Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

Управление ФСТЭК России по Сибирскому федеральному округу

ПРИЩЕНКО Александр Вальтемарович

ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

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

Вступил в силу с 1 января 2018 г.

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

Требования
по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЗАРЕГИСТРИРОВАНО

Регистрационный № *50524*

от *«26» марта* 2018 г.

- **I. Общие положения**
- **II. Требования к обеспечению безопасности значимых объектов в ходе их создания, эксплуатации и вывода из эксплуатации значимых объектов**
- **III. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов**
- **Приложение. Состав мер по обеспечению безопасности и их базовые наборы для соответствующей категории значимого объекта критической информационной инфраструктуры**

I. ОБЩИЕ ПОЛОЖЕНИЯ

ЗНАЧИМЫЕ ОБЪЕКТЫ КИИ

Статья 7
Федерального закона № 187-ФЗ

- **Информационные системы**
- **Автоматизированные системы управления**
- **Информационно-телекоммуникационные сети**

Обеспечение устойчивого функционирования при проведении компьютерных атак

СУБЪЕКТЫ КИИ

- **Государственные органы**
- **Государственные учреждения**
- **Российские юридические лица**
- **Российские индивидуальные предприниматели**

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ

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

Законодательство РФ о государственной тайне

Обеспечение безопасности значимых объектов, являющихся государственными информационными системами

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования по обеспечению безопасности значимых объектов

Обеспечение безопасности значимых объектов, являющихся информационными системами персональных данных

Постановление Правительства РФ от 1 ноября 2012 г. № 1119

Обеспечения безопасности значимых объектов, являющихся информационно-телекоммуникационными сетями

Нормативные правовые акты Минкомсвязи России

РЕАЛИЗАЦИЯ ТРЕБОВАНИЙ

Приказ ФСТЭК России от 25 декабря 2017 г. № 239

ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЭТАПЫ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ КИИ

- **Установление требований к обеспечению безопасности значимого объекта**

- Разработка организационных и технических мер по обеспечению безопасности значимого объекта
- Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие
- Обеспечение безопасности значимого объекта в ходе его эксплуатации
- Обеспечение безопасности значимого объекта при выводе его из эксплуатации
- Меры обеспечения безопасности значимого объекта

УСТАНОВЛЕНИЕ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМОГО ОБЪЕКТА

Задание Требований к обеспечению безопасности

- Категорией значимости значимого объекта
- Перечня показателей критериев значимости объектов КИИ

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

П О С Т А Н О В Л Е Н И Е

от 8 февраля 2018 г. № 127

МОСКВА

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 (частное техническое) на создание подсистемы безопасности значимого объекта

- Цель и задачи обеспечения безопасности
- Категорию значимости объекта
- Перечень НПА, МД и НС
- Перечень типов объектов защиты
- Организационные и технические меры, применяемые для обеспечения безопасности
- Стадии (этапы работ) создания подсистемы безопасности
- Требования к применяемым к программным и ПАС, в т.ч. СЗИ
- Требования к защите средств и систем, обеспечивающих функционирование ЗнО
- Требования к информационному взаимодействию ЗнО с иными объектами КИИ

Положения организационно-распорядительных документов по обеспечению безопасности значимых объектов, разрабатываемых субъектами КИИ

ЭТАПЫ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ КИИ

- Установление требований к обеспечению безопасности значимого объекта
- **Разработка организационных и технических мер по обеспечению безопасности значимого объекта**
- Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие
- Обеспечение безопасности значимого объекта в ходе его эксплуатации
- Обеспечение безопасности значимого объекта при выводе его из эксплуатации

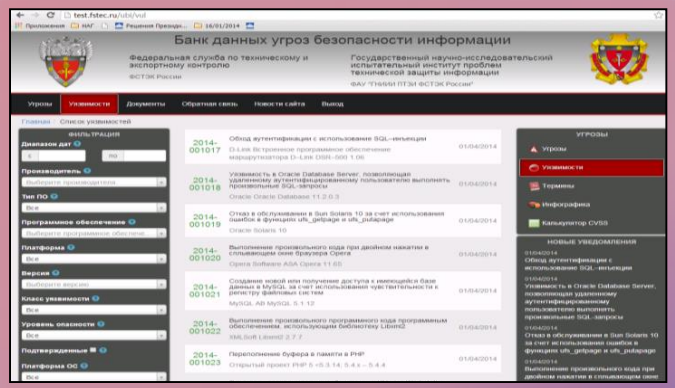
РАЗРАБОТКА ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМОГО ОБЪЕКТА

РАЗРАБОТКА ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР

- Анализ угроз безопасности информации
- Проектирование подсистемы безопасности
- Разработка рабочей (эксплуатационной) документации

Модель угроз безопасности информации

1. **Описание архитектуры значимого объекта**
2. **Анализ угроз безопасности информации**
   - 2.1. Выявление источников угроз БИ и возможностей нарушителей
   - 2.2. Анализ возможных уязвимостей значимого объекта и его программных, ПАС
   - 2.3. Определение возможных способов реализации угроз БИ
   - 2.4. Оценка возможных последствий от реализации угроз БИ



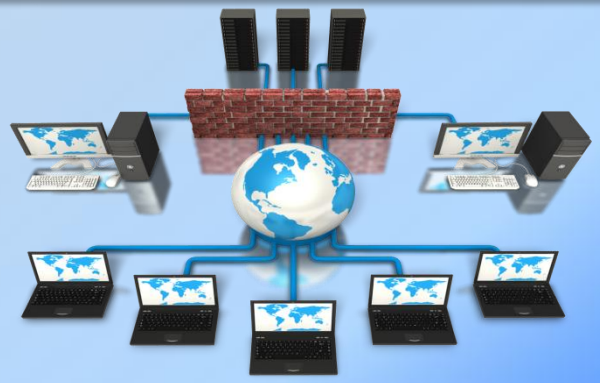
Банк данных угроз безопасности информации

РАЗРАБОТКА ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМОГО ОБЪЕКТА

РАЗРАБОТКА ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР

- Анализ угроз безопасности информации
- Проектирование подсистемы безопасности
- Разработка рабочей (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
- Осуществление выбора СЗИ и их разработка с учетом категории значимости
- Разработка архитектуры подсистемы безопасности
- Определение требований к параметрам настройки программных и ПАС
- Определение мер по обеспечению безопасности при взаимодействии ЗнО с иными объектами КИИ, ИС, АСУ или ИТС

Проектная документация на значимый объект (подсистема безопасности значимого объекта)

РАЗРАБОТКА ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМОГО ОБЪЕКТА

РАЗРАБОТКА ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР

- Анализ угроз безопасности информации
- Проектирование подсистемы безопасности
- Разработка рабочей (эксплуатационной) документации

Проектная документация

ТЗ на создание значимого объекта
и (или)
ЧТЗ на создание подсистемы безопасности значимого объекта

- Описание архитектуры подсистемы безопасности значимого объекта
- Порядок и параметры настройки программных и ПАС, в т.ч. средств защиты информации
- Правила эксплуатации программных и ПАС, в т.ч. средств защиты информации

ЭТАПЫ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ КИИ

- Установление требований к обеспечению безопасности значимого объекта
- Разработка организационных и технических мер по обеспечению безопасности значимого объекта
- **Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие**
- Обеспечение безопасности значимого объекта в ходе его эксплуатации
- 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, настройка программных и ПАС
- Разработка организационно-распорядительных документов по безопасности значимого объекта
- Внедрение организационных мер по обеспечению безопасности значимого объекта
- Предварительные испытания значимого объекта и его подсистемы безопасности
- Опытная эксплуатация значимого объекта и его подсистемы безопасности
- Анализ уязвимостей значимого объекта
- Приемочные испытания значимого объекта и его подсистемы безопасности

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 (в случае их наличия в Эксплуатационной документации)
- **Разработка организационно-распорядительных документов по безопасности значимого объекта** →
  1. **Определять правила и процедуры реализации отдельных организационных и (или) технических мер**
  2. **Устанавливать правила безопасной работы работников значимых объектов**
  3. **Устанавливать действия работников значимых объектов при возникновении нештатных ситуаций, в т.ч. вызванных компьютерными инцидентами**
- Предварительные испытания значимого объекта и его подсистемы безопасности
- Опытная эксплуатация значимого объекта и его подсистемы безопасности
- Анализ уязвимостей значимого объекта
- Приемочные испытания значимого объекта и ввод его в действие

ВНЕДРЕНИЕ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМОГО ОБЪЕКТА

ВНЕДРЕНИЕ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР

Предварительные испытания	Программа и методика предварительных испытаний	1. Проверка работоспособности подсистемы безопасности. 2. Оценка влияния подсистемы безопасности на функционирование ЗнО в проектных режимах его работы
Опытная эксплуатация	Программа и методика опытной эксплуатации	1. Проверка функционирования подсистемы безопасности ЗнО. 2. Реализация организационных и технических мер. 3. Необходимых знаний и умений пользователей и администраторов
Анализ уязвимостей	Уязвимости кода, конфигурации и архитектуры значимого объекта	Подтверждение отсутствия уязвимостей, содержащихся в банке данных угроз безопасности ФСТЭК России

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

- Модель угроз безопасности информации
- Акт категорирования
- ТЗ (ЧТЗ) и Эксплуатационная документация
- Организационно-распорядительные документы
- Результаты анализа уязвимостей ЗнО
- Материалы предварительных испытаний и опытной эксплуатации

ИЛИ

Аттестат соответствия (если ГИС и в иных случаях)

ЭТАПЫ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ КИИ

- Установление требований к обеспечению безопасности значимого объекта
- Разработка организационных и технических мер по обеспечению безопасности значимого объекта
- Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие
- **Обеспечение безопасности значимого объекта в ходе его эксплуатации**
- Обеспечение безопасности значимого объекта при выводе его из эксплуатации

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЗНАЧИМОГО ОБЪЕКТА В ХОДЕ ЕГО ЭКСПЛУАТАЦИИ

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В ХОДЕ ЕГО ЭКСПЛУАТАЦИИ

- **Планирование мероприятий по обеспечению безопасности** значимого объекта
- Анализ угроз безопасности информации в значимом объекте и последствий 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 ситуациях** в ходе эксплуатации значимого объекта
- Информирование и обучение персонала значимого объекта
- **Контроль за обеспечением безопасности** значимого объекта

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЗНАЧИМОГО ОБЪЕКТА В ХОДЕ ЕГО ЭКСПЛУАТАЦИИ

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В ХОДЕ ЭКСПЛУАТАЦИИ

Планирование мероприятий по обеспечению безопасности значимого объекта

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

Обеспечение действий в нештатных (непредвиденных) ситуациях в ходе эксплуатации значимого объекта

- Планирование мероприятий по обеспечению безопасности
- Обучение и отработка действий персонала в случае возникновения нештатных ситуаций
- Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций
- Резервирование программных и ПАС, в т.ч. СЗИ, каналов связи
- Обеспечение возможности восстановления значимого объекта и (или) его компонентов
- Определение порядка анализа возникших нештатных ситуаций и принятия мер по недопущению их возникновения

Контроль за обеспечением уровня безопасности значимого объекта

- Контроль (анализ) защищенности значимого объекта
- Анализ и оценка функционирования ЗнО и его подсистемы
- Документирование процедур и результатов контроля
- Принятие решения по результатам контроля о необходимости доработки (модернизации) его подсистемы безопасности

ЭТАПЫ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ КИИ

- Установление требований к обеспечению безопасности значимого объекта
- Разработка организационных и технических мер по обеспечению безопасности значимого объекта
- Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие
- Обеспечение безопасности значимого объекта в ходе его эксплуатации
- **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 КИИ

Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации. Уничтожение данных об архитектуре и конфигурации

- ➢ Передача машинного носителя информации другому пользователю
- ➢ Ремонт, техническое обслуживание или дальнейшее уничтожение

СОСТАВ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ДЛЯ ЗНАЧИМОГО ОБЪЕКТА

- Идентификация и аутентификация
- Управление доступом
- Ограничение программной среды
- Защита машинных носителей информации
- Аудит безопасности
- Антивирусная защита
- Предотвращение вторжений (компьютерных атак)
- Обеспечение целостности
- Обеспечение доступности
- Защита технических средств и систем
- Защита информационной (автоматизированной) системы (сети) и ее компонентов
- Планирование мероприятий по обеспечению безопасности
- Управление конфигурацией
- Управление обновлениями программного обеспечения
- Реагирование на инциденты информационной безопасности
- Обеспечение действий в нештатных ситуациях
- Информирование и обучение персонала

Состав мер по обеспечению безопасности для значимых объектов соответствующей категории значимости **приведен в Приложении к настоящим Требованиям**
(всего 152 меры по 17 разделам)

СОСТАВ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ДЛЯ ЗНАЧИМОГО ОБЪЕКТА

ВЫБОР МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМОГО ОБЪЕКТА ВКЛЮЧАЕТ:

- **Определение базового набора мер по обеспечению безопасности значимого объекта**
- **Адаптацию базового набора мер по обеспечению безопасности значимого объекта**
- **Дополнение адаптированного набора мер по обеспечению безопасности значимого объекта мерами, установленными иными нормативными правовыми актами в области обеспечения безопасности КИИ Российской Федерации и защиты информации**

СООТВЕТСТВИЕ КАТЕГОРИИ И КЛАССА СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Информационная система

Категория	Класс защиты средства защиты информации
1	4
2	5
3	6

Во всех категориях значимых объектов –
применяются средства вычислительной техники **не ниже 5 класса**.

При этом в значимых объектах 1 и 2 категорий –
применяются сертифицированные СЗИ, прошедшие проверку не ниже чем по **4 уровню контроля отсутствия недекларированных возможностей**

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЗНАЧИМОГО ОБЪЕКТА

В ЗНАЧИМОМ ОБЪЕКТЕ НЕ ДОПУСКАЕТСЯ

- **Наличие удаленного доступа непосредственно (напрямую) к программным и программно-аппаратным средствам, в т.ч. средствам защиты информации, для обновления или управления со стороны лиц, не являющихся работниками субъекта КИИ**
- **Наличие локального бесконтрольного доступа к программным и программно-аппаратным средствам, в т.ч. средствам защиты информации, для обновления или управления со стороны лиц, не являющихся работниками субъекта КИИ**
- **Передача информации, в т.ч. технологической информации, разработчику (производителю) программных и программно-аппаратных средств, в т.ч. средств защиты информации, или иным лицам без контроля со стороны субъекта КИИ**

Спасибо за внимание!

(383) 203-54-13