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

Начальник отдела Управления ФСТЭК России по Дальневосточному федеральному округу

06.02.2024

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

Федеральный закон
от 26 июля 2017 г. № 187-ФЗ

«О безопасности критической информационной инфраструктуры Российской Федерации»

Федеральным законом от 10 июля 2023 г. № 312-ФЗ внесенные изменения

Статья 2 пункт 8

Добавлена сфера

государственная регистрация прав на недвижимое имущество и сделок с ним

Перечни типовых отраслевых объектов критической информационной инфраструктуры

Правила категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденные Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127

10. Исходными данными для категорирования являются:

ж) перечни типовых отраслевых объектов критической информационной инфраструктуры, которые могут формироваться государственными органами и российскими юридическими лицами, выполняющими функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, по согласованию с ФСТЭК России

(пп. "ж" введен Постановлением Правительства РФ от 20.12.2022 N 2360)

- **Сфера транспорта**
- **Сфера энергетики**
- **Сфера топливно-энергетического комплекса**
- **Горнодобывающая промышленность (*в части руд, камней*)**
- **Химическая промышленность**
- **Сфера здравоохранения**
- **Металлургическая промышленность**
- **Оборонная промышленность**

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»

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 технической поддержки со стороны разработчика

Приказ ФСТЭК России от 1 сентября 2023 г. № 177

Приказ
ФСТЭК России
от 1 сентября 2023 г. № 177

«О внесении изменений в Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденный приказом ФСТЭК России от 6 декабря 2017 г. № 227»

Определен номер регистрации в реестре объектов КИИ, функционирующих в сфере государственной регистрации прав на недвижимое имущество и сделок с ним

Определен порядок присвоения регистрационного номера в реестре объектам КИИ, функционирующим одновременно в нескольких сферах либо на территории нескольких федеральных округов

Определен порядок присвоения регистрационного номера в реестре объектам КИИ в случаи их объединения в один объект либо их разделения на несколько объектов

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:

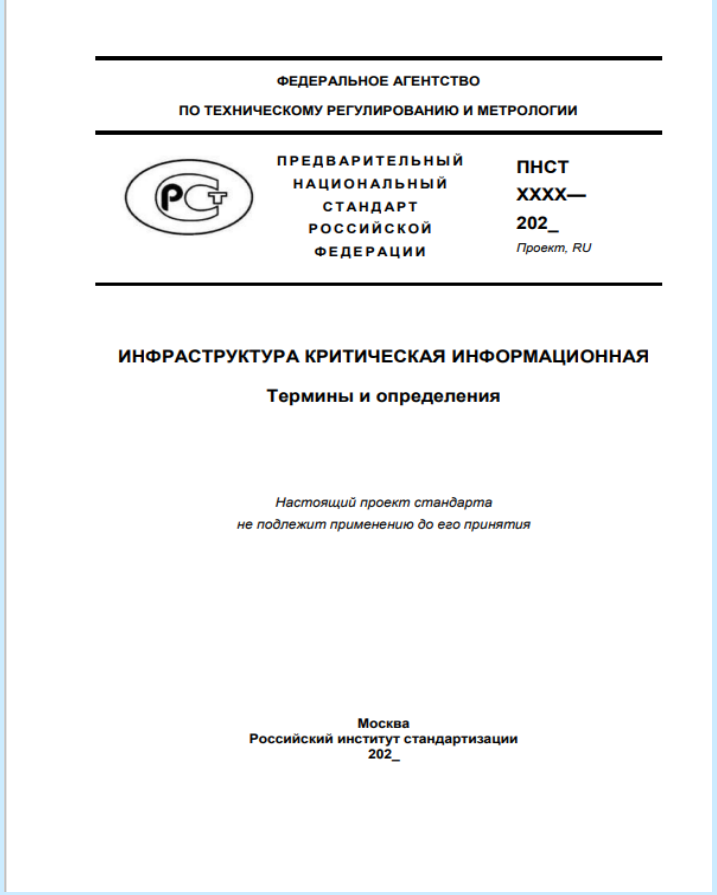
V. Аудит безопасности (АУД)

АУД.0 - Регламентация правили процедур аудита безопасности

АУД.2 - Анализ уязвимостей и их устранение

Проекты национальных стандартов в области критической информационной инфраструктуры

1. Термины и определения



ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ XXXX—202_

Проект, RU

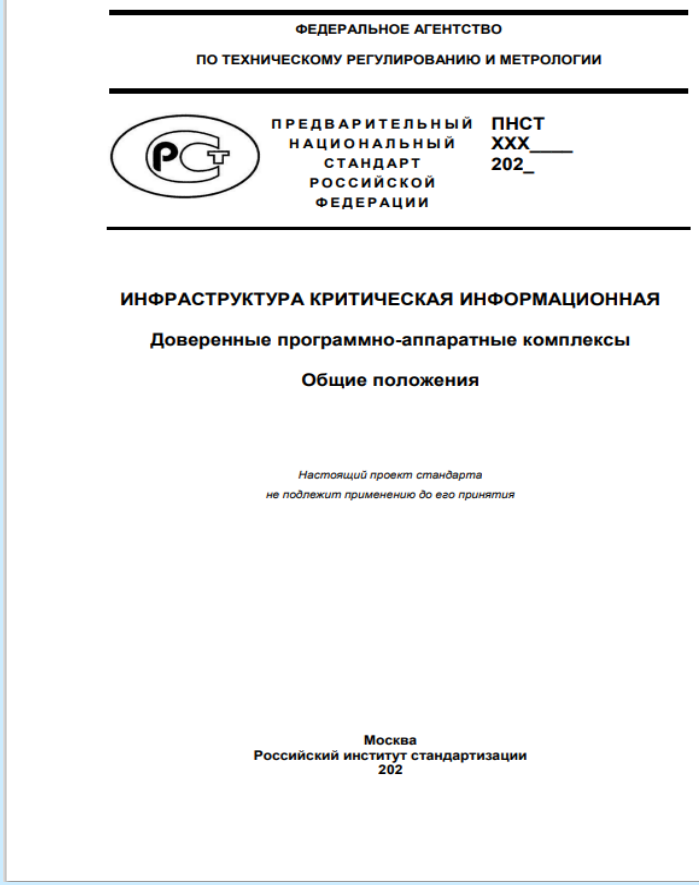
ИНФРАСТРУКТУРА КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ

Термины и определения

Настоящий проект стандарта не подлежит применению до его принятия

Москва
Российский институт стандартизации
202_

2. Доверенные программно-аппаратные комплексы



ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ XXX____202_

ИНФРАСТРУКТУРА КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ

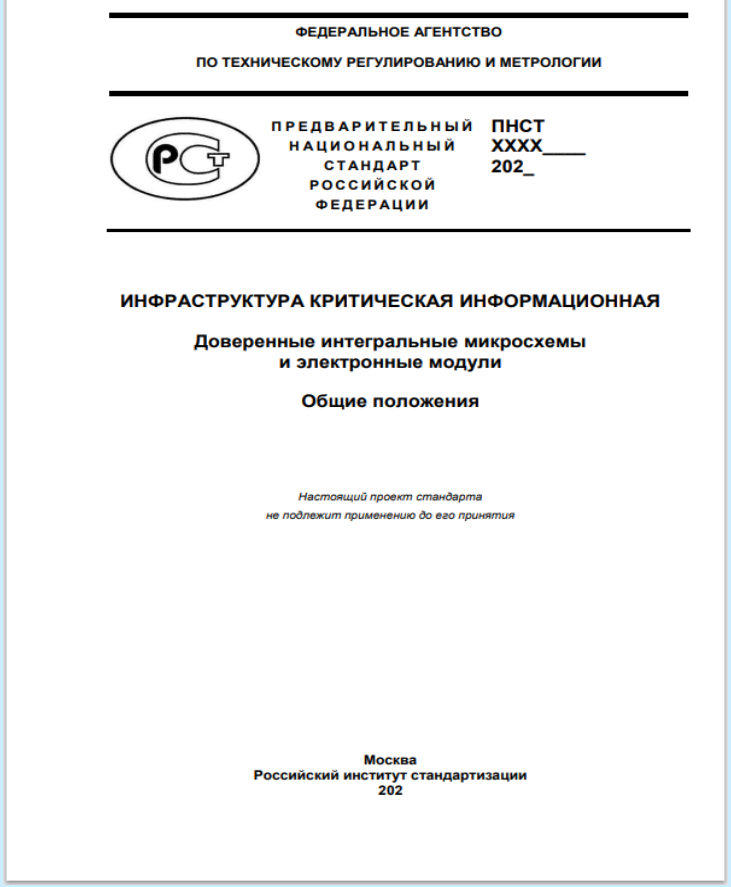
Доверенные программно-аппаратные комплексы

Общие положения

Настоящий проект стандарта не подлежит применению до его принятия

Москва
Российский институт стандартизации
202

3. Доверенные интегральные микросхемы и электронные модули



ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ XXXX____202_

ИНФРАСТРУКТУРА КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ

Доверенные интегральные микросхемы и электронные модули

Общие положения

Настоящий проект стандарта не подлежит применению до его принятия

Москва
Российский институт стандартизации
202

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 рассмотрении 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. При определении объектов КИИ осуществляется неверное разделение объекта при котором нарушается технология обработки информации (выполнения производственного процесса)
(Пример: АСУ разделяется на объект КИИ, представляющий верхний и средний уровень АСУ, и отдельный объект КИИ, представляющий только нижний уровень АСУ)

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

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

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

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

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

8. 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 показателям критериев значимости объектов КИИ

9. 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

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

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

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

3. **Не определены задачи** по обеспечению безопасности значимых объектов КИИ подразделений, эксплуатирующих значимый объект КИИ

4. **Не создана** подсистема безопасности значимых объектов КИИ

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

6. 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, либо **не определено структурное подразделение,** ответственное по данным вопросам

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

7. **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

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

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

10. **Не разработан план мероприятий** по обеспечению безопасности значимых объектов КИИ

11. 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**

12. **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**

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

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

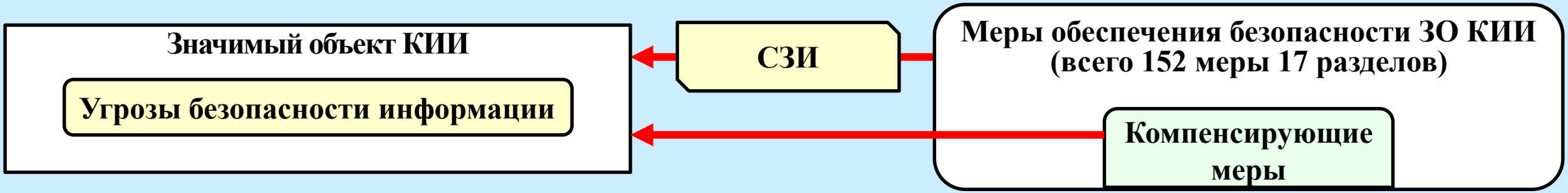
14. На значимом объекте КИИ применяются средства защиты информации, **не прошедшие оценку** на соответствие требованиям безопасности в формах обязательной сертификации, испытаний или приемки

15. 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

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

17. В **документах** по безопасности значимых объектов КИИ **отсутствует обоснование применения компенсирующих мер**

Компенсирующие меры по обеспечению безопасности значимого объекта КИИ



Если принятые меры по обеспечению промышленной, функциональной безопасности и (или) физической безопасности достаточны для блокирования (нейтрализации) отдельных угроз безопасности информации, дополнительные меры, Требований, могут не применяться. При этом должно быть обоснована достаточность применения данных мер по блокирования (нейтрализации) соответствующих угроз безопасности информации

В ходе разработки организационных и технических мер по обеспечению безопасности значимого объекта должно быть обосновано применение компенсирующих мер, а при приемочных испытаниях (аттестации) оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации