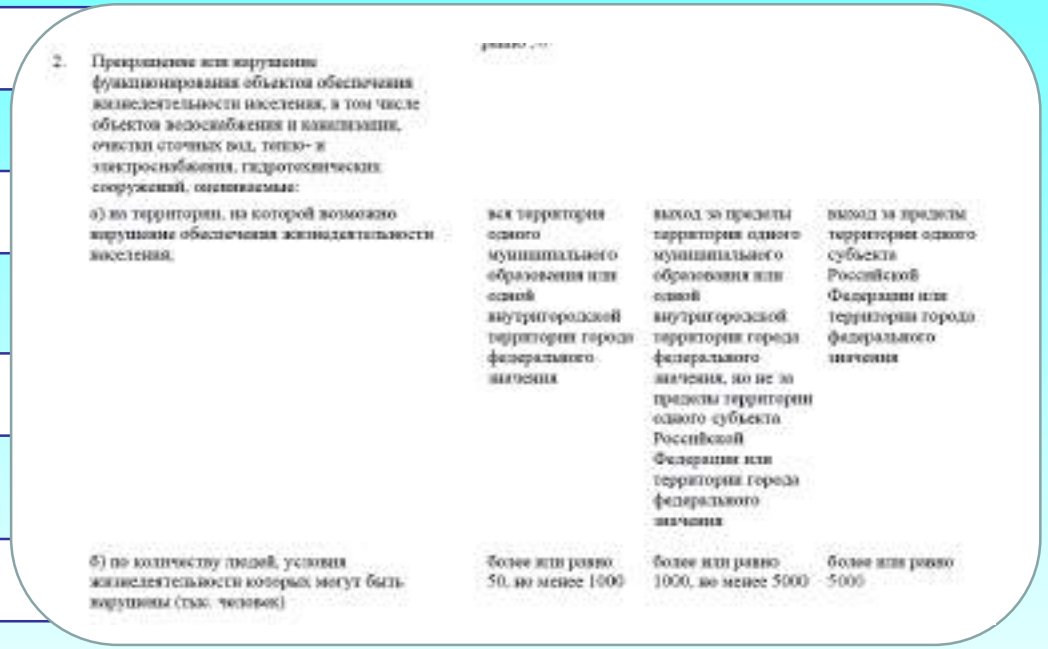
3.1 | 3.2 | 3.3

IV экологическая значимость

4.1

V значимость для обеспечения обороны страны, безопасности государства и правопорядка

5.1 | 5.2 | 5.3



2. Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения, гидротехнических сооружений, оцениваемые:			
а) по территории, на которой возможно нарушение обеспечения жизнедеятельности населения	вся территория одного муниципального образования или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта Российской Федерации или территории города федерального значения	выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения
б) по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек)	более или равно 50, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000

Оценка производится по каждому из значений!

Категория присваивается по наивысшему значению

Правила категорирования объектов КИИ РФ

Акт
категорирования объекта КИИ

должен содержать сведения об объекте КИИ (п. 16 Правил)

подписывается членами комиссии и утверждается руководителем субъекта КИИ

Субъект КИИ обеспечивает хранение акта категорирования

Допускается оформление единого акта по результатам категорирования нескольких объектов КИИ

Форма Акта категорирования определяется субъектом КИИ

Акт категорирования НЕ ПРЕДСТАВЛЯЕТСЯ в ФСТЭК России

Направление сведений о результатах категорирования в ФСТЭК России

Пункт 17
Правил категорирования

ФСТЭК России
ПРИКАЗ
от 22 декабря 2017 г.
№ 236

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

Рекомендуется прикладывать
СВЕДЕНИЯ
В ЭЛЕКТРОННОМ ВИДЕ

- **сведения об объекте КИИ**
- **сведения о субъекте КИИ**
- **сведения о взаимодействии объекта КИИ и сетей электросвязи**
- **сведения о лице, эксплуатирующем объект КИИ**
- **сведения о программных и программно-аппаратных средствах, используемых на КИИ**
- **сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта КИИ**
- **возможные последствия в случае возникновения компьютерных инцидентов на объекте КИИ**
- **категория значимости, которая присвоена объекту КИИ, а также сведения о результатах оценки показателей критериев значимости**
- **организационные и технические меры, применяемые для обеспечения безопасности объекта КИИ**

Типовые недостатки при подготовке сведений о результатах категорирования объекта КИИ

- Нарушен порядок категорирования
- Представлены недостоверные сведения
- Представлены не полные сведения
- Сведения не утверждены
- Сведения подготовлены не по форме (или не по той форме)
- Указаны не все показатели критериев значимости
- Отсутствует обоснование неприменимости критериев значимости

Сведения об отсутствии необходимости присвоения объекту КИИ категории значимости также представляются в ФСТЭК России

1. Сведения об объекте КИИ

Наименование объекта (наименование ИС, АСУ или ИТКС)	**Автоматизированная система расчетов «Наименование»**
Адреса размещения объекта, в том числе адреса обособленных подразделений (филиалов, представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства)	**Подразделение / филиал / представительство: Адрес:** **–название улицы, номер дома;** **–название населенного пункта (города, поселка и т.п.);** **–название района;** **–название республики, края, области, автономного округа (области);** **–почтовый индекс** **Сегментов нет [указываются в случае наличия вместе с адресами размещения]**
Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"	**Связь**
Назначение объекта	**1. Автоматизация расчетов с абонентами за любые виды оказываемых им или заказываемых ими услуг связи в любом сочетании за исключением услуг связи, оказываемых с использованием таксофонов, услуг телеграфной связи и услуг почтовой связи.** **2. Автоматизация предобработки информации об оказанных услугах связи (пребиллинг).** **3. Хранение данных о состоянии счетов абонентов.**
Критические процессы (управленческие, технологические, производственные, финансово-экономические и (или) иные процессы, функции управления и контроля), которые обеспечиваются объектом **Тип объекта (ИС, АСУ, ИТКС)**	**Управление и эксплуатация услуг (SM&O)**
Архитектура объекта (одноранговая сеть, клиент-серверная система, технология "тонкий клиент", сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура)	**Клиент-серверная система,** **технология «тонкий клиент» [указываются в случае наличия технологии «тонкий клиент»]**

2. Сведения о субъекте КИИ

Наименование субъекта	***Наименование оператора связи***
Адрес местонахождения субъекта	***Адрес места государственной регистрации оператора связи:*** ***–название улицы, номер дома;*** ***–название населенного пункта (города, поселка и т.п.);*** ***–название района;*** ***–название республики, края, области, автономного округа (области);*** ***–почтовый индекс***
Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	***Должность, фамилия, имя, отчество***
Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов, или в случае отсутствия такого должностного лица, наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта.	***Должность, фамилия, имя, отчество***
Структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) штатного специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии) **2.6. ИНН субъекта и КПП его обособленных подразделений**	***Наименование структурного подразделения*** **[** ***указываются в случае наличия данного подразделения*** **],** ***Должность руководителя подразделения*** **[** ***указываются в случае наличия данного подразделения*** **]** ***или штатного специалиста,*** ***фамилия, имя, отчество,*** ***телефон,*** ***адрес электронной почты***

3. Сведения о взаимодействии объекта КИИ и сетей электросвязи

Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при помощи электромагнитных систем) или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	**Общего пользования** **[** ***указываются иные категории сетей электросвязи в случае наличия взаимодействия*** **]**
Наименование оператора связи и (или) провайдера хостинга	***Наименование оператора связи*** **[** ***это сам оператор связи, т.к. с его сетью электросвязи взаимодействует объект КИИ*** **]**
Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	**Контроль/мониторинг технологического оборудования (оборудование сети электросвязи),** **оказание услуг связи, управление [** ***указывается в случае наличия и использования данного функционала*** **]**
Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной) протоколов взаимодействия	**Тип доступа: Проводной, беспроводной.** **Технология доступа: xDSL, FE, P2P fiber.** **Протокол взаимодействия: протоколы стека TCP/IP** **[** ***может быть уточнено по решению оператора связи*** **]**

4. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

Наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя, эксплуатирующего объект	**[** ***Ввести сквозную нумерацию эксплуатантов*** **]** ***1. Наименование оператора связи*** **[** ***если оператор связи сам эксплуатирует объект КИИ*** **]** ***2. Название юридического лица*** **[** ***если оно эксплуатирует объект КИИ*** **].** ***3. Фамилия, имя, отчество индивидуального предпринимателя*** **[** ***если он эксплуатирует объект КИИ*** **]**
Адрес местонахождения юридического лица или адрес места жительства индивидуального предпринимателя, эксплуатирующего объект	**[** ***Указывается последовательно с учетом введенной в п. 4.1. сквозной нумерации эксплуатантов*** **]** ***1. Адрес:*** ***–название улицы, номер дома;*** ***–название населенного пункта (города, поселка и т.п.);*** ***–название района;*** ***–название республики, края, области, автономного округа (области);*** ***–почтовый индекс***
Элемент (компонент) объекта, который эксплуатируется лицом (центр обработки данных, серверное оборудование, телекоммуникационное оборудование, технологическое, производственное оборудование (исполнительные устройства), иные элементы (компоненты) **4.4. ИНН лица, эксплуатирующего объект и КПП**	**[** ***Указывается последовательно с учетом введенной в п. 4.1. сквозной нумерации эксплуатантов*** **]** ***1. Элементы:*** ***< Биллинг-платформа >*** ***< Пребиллинг-платформа >*** ***< Веб-сервер >*** ***< АРМ пользователя >*** ***< иные компоненты >*** **[** ***указываются в случае наличия*** **]** ***2. Элементы: …***

5. Сведения о программных и программно-аппаратных средствах, используемых на объекте КИИ

Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, технологического, производственного оборудования (исполнительных устройств), иных средств) и их количество	***Наименования программно-аппаратных средств и их количество (шт.)***
Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	***Наименование общесистемного программного обеспечения***
Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	***Наименования прикладных программ***
Применяемые средства защиты информации (в том числе встроенные в общесистемное, ППО) (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки или сведения об отсутствии средств защиты информации).	**Наименования средств защиты информации (< *номер и дата выдачи сертификата(ов) соответствия* > или < *номер и дата документа, содержащего результаты оценки соответствия* > или < *оценка соответствия не проводилась* >).** **Функции идентификации и аутентификации, управления доступом, регистрации событий, резервного копирования, отказоустойчивости, обеспечения целостности обрабатываемой информации** ***иные функции* [*указываются в случае наличия*]**

6. Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта КИИ

Категория нарушителя (внешний или внутренний), краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации	**Внешние и внутренние нарушители, оснащенные в т.ч. средствами, сделанными на заказ, с компетенцией профессионалов, со знанием чувствительной информации и с достаточной мотивацией для реализации угроз безопасности информации**
Основные угрозы безопасности информации или обоснование их неактуальности	**1. Угрозы создания нештатных режимов работы.** **2. Угрозы доступа (проникновения) в операционную среду.** **1. Угрозы непосредственного доступа.** **1. Угрозы, реализуемые в ходе загрузки ОС.** **2. Угрозы, реализуемые после загрузки ОС, независимо от того, какая программа запускается пользователем.** **3. Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ.** **2. Угрозы удаленного доступа (сетевые атаки).** **1. Анализ сетевого трафика.** **2. Сканирование сети.** **3. «Парольная» атака.** **4. Подмена доверенного объекта сети.** **5. Навязывание ложного маршрута.** **6. Внедрение ложного объекта сети.** **7. Отказ в обслуживании.** **8. Удаленный запуск приложений.** **3. УБИ.88**

7. Возможные последствия в случае возникновения компьютерных инцидентов

Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак (отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта), или обоснование невозможности наступления компьютерных инцидентов	***1. Отказ в обслуживании.*** ***2. Несанкционированный доступ.*** ***3. Утечка данных (нарушение конфиденциальности).*** ***4. Модификация (подмена) данных.*** ***5. Нарушение функционирования технических средств.*** ***6. Несанкционированное использование вычислительных ресурсов объекта*** ***Или*** ***обоснование невозможности наступления компьютерных инцидентов***
Ущерб, который может быть причинен в результате возникновения компьютерных инцидентов, в соответствии с показателями критериев значимости, утверждаемыми в соответствии с пунктом 1 части 2 статьи 6 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" или обоснование отсутствия возможности причинения ущерба вследствие компьютерных инцидентов	**Социальный «Прекращение или нарушение функционирования сети связи» (*количество абонентов, зона обслуживания*).** **Экономический «Возникновение ущерба бюджетам Российской Федерации» (*значения потенциально возможных ущербов бюджетам, тыс. рублей и процент*)** ***< Политический >, < Экологический > или < Для обороны страны, безопасности государства и правопорядка > с соответствующими показателями и значениями [если рассмотрены соответствующие виды негативных последствий]***

8. Категория значимости, которая присвоена объекту КИИ

Категория значимости, которая присвоена объекту КИИ, или сведения об отсутствии необходимости присвоения	***< I категория >*** ***< II категория >*** ***< III категория >*** ***< Отсутствует необходимость присвоения одной из категорий значимости >***
Полученные значения по каждому из показателей критериев значимости с обоснованием или информация о неприменимости показателя к объекту с соответствующим обоснованием **8.3. Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту**	**4. а) Территория, на которой возможно прекращение или нарушение функционирования сети связи:** ***указать наименование субъекта(ов) РФ (зону обслуживания данным объектом КИИ).*** **4. б) Количество людей, для которых могут быть недоступны услуги связи:** ***указать количество абонентов (тысяч).*** **9. а) Снижение доходов федерального бюджета:** ***указать значение потенциально возможного ущерба бюджету в тыс. рублей и процентах.*** **9. б) Снижение доходов бюджета субъекта РФ:** ***указать значение потенциально возможного ущерба бюджету в тыс. рублей и процентах*** **[** ***указываются последовательно для всех субъектов РФ, входящих в зону обслуживания данным объектом КИИ*** **]** **9. в) Не возникает снижение доходов бюджетов государственных внебюджетных фондов вследствие компьютерных атак на объект КИИ** **[** ***Информация о неприменимости остальных показателей, если показатель применим, то требуется указать его и полученное по нему значение*** **]**

9. Организационные и технические меры, применяемые для обеспечения безопасности объекта

Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта)	***Установлена контролируемая зона.*** ***Обеспечен контроль физического доступа к объекту КИИ.*** **Разработаны документы (регламенты, инструкции, руководства):** ***–Название и реквизиты документа;*** ***–Название и реквизиты документа*** ***Иные меры* [*указываются в случае наличия*]**
Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспечению безопасности значимых объектов	– ***идентификация и аутентификация (ИАФ);*** – ***управление доступом (УПД);*** – ***ограничение программной среды (ОПС);*** – ***защита машинных носителей информации (ЗНИ);*** – ***аудит безопасности (АУД);*** – ***антивирусная защита (АВЗ);*** – ***предотвращение вторжений (компьютерных атак) (СОВ);*** – ***обеспечение целостности (ОЦЛ);*** – ***обеспечение доступности (ОДТ);*** – ***защита технических средств и систем (ЗТС);*** – ***защита информационной (автоматизированной) системы и ее компонентов (ЗИС).***

Вопрос № 2

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

Требования к созданию систем безопасности значимых объектов

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 50118
от "22" февраля 2018 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«21» декабря 2017 г. Москва № 235

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

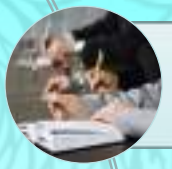
В соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) П Р И К А З Ы В А Ю:

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

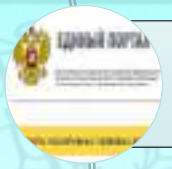
ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

При разработке учтены **лучшие практики** и **зарубежные документы**



При разработке **учтено мнение** ведущих **экспертов**



Прошли **общественное обсуждение**

Согласованы с **Банком России**

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

Зарегистрирован Минюстом России 22 февраля 2018 г. № 50118

Система безопасности значимых объектов

Система безопасности

Правовые меры

Организац. меры

Технические меры

Другие меры

Всех значимых объектов КИИ (филиалов, представительств)

Объекты КИИ субъекта

ИС$_2$	АСУ ТП$_1$	ИТКС$_1$ (знач.)
…	АСУ ТП$_2$ (знач.)	ИТКС$_2$
Ис$_n$ (знач.)	…	…
	АСУ ТП$_l$	ИТКС$_m$ (знач.)

Создается в целях обеспечения устойчивого функционирования значимых объектов критической информационной инфраструктуры при проведении в отношении них компьютерных атак

Состав системы безопасности значимых объектов

С учетом филиалов, представительств

- **подразделения (работники) субъекта КИИ, ответственные за обеспечение безопасности значимых объектов КИИ;**
- **иные подразделения (работники), участвующие в обеспечении безопасности значимых объектов КИИ, включая:**
  - **подразделения (работников), эксплуатирующие (эксплуатирующих) значимые объекты КИИ,**
  - **подразделения (работников), обеспечивающие (обеспечивающих) функционирование (сопровождение, обслуживание, ремонт) значимых объектов КИИ**

программные и программноаппаратные средства, применяемые для обеспечения безопасности значимых объектов

разрабатываются субъектами критической информационной инфраструктуры в соответствии с Требованиями

Задачи системы безопасности значимых объектов

предотвращение неправомерного доступа к информации, обрабатываемой значимыми объектами

недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимых объектов

восстановление функционирования значимых объектов

ГОССОПКА

непрерывное взаимодействие с ГосСОПКА

Силы системы безопасности значимых объектов

определяет состав и структуру системы безопасности, а также функции ее участников при обеспечении безопасности значимых объектов

руководитель субъекта КИИ

организация – лицензиат (ТЗИ или ТЗКИ)

создает систему безопасности, организует и контролирует ее функционирование, а также принимает меры по ее совершенствованию

уполномоченное лицо

должны быть ознакомлены с организационно-распорядительными документами по безопасности значимых объектов

подразделения, эксплуатир. значимые объекты

должны обеспечивать безопасность эксплуатируемых ими значимых объектов

подразделения, обеспечивающ. функционир. значимых объектов

осуществляют свои функции в соответствии с правилами безопасности, установленными организационно-распорядительными документами

подразделение, ответственное за обеспечение безопасности значимых объектов

выполняют только задачи, определенные в должностных регламентах и связанные с обеспечением безопасности значимых объектов или обеспечением ИБ субъекта КИИ

Функции структурного подразделения по безопасности

- ✓ разработка предложений по совершенствованию организационно-распорядительных документов по безопасности значимых объектов и представление их руководителю субъекта КИИ (уполномоченному лицу);
- ✓ проведение анализа угроз безопасности информации в отношении значимых объектов и выявление уязвимостей в них;
- ✓ обеспечение реализации требований по обеспечению безопасности значимых объектов;
- ✓ обеспечение в соответствии с требованиями по обеспечению безопасности значимых объектов реализации организационных мер и применения средств защиты информации, эксплуатации средств защиты информации;
- ✓ осуществление реагирования на компьютерные инциденты;
- ✓ организация проведения оценки соответствия значимых объектов требованиям по безопасности;
- ✓ подготовка предложений по совершенствованию функционирования систем безопасности, а также по повышению уровня безопасности значимых объектов;
- ✓ обладание знаниями и навыками, необходимыми для обеспечения безопасности значимых объектов;
- ✓ прохождение повышения уровня знаний по вопросам обеспечения безопасности КИИ и о возможных угрозах безопасности информации не реже одного раза в год.

Средства системы безопасности значимых объектов

Прошли оценку соответствия в форме обязательной сертификации, приемки или испытаний

В приоритетном порядке применяются встроенные в ОПО и СПО СЗИ

Применяются в соответствии с эксплуатационной документацией

Должна быть обеспечена поддержка СЗИ

Должны быть учтены возможные ограничения со стороны разработчика

Должны обеспечивать реализацию технических мер обеспечения безопасности

встроенные в общесистемное, прикладное программное обеспечение средства защиты информации

межсетевые экраны

средства обнаружения (предотвращения) вторжений

средства антивирусной защиты

средства (системы) контроля (анализа) защищенности

средства управления событиями безопасности

средства защиты каналов передачи данных

Требования к организационно-распорядительным документам по безопасности значимых объектов

Организационно-распорядительные документы по безопасности значимых объектов должны определять:

- ✓ цели и задачи обеспечения безопасности значимых объектов
- ✓ основные угрозы безопасности информации и категории нарушителей
- ✓ основные организационные и технические мероприятия по обеспечению безопасности значимых объектов
- ✓ состав и структуру системы безопасности и функции ее участников
- ✓ порядок применения, формы оценки соответствия значимых объектов и СЗИ

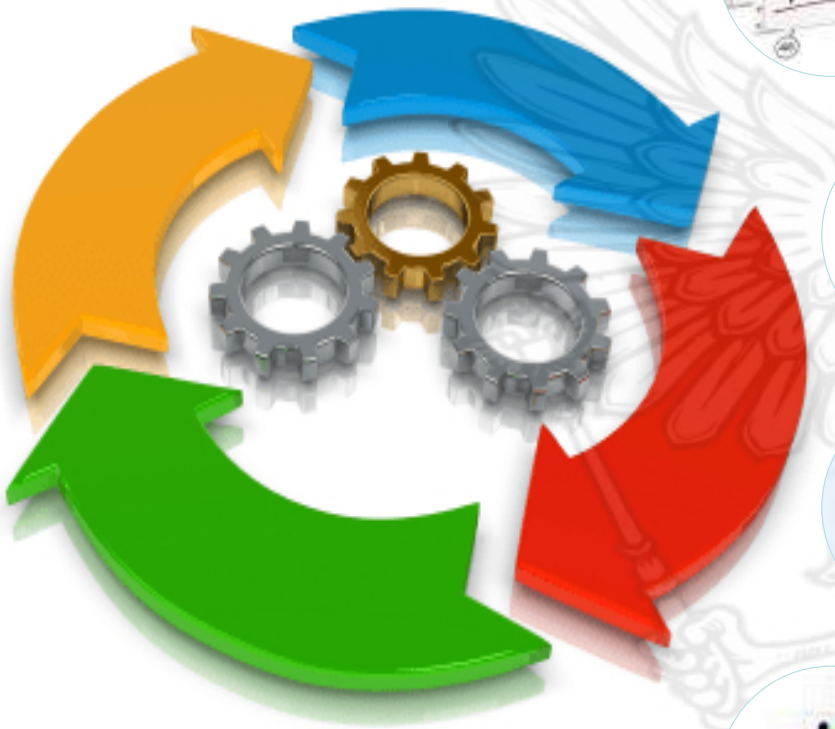
- ✓ правила безопасной работы работников субъекта КИИ на значимых объектах
- ✓ действия работников субъекта КИИ при возникновении компьютерных инцидентов и иных нештатных ситуаций

- ✓ планы мероприятий по обеспечению безопасности значимых объектов
- ✓ порядок реализации отдельных мер по обеспечению безопасности значимых объектов
- ✓ порядок проведения испытаний или приемки средств защиты информации
- ✓ порядок реагирования на компьютерные инциденты
- ✓ порядок информирования и обучения работников субъекта КИИ
- ✓ порядок взаимодействия подразделений (работников) субъекта КИИ при решении задач обеспечения безопасности значимых объектов
- ✓ порядок взаимодействия субъекта КИИ с ГосСОПКА

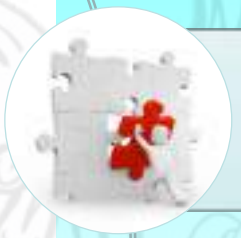
Являются частью документов по вопросам обеспечения информационной безопасности (защиты информации) субъекта КИИ, доводятся в части касающейся

Состав и формы документов определяются субъектом КИИ

Требования к функционированию системы безопасности значимых объектов



планирование и разработка мероприятий по обеспечению безопасности значимых объектов



реализация (внедрение) мероприятий по обеспечению безопасности значимых объектов

контроль состояния безопасности значимых объектов

совершенствование безопасности значимых объектов

Планирование и разработка мероприятий по обеспечению безопасности значимых объектов

Утверждаю
руководитель субъекта КИИ

План мероприятий по обеспечению безопасности значимых объектов

Мероприятие № 1

Наименование мероприятия.
Срок исполнения мероприятия.
Наименования подразделений (работников), ответственных за реализацию мероприятия.

…

Мероприятие № n

Наименование мероприятия.
Срок исполнения мероприятия.
Наименования подразделений (работников), ответственных за реализацию мероприятия.

Разрабатывается не менее чем на 1 год
Доводится до подразделений в части, их касающейся

Разрабатывается структурным подразделением по безопасности с участием подразделений, эксплуатирующих значимые объекты и подразделений, обеспечивающих их функционирование

Включаются мероприятия по обеспечению функционирования системы безопасности, а также организационные и технические мероприятия по обеспечению безопасности значимых объектов, направленные на решение задач системы обеспечения безопасности

Контроль за выполнением плана мероприятий осуществляется структурным подразделением по безопасности

Подразделение по безопасности ежегодно готовит отчет о выполнении плана мероприятий, который представляется руководителю субъекта КИИ

Может быть включен в общий план деятельности субъекта КИИ в качестве отдельного раздела

Порядок разработки, утверждения и внесения изменений в план мероприятий определяется в организационно-распорядительных документах по безопасности значимых объектов

Реализация (внедрение) мероприятий по обеспечению безопасности значимых объектов

Выполнение плана мероприятий

В соответствии с организационно-распорядительными документами

Принятие мер

Организационных	**Применение СЗИ**

Документирование результатов

В соответствии с организационно-распорядительными документами

Контроль состояния безопасности значимых объектов

Проводится ежегодно

Внутренний контроль организации работ по обеспечению безопасности значимых объектов и эффективности принимаемых организационных и технических мер

Внешняя оценка (внешний аудит) состояния безопасности значимых объектов

Проводит **комиссия**, назначаемая субъектом КИИ, **в состав** которой **входят работники структурного подразделения по безопасности, работники подразделений, эксплуатирующих значимые объекты, и подразделений, обеспечивающих их функционирование**

Проводят **организации**, имеющие **лицензии на деятельность в области ЗИ (в части услуг по контролю защищенности информации от НСД и ее модификации в средствах и системах информатизации)**

Акт, подписываемый членами комиссии и утверждаемый руководителем субъекта (уполномоченным лицом)

Выявленные замечания подлежат устранению в порядке и сроки, установленные руководителем субъекта КИИ (уполномоченным лицом)

Совершенствование безопасности значимых объектов

Осуществляется структурным подразделением по безопасности, специалистами по безопасности с участием подразделений (работников), эксплуатирующих значимые объекты, и подразделений (работников), обеспечивающих функционирование значимых объектов

Проведение анализа

- функционирования системы безопасности
- состояния безопасности значимых объектов

Разработка предложений

- по развитию системы безопасности
- по мерам по совершенствованию безопасности значимых объектов

Предложения представляются руководителю субъекта КИИ

Предложения могут быть внесены в план мероприятий (по решению руководителя субъекта КИИ)

Новые требования
(вступают в силу с 1 января 2021 г.)

Руководитель структурного подразделения по безопасности должен иметь:

1. Высшее профессиональное образование по направлению подготовки (специальности) в области информационной безопасности или иное высшее профессиональное образование по направлению подготовки (специальности) в указанных областях и пройти обучение по программам профессиональной переподготовки по направлению «Информационная безопасность» **(со сроком обучения не менее 360 часов)**
2. Стаж работы в сфере информационной безопасности не менее 3 лет.

Штатные работники структурного подразделения по безопасности, штатные специалисты по безопасности должны иметь:

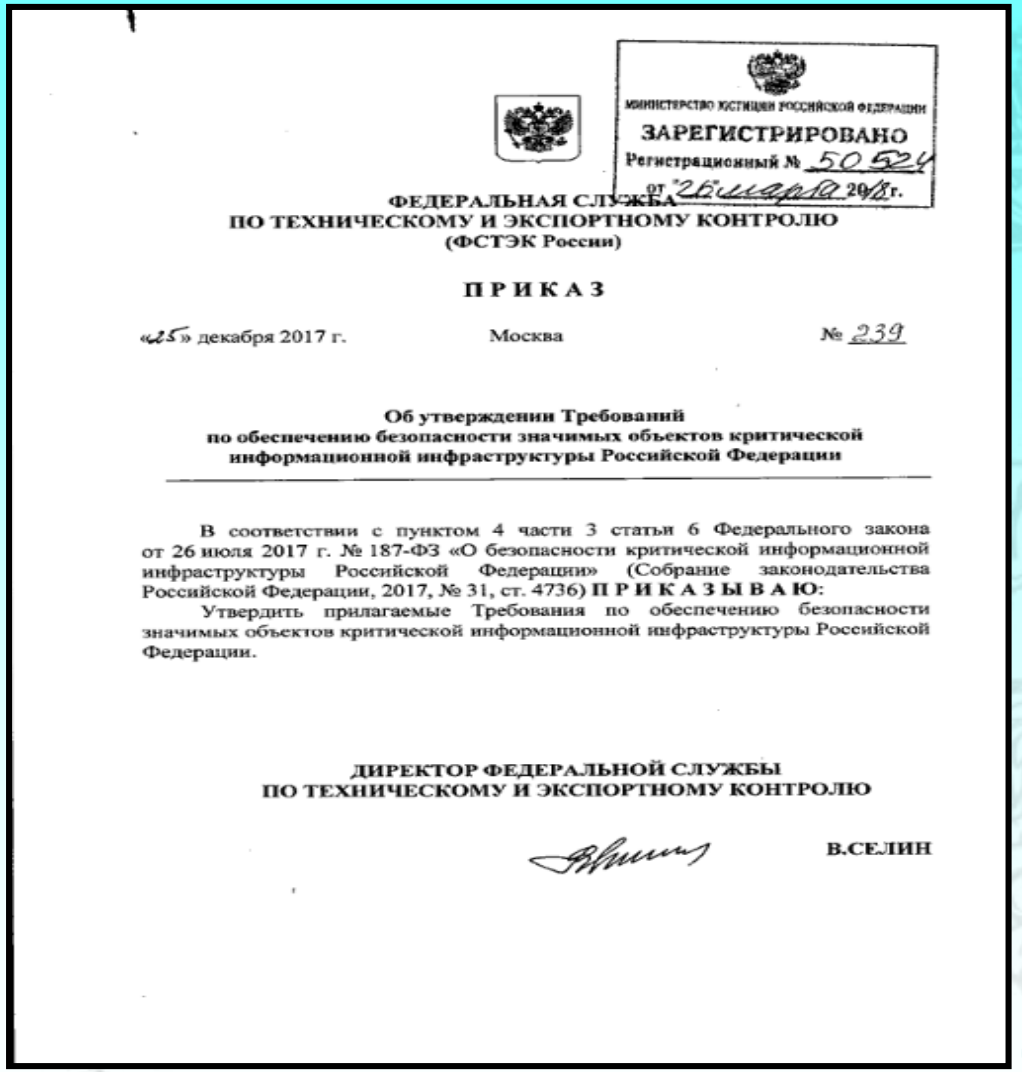
1. Высшее профессиональное образование по направлению подготовки (специальности) в области информационной безопасности или иное высшее профессиональное образование по направлению подготовки (специальности) в указанных областях и пройти обучение по программам профессиональной переподготовки по направлению и пройти обучение по программам повышения квалификации «Информационная безопасность» **(со сроком обучения не менее 72 часов)**

Обучение про программам повышения квалификации по направлению «Информационная безопасность» (не реже 1 раза в 5 лет)

Вопрос № 3

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

Требования по обеспечению безопасности значимых объектов



МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
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

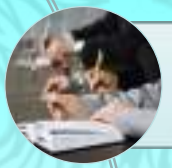
В соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) **П Р И К А З Ы В А Ю:**

Утвердить прилагаемые Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

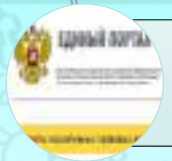
ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

При разработке учтен **опыт применения приказов № 17, № 21, № 31**



При разработке **учтено мнение** ведущих **экспертов**



Прошли **общественное обсуждение**

Согласованы с **Минкомсвязью России**

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

Зарегистрирован Минюстом России 26 марта 2018 г. № 50524

Требования по обеспечению безопасности значимых объектов

Обеспечение безопасности значимых объектов, в которых обрабатывается информация, составляющая государственную тайну

Обеспечение безопасности значимых объектов, являющихся государственными информационными системами

Обеспечение безопасности значимых объектов, являющихся информационными системами персональных данных

Обеспечения безопасности значимых объектов, являющихся информационно-телекоммуникационными сетями

Приказ ФСТЭК России
от 25 декабря 2017 г. № 239

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

Законодательство РФ о государственной тайне

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Постановление Правительства РФ от 1 ноября 2012 г. № 1119

Нормативные правовые акты Минкомсвязи России

Формы оценки соответствия СЗИ и подтверждения соответствия значимого объекта

Оценка соответствия средств защиты информации

Сертификация

Применяется в случаях, установленных **законодательством РФ** и по **решению субъекта КИИ**

Испытания

Приемка

В **иных случаях** и проводятся **самостоятельно** или с **привлечением организаций-лицензиатов**

Подтверждение соответствия значимого объекта

Аттестация

В случаях, если значимый объект – **ГИС** в **соответствии с законодательством РФ** и **по решению субъекта КИИ**

Приемочные испытания

В иных случаях

Соответствие категории и класса средства защиты информации

Категория значимости объекта	Класс защиты средства защиты информации и уровни доверия	
1	4	или более высокому уровню доверия
2	5	или более высокому уровню доверия
3	6	или более высокому уровню доверия

Во всех категориях значимых объектов - средства вычислительной техники не ниже 5 класса,
В значимых объектах 1 и 2 категорий – СЗИ, программное
обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей

Объекты защиты на значимых объектах

Информационно-телекоммуникационная сеть

- передаваемая информация
- телекоммуникационное оборудование
- средства защиты информации
- архитектура и конфигурация

Автоматизированная система управления

- данные о параметрах управляемого объекта (процесса)
- программно-аппаратные средства
- программные средства
- средства защиты информации
- архитектура и конфигурация

Информационная система

- обрабатываемая информация
- программно-аппаратные средства
- программные средства
- средства защиты информации
- архитектура и конфигурация

Состав мер по обеспечению безопасности значимого объекта КИИ

- Аудит безопасности (АУД)
- Реагирование на инциденты информационной безопасности (ИНЦ)
- Управление конфигурацией (УКФ)
- Управление обновлениями программного обеспечения (ОПО)
- Планирование мероприятий по обеспечению безопасности (ПЛН)
- Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)
- Информирование и обучение персонала (ИПО)
- Идентификация и аутентификация (ИАФ)
- Управление доступом (УПД)
- Ограничение программной среды (ОПС)
- Защита машинных носителей информации (ЗНИ)
- Антивирусная защита (АВЗ)
- Предотвращение вторжений (компьютерных атак) (СОВ)
- Обеспечение целостности (ОЦЛ)
- Обеспечение доступности (ОДТ)
- Защита технических средств и систем (ЗТС)
- Защита информационной (автоматизированной) системы (сети) и ее компонентов (ЗИС)

Этапы реализации требований по обеспечению безопасности значимых объектов 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

Формирование требований к обеспечению безопасности значимого объекта

Формирование требований

Категорирование объекта КИИ

Требования к обеспечению безопасности

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

Техническое задание на создание значимого объекта и (или) техническое задание на создание подсистемы безопасности

Положения организационно-распорядительных документов по обеспечению безопасности значимых объектов

- **Цель и задачи обеспечения безопасности**
- **Категория значимости объекта**
- **Перечень документов разработки**
- **Перечень защищаемых информационных ресурсов (объектов защиты)**
- **Требования к организационным мерам и средствам защиты информации**
- **Стадии (этапы работ) создания подсистемы безопасности**
- **Требования к организационным мерам и средствам защиты информации**
- **Требования к защите обеспечивающей инфраструктуры**
- **Требования к информационному взаимодействию значимого объекта**

Этапы реализации требований по обеспечению безопасности значимых объектов 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

Разработка организационных и технических мер по обеспечению безопасности значимого объекта

РАЗРАБОТКА ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР

- **Моделирование угроз**
- **Проектирование подсистемы безопасности**
- **Разработка эксплуатационной документации**

Модель угроз безопасности информации

1. **Описание архитектуры**
2. **Описание угроз**
   - 2.1. Выявление источников угроз
   - 2.2. Потенциальные уязвимости
   - 2.3. Способы реализации угроз
   - 2.4. Последствия от реализации угроз

Разработка организационных и технических мер по обеспечению безопасности значимого объекта

РАЗРАБОТКА ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР

- **Моделирование угроз**
- **Проектирование подсистемы безопасности**
- **Разработка эксплуатационной документации**

Макетирование подсистемы безопасности

- **Определение субъектов доступа и объектов доступа**
- **Определение политики управления доступом**
- **Обоснование организационных и технических мер**
- **Определение видов и типов средств защиты информации**
- **Определение структуры подсистемы безопасности**
- **Выбор средств защиты информации**
- **Требования к параметрам настройки программных и программно-аппаратных средств**
- **Определение мер при информационном взаимодействии**

Проектная документация на значимый объект (подсистему безопасности)

Разработка организационных и технических мер по обеспечению безопасности значимого объекта

РАЗРАБОТКА ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР

- Моделирование угроз
- Проектирование подсистемы безопасности
- Разработка эксплуатационной документации

Эксплуатационная документация

- **Структура подсистемы безопасности значимого объекта**
- **Состав, места установки, параметры и порядок настройки средств защиты информации, программного обеспечения и аппаратных средств**
- **Правила эксплуатации средств защиты информации значимого объекта**

Этапы реализации требований по обеспечению безопасности значимых объектов 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

Внедрение организационных и технических мер по обеспечению безопасности значимого объекта

ВНЕДРЕНИЕ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР

- **Установка и настройка средств защиты информации** → **Ограничения на эксплуатацию средств защиты информации**
- **Разработка документов по безопасности значимого объекта**
  1. Правила и процедуры реализации отдельных организационных и (или) технических мер
  2. Правила безопасной работы работников субъекта
  3. Действия работников субъекта КИИ при возникновении компьютерных инцидентов и иных нештатных ситуаций
  4. ……
- **Предварительные испытания значимого объекта**
- **Опытная эксплуатация значимого объекта**
- **Выявление уязвимостей**
- **Приемочные испытания**

Внедрение организационных и технических мер по обеспечению безопасности значимого объекта

ВНЕДРЕНИЕ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР

Предварительные испытания	**Программа и методика предварительных испытаний**	**Проверка работоспособности подсистемы безопасности** **Влияние подсистемы безопасности на штатный режим функционирования**
Опытная эксплуатация	**Программа и методика опытной эксплуатации**	**Проверка функционирования подсистемы безопасности** **Реализация организационных и технических мер** **Готовность пользователей и администраторов**
Выявление уязвимостей	**Уязвимости кода, конфигурации и архитектуры значимого объекта**	**Подтверждение отсутствия уязвимостей, содержащихся в банке данных угроз**

Внедрение организационных и технических мер по обеспечению безопасности значимого объекта

ВНЕДРЕНИЕ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР

Приемочные испытания

Программа и методика приемочных испытаний

Акт приемки значимого объекта в эксплуатацию

Ввод в действие

ИЛИ

Аттестат соответствия

- **Модель угроз**
- **Результаты выявления уязвимостей**
- **Результаты предварительных испытаний**
- **Эксплуатационная документация**
- **Акт категорирования**
- **Документы по безопасности**

Этапы реализации требований по обеспечению безопасности значимых объектов 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

Обеспечение безопасности значимого объекта в ходе его эксплуатации

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЗНАЧИМОГО ОБЪЕКТА В ХОДЕ ЕГО ЭКСПЛУАТАЦИИ

- Планирование мероприятий по обеспечению безопасности значимого объекта
- Периодический анализ угроз безопасности информации на значимом объекте и рисков от их реализации
- Управление (администрирование) подсистемой безопасности значимого объекта
- Управление конфигурацией значимого объекта и его подсистемой безопасности
- Реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта
- Обеспечение действий в нештатных (непредвиденных) ситуациях в ходе эксплуатации значимого объекта
- Информирование и обучение персонала значимого объекта
- Контроль за обеспечением уровня безопасности значимого объекта

Обеспечение безопасности значимого объекта в ходе его эксплуатации

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В ХОДЕ ЭКСПЛУАТАЦИИ

Планирование мероприятий по обеспечению безопасности объекта

- Определение лиц, ответственных за планирование и контроль мероприятий по обеспечению безопасности
- Разработка, утверждение и актуализация плана мероприятий
- Контроль выполнения мероприятий по обеспечению безопасности значимого объекта, предусмотренных утвержденным планом

Обеспечение действий в нештатных ситуациях при эксплуатации объекта

- Планирование мероприятий
- Обучение и отработка действий персонала
- Создание альтернативных мест хранения информации
- Резервирование программно-аппаратных средств
- Обеспечение возможности восстановления объекта

Контроль за обеспечением уровня безопасности объекта

- Мониторинг событий безопасности
- Документирование процедур и результатов контроля
- Контроль (анализ) защищенности значимого объекта
- Анализ и оценка функционирования значимого объекта

Этапы реализации требований по обеспечению безопасности значимых объектов 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

Обеспечение безопасности значимого объекта при выводе его из эксплуатации

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЗНАЧИМОГО ОБЪЕКТА ПРИ ВЫВОДЕ ЕГО ИЗ ЭКСПЛУАТАЦИИ

Архивирование информации, содержащейся в значимом объекте → **Дальнейшее использование информации в деятельности субъекта**

Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации → **1. Передача машинного носителя информации**
2. Ремонт, техническое обслуживание

Реализация Федерального закона от 26 июня 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Начальник 1 отдела Управления ФСТЭК России по Южному и Северо-Кавказскому федеральным округам

Чернов Николай Иванович

Телефон: (863) 200-75-25

СПАСИБО ЗА ВНИМАНИЕ!