Актуальные вопросы реализации требований законодательства Российской Федерации о безопасности критической информационной инфраструктуры

Начальник отдела Управления ФСТЭК России по Дальневосточному федеральному округу

Изменения в правила категорирования объектов КИИ и в перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений

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»**

***(изменения внесены постановлениями Правительства РФ
от 13 апреля 2019 г. № 452,
от 24 декабря 2021 г. № 2431,
от 19 августа 2022 № 1463,
от 20 декабря 2022 г. № 2360)***

постановление Правительства Российской Федерации от 24 декабря 2021 г. № 2431

Статья 19.1 Направление новых сведений в случае изменения сведений об объекте КИИ (20 раб. дней)

Статья 19.2 Мониторинг отраслевыми ОГВ представления субъектами КИИ актуальных и достоверных сведений об объектах КИИ

постановление Правительства Российской Федерации от 19 августа 2022 г. № 1463

Статья 19.3 К мониторингу могут привлекаться подведомственные организации (имеющие лицензии по ТЗИ, ТЗКИ) в части оценки актуальности и достоверности сведений

постановление Правительства Российской Федерации от 20 декабря 2022 г. № 2360

1) Уточнение процедуры мониторинга представления сведений об объектах КИИ
2) Изменения показателей критериев значимости объектов КИИ и их значений

Изменения в Кодекс Российской Федерации об административных правонарушениях

Федеральный закон
от 30 декабря 2001 г. № 195-ФЗ

Кодекс
Российской Федерации
об административных
правонарушениях

Статья 19.7.15. Непредставление сведений, предусмотренных законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

Федеральным законом от 19 декабря 2022 г. № 518-ФЗ внесенные изменения.

Ответственность за непредставление или нарушение сроков предоставления…сведений, представление недостоверных сведений

влечет наложение административного штрафа:
на должностных лиц в размере от 10 тыс. до 50 тыс. руб.;
на юридических лиц – от 50 тыс. до 100 тыс. руб.

Ответственность за повторное совершение административного правонарушения

влечет наложение административного штрафа:
на должностных лиц в размере от 50 тыс. до 100 тыс. руб.;
на юридических лиц – от 100 тыс. до 200 тыс. руб.

Отраслевые перечни типовых объектов критической информационной инфраструктуры

УТВЕРЖДАЮ

Заместитель Министра транспорта

Российской Федерации

_____ Д.В. Баканов

«15» 05 2023 г.

Перечень типовых отраслевых объектов критической информационной инфраструктуры, функционирующих в сфере транспорта

№ п/п	Типовые отраслевые объекты КИИ (ИС, ИТКС, АС)	Виды деятельности, для обеспечения которых используется объект (в соответствии с ОКВЭД)	Осуществляемые критические процессы типовым отраслевым объектом КИИ
Сфера транспорта			
1	Автоматизированные системы, предназначенные для управления интроскопами.	49 – Деятельность сухопутного и трубопроводного транспорта. 50 – Деятельность водного транспорта. 51 – Деятельность воздушного и космического транспорта.	Обнаружение радиоактивных веществ, взрывчатых веществ, оружия, боеприпасов, патронов к оружию, взрывных устройств, элементов взрывных устройств, а также других предметов и веществ, вносимых на территорию объекта транспортной инфраструктуры.
2	Автоматизированные системы, предназначенные для управления техническими средствами обеспечения транспортной безопасности.	52.2 – Деятельность транспортная вспомогательная.	Обеспечение доступа к данным с технических средств обеспечения транспортной безопасности, а также передача таких данных в соответствии с установленными требованиями. Управление техническими средствами и силами обеспечения транспортной безопасности.
Сфера воздушного транспорта			
3	Автоматизированные системы, предназначенные для управления аэропортом.	51.10 – Деятельность пассажирского воздушного транспорта. 51.21 – Деятельность грузового воздушного транспорта.	Планирование потребностей ресурсов аэропорта. Управление графиками смен. Планирование и учет использования материальных ресурсов и работы персонала, требуемых

Приказ ФСТЭК России от 22 февраля 2020 г. № 35

Приказ
ФСТЭК России
от 22 февраля 2020 г. № 35

«О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом ФСТЭК России от 25 декабря 2017 г. № 239»

С 1 января 2023 г. вступили в силу:

Требования к оценки соответствия средств защиты информации, проводимой в форме испытаний или приемки

Требования безопасности к прикладному ПО, планируемого к внедрению в рамках создания (модернизации или реконструкции, ремонта) значимого объекта КИИ

Приказ ФСТЭК России от 20 апреля 2023 г. № 69

Приказ
ФСТЭК России
от 20 апреля 2023 г. № 69

«О внесении изменений в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом ФСТЭК России от 21 декабря 2017 г. № 235»

(Зарегистрирован 23 июня 2023 г. № 73969)

Замена «уполномоченного лица» руководителя субъекта КИИ по вопросам ОБ ЗО КИИ на «заместителя руководителя субъекта КИИ», на которого возложены полномочия по обеспечению информационной безопасности

Изменение требований к уровню подготовки

Исключение требований к сроку обучения по программам профессиональной переподготовки (повышения квалификации)

Повышение периодичности прохождения обучения по программам повышения квалификации (вместо одного раза в 5 лет на один раз в 3 года)

Допуск к ОБ ЗО КИИ работников со средним профессиональным образованием по специальности в области информационной безопасности

Реализация орг. и тех. мер блокирующих УБИ при использовании средств защиты информации, не имеющих техническую поддержку со стороны разработчика

Руководство по организации процесса управления уязвимостями в органе (организации)

Утвержден ФСТЭК России
17 мая 2023 г.

Методический документ

Руководство по организации процесса управления уязвимостями в органе (организации)

Требования по обеспечению безопасности значимых объектов КИИ Российской Федерации

Обеспечение безопасности значимого объекта в ходе его эксплуатации

13.2. В ходе анализа УБИ в значимом объекте и возможных последствий их реализации осуществляются:

а) анализ уязвимостей значимого объекта, возникающих в ходе его эксплуатации

22. В значимых объектах должны быть реализованы следующие орг. и тех. меры:

V. Аудит безопасности (АУД)

АУД.0 - Регламентация правили процедур аудита безопасности

АУД.2 - Анализ уязвимостей и их устранение

Методические документы ФСТЭК России от 28 октября 2022 г.

Утвержден ФСТЭК России
28 октября 2022 г.

Методический документ

Методика тестирования обновлений безопасности программных, программно-аппаратных средств

Утвержден ФСТЭК России
28 октября 2022 г.

Методический документ

Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств

Полномочия управления ФСТЭК России по Дальневосточному федеральному округу

информационное сообщение ФСТЭК России от 18 июня 2021 г. № 240/82/1037

↓

Здравоохранение

↓

С 1 мая 2021 г.

информационное сообщение ФСТЭК России от 18 декабря 2021 г. № 240/81/2547

↓

Наука, ОПК

↓

С 1 января 2022 г.

информационное сообщение ФСТЭК России от 28 июня 2022 г. № 240/83/1698

↓

Энергетика, ТЭК

↓

С 1 июля 2022 г.

информационное сообщение ФСТЭК России от 28 апреля 2023 г. № 240/82/818

↓

Связь

↓

С 1 мая 2023 г.

Рассмотрение (подготовка предложений по корректировке) **перечней объектов КИИ**, подлежащих категорированию

Проверка соблюдения порядка осуществления **категорирования** и правильности присвоения объектам КИИ одной из категорий значимости либо неприсвоения им ни одной из таких категорий на основании представляемых субъектами КИИ сведений

Недостатки, выявляемые при рассмотрение перечней объектов КИИ и сведений о результатах категорирования

1. В перечне объектов КИИ указывается **не точная дата категорирования** объектов КИИ (Пример: ноябрь 2022 г., 2023 г. и пр.)

2. В перечень объектов КИИ **не включаются объекты КИИ**, подлежащие категорированию (Пример: станок с ЧПУ, компьютеризованное медицинское оборудование, локальная сеть, и пр.)

3. В сведениях о результатах категорирования **не конкретизирована информация** о применяемых на объекте КИИ программно-аппаратных средствах, общесистемном и прикладном ПО

4. Сведения о результатах категорирования **содержат противоречивую информацию** об объекте КИИ в части его: назначения, архитектуры, взаимодействии с сетями электросвязи, программных и программно-аппаратных средств

5. При категорировании **не рассматриваются внутренние нарушители** безопасности информации либо при наличии подключения к внешним сетям электросвязи не рассматриваются внешние нарушители

Недостатки, выявляемые при рассмотрение перечней объектов КИИ и сведений о результатах категорирования

6. При категорировании не рассматривается наихудший сценарий проведения компьютерных атак, а так же взаимодействие объекта КИИ с другими объектами КИИ

7. В сведениях о результатах категорирования не указываются рассчитанные значения по каждому из показателей критериев значимости, а также не указывается информация о неприменимости показателя критерия значимости к объекту КИИ либо указываются частично не по всем показателей критериев значимости объектов КИИ

8. В сведениях о результатах категорирования обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту КИИ не раскрывает причину присвоения одной из категорий значимости или неприменимости показателя критерия значимости к объекту КИИ

9. При расчете показателей критериев значимости не учитываются изменения, внесенные в перечень показателей критериев значимости объектов КИИ Российской Федерации и их значений 20 декабря 2022 г.

10. Перечни объектов КИИ и сведениях о результатах категорирования представляются не утвержденными (без даты утверждения и (или) подписи руководителя субъекта КИИ или уполномоченного им лица), а также только в печатном виде либо только в электронном виде. При этом электронный вид представления документов не соответствует установленным форматам («.ods», «.odt»)

Нарушения, выявляемые в ходе государственного контроля в области обеспечения безопасности значимых объектов КИИ

1. Субъектом КИИ проведено **категорирование не всех** принадлежащих ему **объектов КИИ**

2. **Фактический состав** компонентов значимых объектов КИИ **не в полной мере соответствует** составу, указанному в сведениях о результатах категорирования

3. **Не определены** состав и структура **системы безопасности значимого объекта КИИ**, а также функции ее участников при обеспечении его безопасности

4. **Не определено** структурное подразделение или **не назначены** отдельные работники, ответственные за обеспечение безопасности значимых объектов КИИ

5. **Не реализовано** внедрение подсистемы безопасности значимых объектов КИИ

6. **Уровень подготовки** работников, ответственных за обеспечение безопасности значимых объектов КИИ, **не соответствует** установленным **требованиям**

7. **Не проводятся мероприятия** по повышению уровня знаний работников по вопросам обеспечения безопасности КИИ и возможных угроз безопасности информации

Нарушения, выявляемые в ходе государственного контроля в области обеспечения безопасности значимых объектов КИИ

8. На заместителя руководителя субъекта КИИ не возложены полномочия по обеспечению информационной безопасности, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, а также не определено структурное подразделение, ответственное по данным вопросам

9. Содержание организационно-распорядительных документов по вопросам по обеспечения безопасности значимых объектов КИИ не соответствует установленным Требованиям, а также не конкретизирует вопросы обеспечения безопасности значимых объектов КИИ

10. Документы по безопасности значимых объектов КИИ не доведены до руководства, а также до иных подразделений (работников), участвующих в обеспечении безопасности значимых объектов КИИ

11. Модель угроз безопасности информации значимого объекта КИИ не разработана

12. Не разработан план реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак

13. Не разработан план мероприятий по обеспечению безопасности значимых объектов КИИ

Нарушения, выявляемые в ходе государственного контроля в области обеспечения безопасности значимых объектов КИИ

14. Отдельные мероприятия, включенные в планы мероприятий по безопасности значимых объектов КИИ, в установленные сроки не реализуются. Результаты реализации мероприятий по обеспечению безопасности значимых объектов КИИ не задокументированы

15. Внутренний контроль организации работ по обеспечению безопасности значимых объектов КИИ и эффективности принимаемых организационных и технических мер или внешняя оценка (внешний аудит) состояния безопасности значимых объектов КИИ не осуществляется

16. Оценка эффективности принятых организационных и технических мер по обеспечению безопасности значимых объектов КИИ не проводится

17. На значимом объекте КИИ применяются средства защиты информации, не прошедшие оценку на соответствие требованиям безопасности в формах обязательной сертификации, испытаний или приемки

18. На значимом объекте КИИ применяются программные и программно-аппаратные средства, средства защиты информации, не обеспеченные технической поддержкой, при этом не реализуются компенсирующие меры блокирующие УБИ

19. Не реализуются организационные и технические меры по обеспечению безопасности значимых объектов КИИ

Обеспечение безопасности значимого объекта КИИ в ходе его эксплуатации