Определение задач по созданию систем безопасности значимых объектов критической информационной инфраструктуры и разработка мероприятий по безопасности

ИЕ ФСТЭК РС
ЕВ АЛЕКСАН

Приказ ФСТЭК России №235, от 21.12.2017 г.

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О безопасности критической информационной инфраструктуры Российской Федерации

Принят Государственной Думой 12 июля 2017 года

Одобрен Советом Федерации 19 июля 2017 года

Пункт 4 части 3 статьи 6

ФСТЭК России устанавливает требования к созданию систем безопасности таких объектов и обеспечению их функционирования

Пункт 1 статьи 10

В целях обеспечения безопасности значимого объекта КИИ субъект КИИ создает систему безопасности такого объекта и обеспечивает ее функционирование

Об утверждении требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования

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

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ (ФСТЭК России)

ПРИКАЗ

«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.

Внесены изменения Приказом № 64, от 27 марта 2019 г.

Требования к образованию работников структурных подразделений занимающихся обеспечением безопасности значимых объектов КИИ

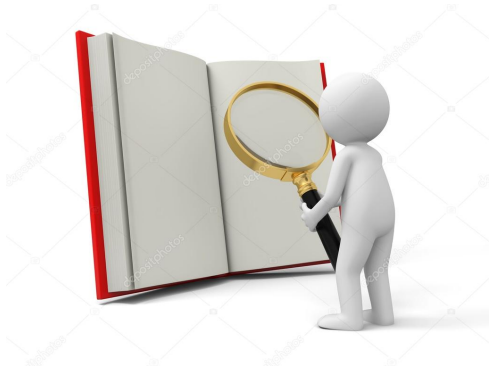
Увеличился срок периодичности контроля с одного года до трех

Структура приказа

Обязателен для исполнения субъектами КИИ имеющими ЗО КИИ

5

РАЗДЕЛОВ



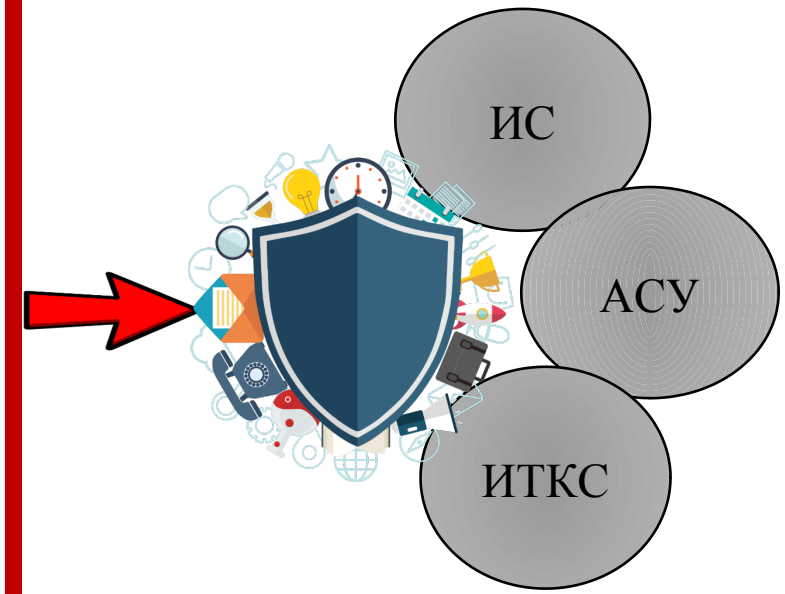
1. Общие положения
2. Требования к силам обеспечения безопасности значимых объектов КИИ
3. Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ
4. Требования к организационно-распорядительным документам по безопасности значимых объектов
5. Требования к функционированию систем безопасности в части организации работ по обеспечению безопасности значимых объектов КИИ

1

Общие положения. Система безопасности

Система безопасности

- Правовые меры
- Организационные меры
- Технические меры
- Другие меры



Создается в целях обеспечения устойчивого функционирования значимых объектов КИИ при проведении в отношении них компьютерных атак

1 Общие положения. 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
Обнаружение. Предупреждение. Ликвидация.

непрерывное взаимодействие с ГосСОПКА

2

Требования к силам обеспечения безопасности значимых объектов КИИ. Состав

Руководитель субъекта (определяет состав и структуру системы безопасности)

Уполномоченное лицо (организует и контролирует функционирование СБ)

Подразделение по безопасности значимого объекта КИИ

ИЛИ

Отдельные работники по безопасности значимого объекта КИИ

Анализ угроз безопасности	239 Приказ ФСТЭК России	
Предложения по улучшению системы	Реагирование на компьютерные инциденты	Защита объектов КИИ в ходе эксплуатации

Не допускается возложение на структурное подразделение по безопасности, специалистов по безопасности функций, не связанных с обеспечением безопасности значимых объектов КИИ или обеспечением информационной безопасности субъекта КИИ в целом

2 Требования к силам обеспечения безопасности значимых объектов КИИ. Образование работников

Работники структурного подразделения должны соответствовать следующим требованиям

Изменения вступят в силу с 01.01.2021 Приказом ФСТЭК России № 64

Руководитель

ВО – Информационная безопасность
Стаж >3 лет

Руководитель

Иное ВО + курс переподготовки по ИБ (360 часов), стаж >3 лет

Штатный специалист

ВО – Информационная безопасность

Штатный специалист

Иное ВО + курс повышения квалификации (72 часа)

Не реже одного раза в пять лет обучение по программам повышения квалификации по направлению «Информационная безопасность»

2 Требования к силам обеспечения безопасности значимых объектов КИИ. Основные моменты

Не допускается возложение функций, не связанных с обеспечением безопасности значимых объектов КИИ

Обязанности, возлагаемые на работников, должны быть определены в их должностных инструкциях

Работники, эксплуатирующие и обеспечивающие функционирование значимого объекта КИИ, выполняют свои обязанности, в соответствии с установленными организационно-распорядительными документами

Субъект КИИ, должен проводить не реже одного раза в год организационные мероприятия, направленные на повышение уровня знаний работников по вопросам ОБ КИИ и о возможных угрозах безопасности информации

3 Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности ЗО КИИ

СЗИ встроенные в ПО и программно-аппаратные средства

Сертификат соответствия или приемочные испытания (**профиль защиты**)

Применяются в соответствии **с эксплуатационной документацией**

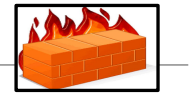
Техническая поддержка СЗИ

Должны быть **учтены** возможные **ограничения на применение СЗИ** со стороны разработчика

Реализация технических мер

средства защиты информации от несанкционированного доступа

межсетевые экраны



средства обнаружения (предотвращения) вторжений

средства антивирусной защиты

средства управления событиями безопасности

средства защиты каналов передачи данных

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4093

Внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации 13 февраля 2019 г.

Выдан 13 февраля 2019 г.
Действителен до: 13 февраля 2024 г.

Настоящий сертификат удостоверяет, что **программно-аппаратный комплекс ViPNet xHttpwall 4**, разработанный и производимый ОАО «ИнфоТеКС», является межсетевым экраном, соответствует требованиям по безопасности информации, установленным в документах «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016) и «Профиль защиты межсетевых экранов типа Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016) при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.00217-01 30 01-ФО.

Сертификат выдан на основании технического заключения от 12.11.2018, оформленного по результатам сертификационных испытаний испытательной лабораторией МОУ «НИИФ» (аттестат аккредитации от 18.11.2016 № СЗИ RU.0001.01БИ00.Б012), и экспертного заключения от 17.01.2019, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 03.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: ОАО «ИнфоТеКС»
Адрес: 127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1
Телефон: (495) 737-6192

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

ИЛИ

Оценка соответствия

4

Требования к организационно-распорядительным документам по безопасности значимых объектов

Организационно-распорядительные документы по безопасности должны определять:

- Цели и задачи обеспечения безопасности значимых объектов
- Основные мероприятия по обеспечению безопасности
- Правила безопасной работы работников субъекта КИИ на значимых объектах
- Действия работников субъекта КИИ при возникновении компьютерных инцидентов и иных нештатных ситуаций

*Состав и формы документов субъект определяет с учетом особенностей его деятельности

4

Пример основного состава организационно-распорядительных документов

- Приказ о структуре системы обеспечения безопасности значимых объектов КИИ
- Приказ о назначении подразделения, ответственного за обеспечение безопасности значимых объектов КИИ
- Приказ о порядке проведения внутреннего контроля состояния обеспечения безопасности значимых объектов КИИ
- Приказ о порядке взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ
- Положение по обеспечению безопасности значимых объектов КИИ
- Положение о подразделении, ответственном за обеспечение безопасности значимых объектов КИИ
- План мероприятий по обеспечению безопасности значимых объектов КИИ

5

Требования к функционированию системы безопасности в части организации работ по обеспечению безопасности ЗО КИИ

ПЛАНИРОВАНИЕ И РАЗРАБОТКА МЕРОПРИЯТИЙ

РЕАЛИЗАЦИЯ (ВНЕДРЕНИЕ) МЕРОПРИЯТИЙ

ЗНАЧИМЫЕ ОБЪЕКТЫ КИИ

ИС, ИТКС, АСУ

КОНТРОЛЬ СОСТОЯНИЯ БЕЗОПАСНОСТИ

СОВЕРШЕНСТВОВАНИЕ БЕЗОПАСНОСТИ

5 Планирование мероприятий по обеспечению безопасности ЗО КИИ

УТВЕРЖДАЮ
Руководитель Субъекта КИИ
И.Фамилия
«___» _____ 2019 г.

ПЛАН
мероприятий по обеспечению безопасности
значимого объекта критической информационной инфраструктуры
на 2020 год

№ П/П	Мероприятия	Исполнитель	Срок проведения	Отметка о выполнении

Начальник структурного подразделения по безопасности И.Фамилия

По решению субъекта КИИ план мероприятий может разрабатываться на более длительный срок

Мероприятия могут включаться в общий план деятельности субъекта КИИ отдельным разделом

План мероприятий предусматривает внедрение организационных и технических мер, а также совершенствование безопасности объекта (выявление новых угроз)

5

Требования к функционированию системы безопасности в части организации работ по обеспечению безопасности ЗО КИИ

Проводится не реже, чем раз в 3 года

Внутренний контроль:
- организации работ по обеспечению безопасности значимых объектов;
- эффективности принимаемых мер

Проводит комиссия, назначаемая субъектом КИИ в составе:
- структурное подразделения (специалист) по безопасности;
- работники, эксплуатирующие и обеспечивающие значимый объект

ИЛИ

Внешняя оценка
(внешний аудит)
состояния безопасности значимых объектов

Проводят организации, имеющие лицензии на деятельность в области защиты информации

Составляется АКТ о выявленных замечаниях, которые подлежат устранению
порядки и сроки устранения замечаний, устанавливаются руководителем субъекта КИИ (уполномоченным лицом)

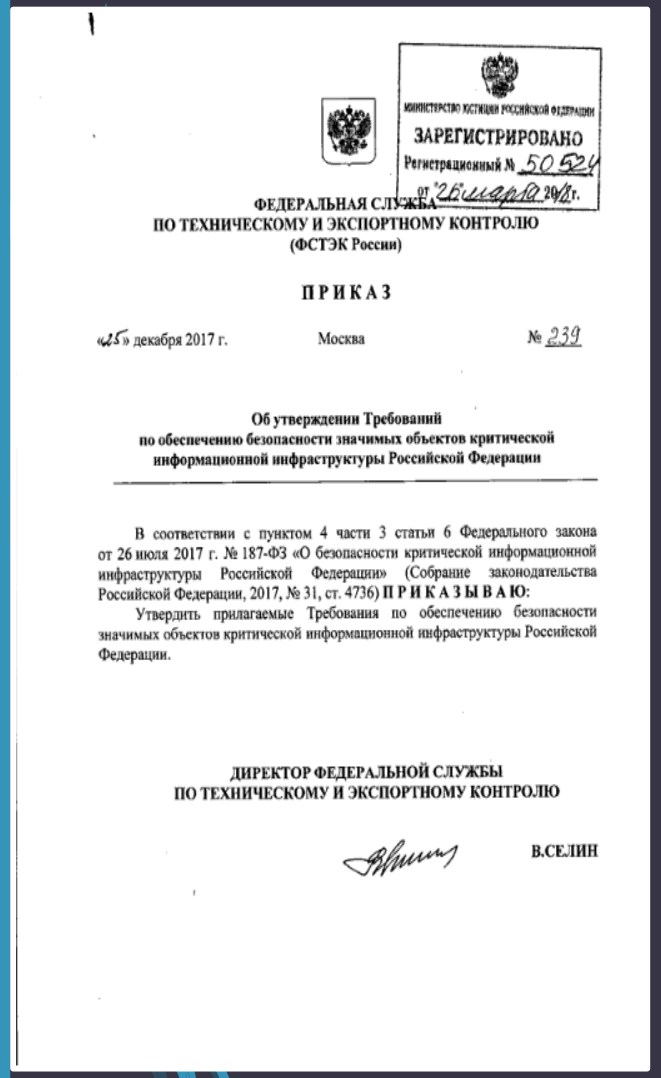
Разработка **мер** по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и порядка их осуществления

Цель обеспечения безопасности значимого объекта

обеспечение его **устойчивого функционирования** в проектных режимах работы в условиях реализации в отношении значимого объекта угроз безопасности информации

ПРИКАЗ
от 25 декабря 2017 г. N 239

Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской федерации



МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 50524
от "26" марта 2018 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

ПРИКАЗ

«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

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

В ходе создания (модернизации), эксплуатации и вывода из эксплуатации проводятся мероприятия по

- ***установлении требований*** к обеспечению безопасности значимого объекта
- разработке ***организационных и технических мер*** по обеспечению безопасности значимого объекта
- ***внедрении*** организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие
- обеспечении безопасности значимого объекта в ***ходе его эксплуатации***
- обеспечении безопасности значимого объекта при ***выводе его из эксплуатации***

Состав и формы документов определяются субъектом критической информационной инфраструктуры

Установление требований к обеспечению безопасности значимого объекта

Исходя из категории значимости объекта критической информационной инфраструктуры формируем

Техническое задание на создание значимого объекта, в соответствии с присвоенной категорией

ГОСТ 34.602-89, с учетом требований приказа ФСТЭК России от 25 декабря 2017 г. N 239

ТЗ должно содержать:

- Цель и задачи
- Категорию
- Перечень НПА, методических документов и НС
- Перечень типов объектов
- Требования к организационным и техническим мерам
- Стадии (этапы, работ) создания подсистемы
- Требования к применяемым П и ПА средствам
- Требования к защите средств и систем, обеспечивающих функционирование
- Требования к информационному взаимодействию
- Требованию к составу и содержанию документации, входе создания ЗО

В ходе создания (модернизации), эксплуатации и вывода из эксплуатации проводятся мероприятия по

установлении требований к обеспечению безопасности значимого объекта

разработке ***организационных и технических мер*** по обеспечению безопасности значимого объекта

внедрении организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие

обеспечении безопасности значимого объекта в ***ходе его эксплуатации***

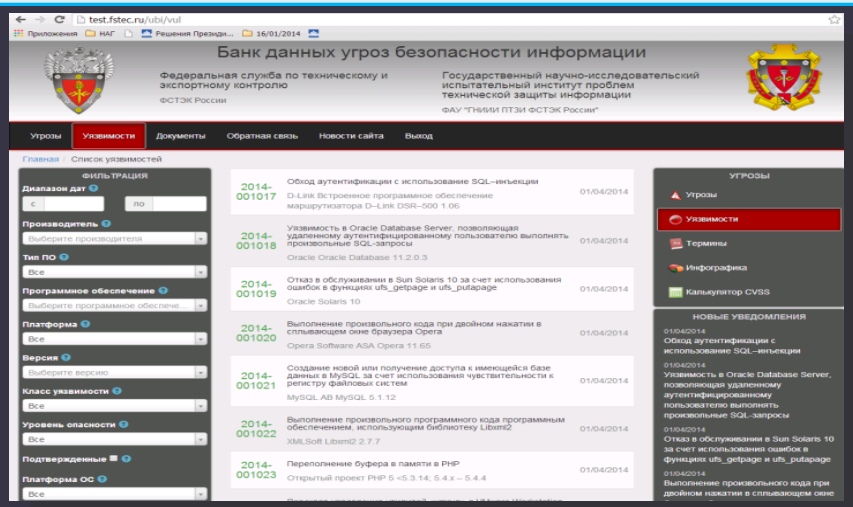
обеспечении безопасности значимого объекта при ***выводе его из эксплуатации***

Состав и формы документов определяются субъектом критической информационной инфраструктуры

Разработка организационных и технических мер по обеспечению безопасности значимого объекта

- анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение (при ее наличии)
- проектирование подсистемы безопасности значимого объекта
- разработку рабочей (эксплуатационной) документации на значимый объект (в части обеспечения его безопасности)

Анализ угроз



http://bdu.fstec.ru

Модель угроз

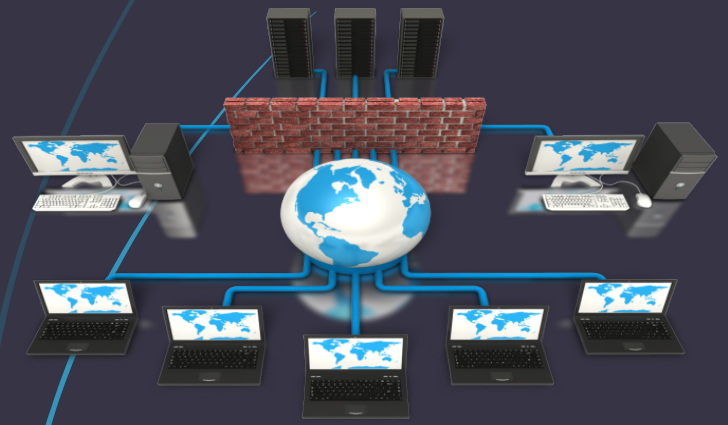
Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России 18 мая 2007 г.

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена ФСТЭК России 14 февраля 2008 г.

Разработка организационных и технических мер по обеспечению безопасности значимого объекта

- анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение (при ее наличии)
- проектирование подсистемы безопасности значимого объекта
- разработку рабочей (эксплуатационной) документации на значимый объект (в части обеспечения его безопасности)

Макетирование подсистемы безопасности



- Определение субъектов доступа и объектов доступа
- Определение политики управления доступом
- Определяются и обосновываются организационные и технические меры
- 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

- анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение (при ее наличии)
- проектирование подсистемы безопасности значимого объекта
- разработку рабочей (эксплуатационной) документации на значимый объект (в части обеспечения его безопасности)

описание архитектуры подсистемы безопасности значимого объекта

порядок и параметры настройки программных и программно-аппаратных средств, в том числе средств защиты информации

правила эксплуатации программных и программно-аппаратных средств, в том числе средств защиты информации (правила безопасной эксплуатации)

В ходе создания (модернизации), эксплуатации и вывода из эксплуатации проводятся мероприятия по

установлении требований к обеспечению безопасности значимого объекта

разработке ***организационных и технических мер*** по обеспечению безопасности значимого объекта

внедрении организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие

обеспечении безопасности значимого объекта в ***ходе его эксплуатации***

обеспечении безопасности значимого объекта при ***выводе его из эксплуатации***

Состав и формы документов определяются субъектом критической информационной инфраструктуры

Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие

- установку и настройку средств защиты информации, настройку программных и программно-аппаратных средств
- разработку организационно-распорядительных документов, регламентирующих правила и процедуры обеспечения безопасности значимого объекта
- внедрение организационных мер по обеспечению безопасности значимого объекта
- предварительные испытания значимого объекта и его подсистемы безопасности
- опытную эксплуатацию значимого объекта и его подсистемы безопасности
- анализ уязвимостей значимого объекта и принятие мер по их устранению
- приемочные испытания значимого объекта и его подсистемы безопасности

ВНЕДРЕНИЕ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР

Приемочные испытания

Программа и методика приемочных испытаний

Акт приемки значимого объекта в эксплуатацию

Ввод в эксплуатацию

ИЛИ

Аттестат соответствия

Акт категорирования

Техническое задание

Модель угроз

Проектная документация

Рабочая документация

Эксплуатационная документация

Результаты выявления уязвимостей

Результаты предварительных испытаний

Организационно-распорядительные документы по безопасности значимых объектов

Документы по безопасности

В ходе создания (модернизации), эксплуатации и вывода из эксплуатации проводятся мероприятия по

установлении требований к обеспечению безопасности значимого объекта

разработке ***организационных и технических мер*** по обеспечению безопасности значимого объекта

внедрении организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие

обеспечении безопасности значимого объекта в ***ходе его эксплуатации***

обеспечении безопасности значимого объекта при ***выводе его из эксплуатации***

Состав и формы документов определяются субъектом критической информационной инфраструктуры

Обеспечение безопасности значимого объекта 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

В ходе создания (модернизации), эксплуатации и вывода из эксплуатации проводятся мероприятия по

установлении требований к обеспечению безопасности значимого объекта

разработке ***организационных и технических мер*** по обеспечению безопасности значимого объекта

внедрении организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие

обеспечении безопасности значимого объекта в ***ходе его эксплуатации***

обеспечении безопасности значимого объекта при ***выводе его из эксплуатации***

Состав и формы документов определяются субъектом критической информационной инфраструктуры

Обеспечение безопасности значимого объекта при выводе его из эксплуатации

- архивирование информации, содержащейся в значимом объекте
- уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации
- уничтожение данных об архитектуре и конфигурации значимого объекта
- архивирование или уничтожение эксплуатационной документации на значимый объект и его подсистему безопасности и организационно-распорядительных документов по безопасности значимого объекта

Акт об уничтожении (стирание) данных с машинных носителей

Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов

В значимых объектах КИИ **объектами**, подлежащими защите от угроз безопасности

Информационные системы

- информация
- программно-аппаратные средства
- программные средства
- средства защиты информации
- архитектура и конфигурация информационной системы

Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов

В значимых объектах КИИ **объектами**, подлежащими защите от угроз безопасности

автоматизированные системы управления

- информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса
- программно-аппаратные средства
- программные средства
- средства защиты информации
- архитектура и конфигурация автоматизированной системы управления

Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов

В значимых объектах КИИ **объектами**, подлежащими защите от угроз безопасности

информационно-телекоммуникационные сети

- информация, передаваемая по линиям связи
- телекоммуникационное оборудование
- средства защиты информации
- архитектура и конфигурация информационно-телекоммуникационной сети

Меры по обеспечению безопасности значимого объекта КИИ

17 групп мер

- Аудит безопасности (АУД)
- Управление конфигурацией (УКФ)
- Управление обновлениями программного обеспечения (ОПО)
- Планирование мероприятий по обеспечению безопасности (ПЛН)
- Реагирование на инциденты информационной безопасности (ИНЦ)
- Информирование и обучение персонала (ИПО)
- Защита технических средств и систем (ЗТС)
- Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)
- 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 информационной (автоматизированной) системы (сети) и ее компонентов (ЗИС)

Выбор мер по обеспечению безопасности значимого объекта

Базовый набор мер в зависимости от категории

Адаптация набора мер в соответствии с моделью угроз

Базовый набор мер обеспечения безопасности значимого объекта

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

Спасибо за внимание!

Гордеев Александр Сергеевич

Начальник отдела обеспечения безопасности
критической информационной инфраструктуры