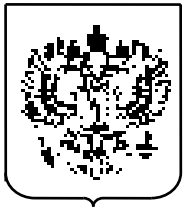
Текущее состояние объектов, отнесенных к критической информационной инфраструктуре:

статистика, требования, перспективы

Изменения, внесенные в Правила категорирования, перечень показателей и их значений



Постановление Правительства Российской Федерации
от 13 апреля 2019 г.
№ 452

«О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»

Установлен срок утверждения перечня объектов, подлежащих категорированию, **1 сентября 2019 г.**

Вводится понятие **Постоянно действующая** комиссия по категорированию

Установлена **причина пересмотра** установленных категорий значимости или решений об отсутствии необходимости присвоения объектам таких категорий **изменение показателей критериев значимости объектов критической информационной инфраструктуры или их значений**

Порядок категорирования объектов критической информационной инфраструктуры

Форма представления сведений
(в редакции приказа ФСТЭК России от 21 марта 2019 г. № 59)

Приказ ФСТЭК России
от 22 декабря 2017 г. № 236
(в редакции приказа ФСТЭК России от 21 марта 2019 г. № 59)

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

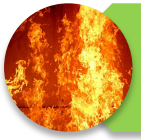
1. Сведения об объекте КИИ

2. Сведения о субъекте КИИ

3. Сведения о взаимодействии объекта КИИ и сетей электросвязи

4. Сведения о лице, эксплуатирующем объект КИИ

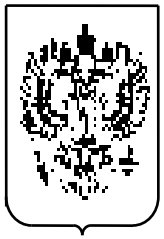
5. Сведения о программных и программно-аппаратных средствах, используемых на КИИ



7. Возможные последствия в случае возникновения компьютерных инцидентов на объекте КИИ

9. Категория значимости, которая присвоена объекту КИИ, сведения об отсутствии необходимости присвоения категории, а также сведения о результатах оценки показателей

Требования к созданию систем безопасности
(в редакции приказа ФСТЭК России от 27 марта 2019 г. № 64)



Приказ ФСТЭК России
от 21 декабря 2017 г. № 235
(в редакции приказа ФСТЭК России от 27 марта 2019 г. № 64)

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

Внесены требования к организации работ по обеспечению безопасности значимых объектов КИИ, эксплуатируемых в филиалах, представительствах, обособленных структурных подразделениях, а также дочерних и зависимых обществах субъекта КИИ

Требование к периодичности контроля состояния безопасности значимых объектов КИИ изменено **с «ежегодно» на «не реже, чем раз в 3 года»**

С 1 января 2021 г. требования к специалистам по безопасности:

руководитель подразделения – профильное высшее профессиональное образование или иное ВПО и профессиональная переподготовка по ИБ (не менее 360 часов), а также стаж в сфере ИБ не менее 3 лет;

иные специалисты – профильное ВПО или иное ВПО и повышение квалификации (не менее 72 часов);

повышение квалификации не реже, чем раз в 5 лет

Требования к системам безопасности значимых объектов КИИ (Приказ ФСТЭК России от 21 декабря 2017 г. № 235)

Программные и программно-аппаратные средства, применяемые для обеспечения безопасности значимых объектов КИИ:

- СЗИ, в том числе СЗИ от НСД (включая встроенные в общесистемное, прикладное программное обеспечение)
- Межсетевые экраны
- Средства обнаружения (предотвращения) вторжений (компьютерных атак)
- Средства антивирусной защиты
- Средства (системы) контроля (анализа) защищенности
- Средства управления событиями безопасности
- Средства защиты каналов передачи данных

Требования к системам безопасности значимых объектов КИИ (Приказ ФСТЭК России от 21 декабря 2017 г. № 235)

Программные и программно-аппаратные средства, применяемые для обеспечения безопасности значимых объектов КИИ:

Средства должны пройти оценку соответствия

в случае, если объектом КИИ обрабатывается государственная тайна или объект КИИ представляет собой государственную информационную систему, сертификация обязательна

в приоритетном порядке применяются встроенные в рабочие системы специальные программные СЗИ

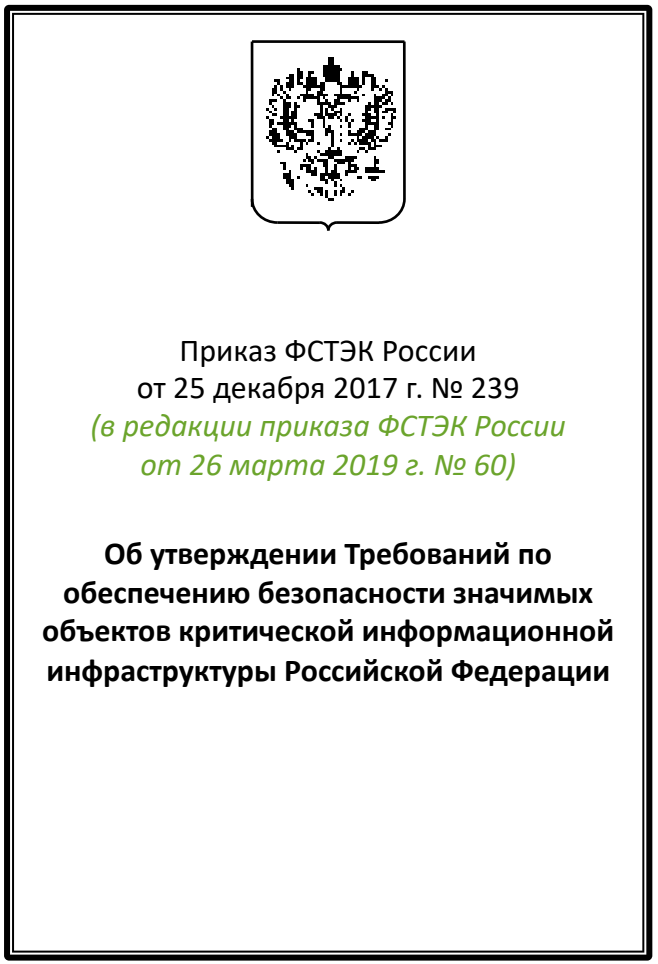
СЗИ должны применяться в соответствии с эксплуатационной документацией и обязательно сопровождаться поддержкой со стороны разработчика

При создании системы также должны учитываться возможные ограничения самого разработчика, например, запрет использования средства на определённых объектах

порядок применения СЗИ определяется субъектом КИИ в организационно-распорядительных документах по безопасности значимых объектов с учетом особенностей деятельности субъекта КИИ

Требования по обеспечению безопасности значимых объектов КИИ

(в редакции приказа ФСТЭК России от 26 марта 2019 г. № 60)



Приказ ФСТЭК России
от 25 декабря 2017 г. № 239
(в редакции приказа ФСТЭК России от 26 марта 2019 г. № 60)

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

Понятие «СЗИ, прошедшие проверку на отсутствие недекларированных возможностей» изменено на «СЗИ, соответствующие уровню доверия»

Установлено требование по размещению на территории Российской Федерации входящих в состав ЗО КИИ 1 категории программных и программно-аппаратных средств хранения и обработки информации

Уточнены некоторые меры защиты.
Вместо понятия «разработка политики» используется «регламентация правил и процедур»

Требования к системам безопасности значимых объектов КИИ (Приказ ФСТЭК России от 25 декабря 2017 г. № 239)

- 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 системы и ее компонентов (ЗИС)
- Планирование мероприятий по обеспечению безопасности
- Управление конфигурацией (УКФ)
- Управление обновлениями программного обеспечения (ОПО)
- Реагирование на инциденты информационной безопасности (ИНЦ)
- Обеспечение действий в нештатных ситуациях (ДНС)
- Информирование и обучение персонала (ИПО)

Требования к системам безопасности значимых объектов КИИ (Приказ ФСТЭК России от 25 декабря 2017 г. № 239)

В значимом объекте НЕ допускаются:

Наличие удаленного доступа непосредственно (напрямую) к программным и программно-аппаратным средства, в том числе СЗИ, для обновления или управления со стороны лиц, не являющихся работниками субъекта КИИ

Наличие локального бесконтрольного доступа к программным и программно-аппаратным средствам, в том числе СЗИ, для обновления или управления со стороны лиц, не являющихся работниками субъекта КИИ

Передача информации, в том числе технологической информации, разработчику (производителю) программно-аппаратных средств, в том числе СЗИ, или иным лицам без контроля со стороны субъекта КИИ

Как работать с КИИ на удалёнке?

1. Проведение инструктажа работников о правилах безопасного удаленного взаимодействия с такими объектами;
2. Определение перечня средств вычислительной техники, которые будут предоставлены работникам для удаленной работы;
3. Определение перечня информации и информационных ресурсов, к которым будет предоставляться удаленный доступ;
4. Назначение минимально необходимых прав и привилегий пользователям при удаленной работе;
5. Идентификация удаленных средств вычислительной техники по MAC-адресам на серверах, предоставление доступа к информационным ресурсам методом «белого списка»
6. Исключение возможности эксплуатации удаленных СВТ посторонними лицами
7. Выделение в отдельный домен работников на «удаленке»
8. Обеспечение двухфакторной аутентификации работников
9. Организация защищенного доступа к серверам с применением средств криптографической защиты информации
10. Применение антивирусной защиты, ежедневное обновление баз антивируса
11. Исключение возможности установки работником стороннего ПО
12. Обеспечение мониторинга безопасности, в том числе ведение журналов регистрации действий работников и их анализ
13. Блокирование сеанса удаленного доступа при неактивности более установленного субъектом КИИ времени
14. Обеспечение возможности оперативного реагирования и принятия мер защиты при возникновении инцидентов

Ответственность

Ответственность возлагается на должностных лиц субъекта КИИ:

- Руководитель субъекта КИИ
- Уполномоченное лицо
- Лица, эксплуатирующие значимые объекты
- Лица, обеспечивающие функционирование значимых объектов
- Лица, обеспечивающие безопасность значимых объектов

УК РФ
Ст. 274.1. Неправомерное воздействие на КИИ РФ

До 10 лет лишения свободы
Невыполнение требований по безопасности КИИ, в случае наступления инцидента с тяжкими последствиями или их угрозой

До 6 лет лишения свободы
Невыполнение требований по безопасности КИИ, нарушение правил эксплуатации

До 10 лет лишения права занимать определенные должности
Ч. 3, 4, 5 ст. 274.1 УК РФ

КоАП РФ
Ст. 19.5.

До 20 000 рублей
Административный штраф
Невыполнение предписания регулятора об устранении нарушения законодательства

+ Проект ФЗ «О внесении изменений в КоАП РФ»

Статистика

Январь 2019 г. - по оценке ФСТЭК России в России **12 000 субъектов** КИИ и **180 000 объектов** КИИ

Октябрь 2019 г. - в реестре объектов КИИ более **45 000 объектов в 20 500 субъектах**

Исходя из ОКВЭД в Архангельской области **1433** организации, ведущие деятельность в сферах, отнесенных к КИИ

Отличники категорирования КИИ:
Здравоохранение, ТЭК, ВПК, металлургия, банки

Перспективы

Изменения в КоАП:

Предусмотрены штрафы:

- за нарушение порядка категорирования ОКИИ,
- за нарушение требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры
- за нарушение требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры
- за нарушение порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры
- за нарушение порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры

Перспективы

Непредставление сведений, предусмотренных законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

1. **Непредставление или нарушение сроков** представления сведений о результатах присвоения объекту критической информационной инфраструктуры РФ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, влечет наложение административного штрафа на должностных лиц в размере **от десяти тысяч до пятидесяти тысяч рублей**; на юридических лиц – **от пятидесяти тысяч до ста тысяч рублей**.

2. **Непредставление или нарушение порядка** либо сроков представления в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации информации, влечет наложение административного штрафа на должностных лиц в размере **от десяти тысяч до пятидесяти тысяч рублей**; на юридических лиц – **от ста тысяч до пятисот тысяч рублей**.

Спасибо за внимание!

ООО «Шартрез»
Архангельск, Новгородский, 32, офис 501
Архангельск, Новгородский, 32, сектор В, офис 310

8 (8182) 424-764

Наш сайт: https://shartrez.com/
Мы в VK: https://vk.com/shartrezco/
Мы в Instagram: https://www.instagram.com/shartrezco/
Мы в Facebook: https://www.facebook.com/ShartrezCo/
Наш информационный блог: https://shartrezco.blogspot.com/

SHARTREZ
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ