Требования к системе безопасности значимого объекта критической информационной инфраструктуры

Деркач Сергей Александрович

начальник отдела аттестации

Главного управления информационных технологий и связи Омской области

Нормативные правовые акты по КИИ, разработанные ФСТЭК России

Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации
(Приказ ФСТЭК России от 6 декабря 2017 года № 227)

Форма направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий
(Приказ ФСТЭК России от 22 декабря 2017 года № 236)

Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры и обеспечению их функционирования
(Приказ ФСТЭК России от 21 декабря 2017 года № 235)

Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации
(Приказ ФСТЭК России от 25 декабря 2017 года № 239)

Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации
(Приказ ФСТЭК России от 11 декабря 2017 г. № 229)

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

21 декабря 2017 г. *№ 235*

ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ К СОЗДАНИЮ СИСТЕМ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ И ОБЕСПЕЧЕНИЮ ИХ ФУНКЦИОНИРОВАНИЯ

регламентирует организационные вопросы к системе обеспечения безопасности значимого объекта КИИ

Обязанности руководителя субъекта КИИ

Определяет состав и структуру системы безопасности, а также функции ее участников

Создает систему безопасности значимого объекта КИИ, организует и контролирует ее функционирование

Создает или определяет структурное подразделение, ответственное за обеспечение безопасности значимых объектов КИИ или назначает отдельных работников

Функции структурного подразделения по безопасности (специалистов по безопасности)

- разрабатывает предложения по совершенствованию организационно-распорядительных документов по безопасности значимых объектов КИИ и представлять их руководителю субъекта КИИ (уполномоченному лицу);
- проводит анализ угроз безопасности информации в отношении значимых объектов КИИ и выявлять уязвимости в них
- обеспечивает реализацию требований по обеспечению безопасности значимых объектов КИИ;

- обеспечивает в соответствии с требованиями по безопасности реализацию организационных мер и применение средств защиты информации, эксплуатацию средств защиты информации;
- осуществляет реагирование на компьютерные инциденты;
- организовывает проведение оценки соответствия значимых объектов КИИ требованиям по безопасности;
- готовит предложения по совершенствованию функционирования систем безопасности, а также по повышению уровня безопасности значимых объектов КИИ.

Обязанности пользователей объекта КИИ

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

Могут возлагаться отдельные функции по обеспечению безопасности значимых объектов КИИ

Координацию и контроль деятельности работников осуществляют структурное подразделение по безопасности, специалисты по безопасности

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

25 декабря 2017 г. *№ 239*

ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

требования к системе безопасности значимого объекта КИИ

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

Законодательство РФ о государственной тайне

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**

Обеспечение безопасности значимых объектов, являющихся **автоматизированными системами управления производственными и технологическими процессами**

Требования по обеспечению безопасности значимых объектов

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Постановление Правительства РФ от 1 ноября 2012 г. № 1119

Нормативные правовые акты Минкомсвязи России

Этапы проведения работ по созданию (модернизации) значимого объекта

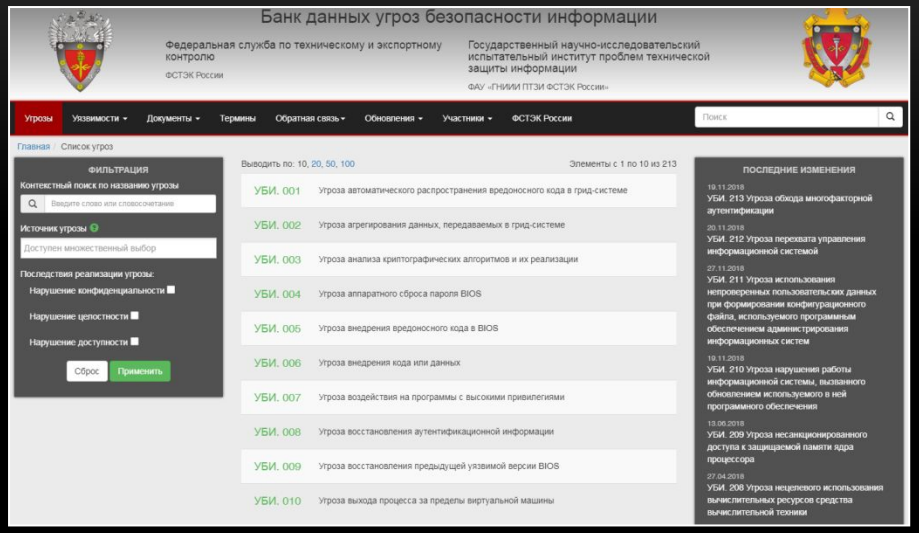
- анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение (при ее наличии);
- проектирование подсистемы безопасности значимого объекта КИИ;
- разработка рабочей (эксплуатационной) документации на значимый объект (в части обеспечения его безопасности).

Анализ угроз безопасности информации объекта КИИ

- выявление источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей;
- анализ возможных уязвимостей значимого объекта и его программных, программно-аппаратных средств;
- определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации;
- оценку возможных последствий от реализации (возникновения) угроз безопасности информации.

Нормативно-методические документы по моделированию угроз объекта КИИ

Банк данных угроз безопасности информации (bdu.fstec.ru)



КИИ - ИСПДн

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

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

Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России от 2007г.

Информационное сообщение ФСТЭК России от 4 мая 2018 г. № 240/22/2339

Проект Методического документа ФСТЭК России от 2015 г. «Методика определения угроз безопасности информации в информационных системах»

Содержание частной модели угроз безопасности информации

Модель
угроз безопасности информации:

1) краткое описание архитектуры значимого объекта

2) модель нарушителя

3) характеристику источников угроз безопасности информации, в том числе модель нарушителя

4) описание всех угроз безопасности информации, актуальных для значимого объекта.

Описание каждой угрозы безопасности информации должно включать:

1) источник угрозы безопасности информации;

2) уязвимости (ошибки), которые могут быть использованы для реализации (способствовать возникновению) угрозы безопасности информации;

3) возможные способы (сценарии) реализации угрозы безопасности информации;

4) возможные последствия от угрозы безопасности информации

Состав мер по обеспечению безопасности для значимого объекта КИИ

- Идентификация и аутентификация
- Управление доступом
- Ограничение программной среды
- Защита машинных носителей информации
- Антивирусная защита
- Предотвращение вторжений (компьютерных атак)
- Обеспечение целостности
- Обеспечение доступности
- Защита технических средств и систем
- Защита информационной (автоматизированной) системы (сети) и ее компонентов

- Аудит безопасности
- Реагирование на инциденты информационной безопасности
- Управление конфигурацией
- Управление обновлениями программного обеспечения
- Планирование мероприятий по обеспечению безопасности
- Обеспечение действий в нештатных (непредвиденных) ситуациях
- Информирование и обучение персонала

Приказ ФСТЭК России от 11 февраля 2013 г. № 17,
Приказ ФСТЭК от 18 февраля 2013 г. России № 21

Выбор мер по обеспечению безопасности для значимого объекта КИИ

Базовый набор мер

Определяется на основе **категории значимости** значимого объекта КИИ

Адаптированный базовый набор мер

Адаптация базового набора мер с учетом:

- модели угрозами безопасности информации;
- применяемых информационных технологий;
- особенностями функционирования значимого объекта КИИ

Дополнение адаптированного базового набора мер

С учетом требований, установленных иными нормативными правовыми актами в области:

- обеспечения безопасности КИИ;
- защиты информации

Меры по обеспечению безопасности

Компенсирующие меры

(меры по обеспечению промышленной, функциональной и (или) физической безопасности значимого объекта КИИ)

Обозначение и номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости		
		3	2	1
I. Идентификация и аутентификация (ИАФ)				
ИАФ.0	Разработка политики идентификации и аутентификации	+	+	+
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	+	+	+
ИАФ.2	Идентификация и аутентификация устройств	+	+	+
ИАФ.3	Управление идентификаторами	+	+	+
ИАФ.4	Управление средствами аутентификации	+	+	+
ИАФ.5	Идентификация и аутентификация внешних пользователей	+	+	+
ИАФ.6	Двусторонняя аутентификация			
ИАФ.7	Защита аутентифицированной информации при передаче	+	+	+

Меры защиты в Приказе ФСТЭК России № 17, Приказе ФСТЭК России № 21, Приказе ФСТЭК России № 31

Меры защиты в Приказе ФСТЭК России № 31

II. Управление доступом (УПД)				
УПД.0	Разработка политики управления доступом	+	+	+
УПД.1	Управление учетными записями пользователей	+	+	+
УПД.2	Реализация политик управления доступом	+	+	+
УПД.3 (УПД.17)	Доверенная загрузка		+	+
УПД.4	Разделение полномочий (ролей) пользователей	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий	+	+	+
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	+	+	+
УПД.7	Предупреждение пользователя при его доступе к информационным ресурсам			
УПД.8	Оповещение пользователя при успешном входе о предыдущем доступе к информационной (автоматизированной) системе			+
УПД.9	Ограничение числа параллельных сеансов доступа			+
УПД.10	Блокирование сеанса доступа пользователя при неактивности	+	+	+
УПД.11	Управление действиями пользователей до идентификации и аутентификации	+	+	+
УПД.12	Управление атрибутами безопасности			
УПД.13	Реализация защищенного удаленного доступа	+	+	+
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	+	+	+

Меры защиты в Приказе ФСТЭК России № 17, Приказе ФСТЭК России № 21, Приказе ФСТЭК России № 31

Меры защиты в Приказе ФСТЭК России № 31

III. Ограничение программной среды (ОПС)				
ОПС.0	Разработка политики ограничения программной среды		+	+
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения			+
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения		+	+
ОПС.3 (ОПС.4)	Управление временными файлами			

Меры защиты в Приказе ФСТЭК России № 17, Приказе ФСТЭК России № 21, Приказе ФСТЭК России № 31

Меры защиты в Приказе ФСТЭК России № 31

IV. Защита машинных носителей информации (ЗНИ)				
ЗНИ.0	Разработка политики защиты машинных носителей информации	+	+	+
ЗНИ.1	Учет машинных носителей информации	+	+	+
ЗНИ.2	Управление физическим доступом к машинным носителям информации	+	+	+
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны			
ЗНИ.4	Исключение возможности несанкционированного чтения информации на машинных носителях информации			
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	+	+	+
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации			+
ЗНИ.7	Контроль подключения машинных носителей информации	+	+	+
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	+	+	+

Меры защиты в Приказе ФСТЭК России № 17, Приказе ФСТЭК России № 21, Приказе ФСТЭК России № 31

Меры защиты в Приказе ФСТЭК России № 31

V. Аудит безопасности (АУД)				
АУД.0	Разработка политики аудита безопасности	+	+	+
АУД.1	Инвентаризация информационных ресурсов	+	+	+
АУД.2 (АНЗ.1)	Анализ уязвимостей и их устранение	+	+	+
АУД.3 (РСБ.6)	Генерирование временных меток и (или) синхронизация системного времени	+	+	+
АУД.4 (РСБ.3)	Регистрация событий безопасности	+	+	+
АУД.5	Контроль и анализ сетевого трафика			+
АУД.6 (РСБ.7)	Защита информации о событиях безопасности	+	+	+
АУД.7 (РСБ.5)	Мониторинг безопасности	+	+	+
АУД.8 (РСБ.4)	Реагирование на сбои при регистрации событий безопасности	+	+	+
АУД.9	Анализ действий пользователей			+
АУД.10	Проведение внутренних аудитов	+	+	+
АУД.11	Проведение внешних аудитов			+

Меры защиты в Приказе ФСТЭК России № 17, Приказе ФСТЭК России № 21, Приказе ФСТЭК России № 31

Меры защиты в Приказе ФСТЭК России № 31

VI. Антивирусная защита (АВЗ)				
АВЗ.0	Разработка политики антивирусной защиты	+	+	+
АВЗ.1	Реализация антивирусной защиты	+	+	+
АВЗ.2	Антивирусная защита электронной почты и иных сервисов	+	+	+
АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов			+
АВЗ.4 (АВЗ.2)	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+
АВЗ.5	Использование средств антивирусной защиты различных производителей			+

Меры защиты в Приказе ФСТЭК России № 17, Приказе ФСТЭК России № 21, Приказе ФСТЭК России № 31

Меры защиты в Приказе ФСТЭК России № 31

VII. Предотвращение вторжений (компьютерных атак) (СОВ)				
СОВ.0	Разработка политики предотвращения вторжений (компьютерных атак)		+	+
СОВ.1	Обнаружение и предотвращение компьютерных атак		+	+
СОВ.2	Обновление базы решающих правил		+	+

Меры защиты в Приказе ФСТЭК России № 17, Приказе ФСТЭК России № 21, Приказе ФСТЭК России № 31

Меры защиты в Приказе ФСТЭК России № 31

VIII. Обеспечение целостности (ОЦЛ)				
ОЦЛ.0	Разработка политики обеспечения целостности	+	+	+
ОЦЛ.1	Контроль целостности программного обеспечения	+	+	+
ОЦЛ.2	Контроль целостности информации			
ОЦЛ.3 (ОЦЛ.6)	Ограничения по вводу информации в информационную (автоматизированную) систему			+
ОЦЛ.4 (ОЦЛ.7)	Контроль данных, вводимых в информационную (автоматизированную) систему		+	+
ОЦЛ.5 (ОЦЛ.8)	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях		+	+
ОЦЛ.6	Обезличивание и (или) деидентификация информации			

Меры защиты в Приказе ФСТЭК России № 17, Приказе ФСТЭК России № 21, Приказе ФСТЭК России № 31

Меры защиты в Приказе ФСТЭК России № 31

IX. Обеспечение доступности (ОДТ)				
ОДТ.0	Разработка политики обеспечения доступности	+	+	+
ОДТ.1	Использование отказоустойчивых технических средств		+	+
0ДТ.2	Резервирование средств и систем		+	+
ОДТ.3	Контроль безотказного функционирования средств и систем		+	+
ОДТ.4	Резервное копирование информации	+	+	+
ОДТ.5	Обеспечение возможности восстановления информации	+	+	+
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	+	+	+
ОДТ.7	Кластеризация информационной (автоматизированной) системы			
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	+	+	+

Меры защиты в Приказе ФСТЭК России № 31

Меры защиты в Приказе ФСТЭК России № 17, Приказе ФСТЭК России № 31

Меры защиты в Приказе ФСТЭК России № 17, Приказе ФСТЭК России № 21, Приказе ФСТЭК России № 31

X. Защита технических средств и систем (ЗТС)				
ЗТС.0	Разработка политики защиты технических средств и систем	+	+	+
ЗТС.1	Защита информации от утечки по техническим каналам			
ЗТС.2	Организация контролируемой зоны	+	+	+
ЗТС.3	Управление физическим доступом	+	+	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+
ЗТС.5	Защита от внешних воздействий	+	+	+
ЗТС.6	Маркирование аппаратных компонентов системы относительно разрешенной к обработке информации			

Меры защиты в Приказе ФСТЭК России № 17, Приказе ФСТЭК России № 21, Приказе ФСТЭК России № 31

Меры защиты в Приказе ФСТЭК России № 31

XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)				
ЗИС.0	Разработка политики защиты информационной (автоматизированной) системы и ее компонентов	+	+	+
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	+	+	+
ЗИС.2 (ЗИС.23)	Защита периметра информационной (автоматизированной) системы	+	+	+
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы	+	+	+
ЗИС.4 (ЗИС.17)	Сегментирование информационной (автоматизированной) системы		+	+
ЗИС.5	Организация демилитаризованной зоны	+	+	+
ЗИС.6	Управление сетевыми потоками			
ЗИС.7	Использование эмулятора среды функционирования программного обеспечения ("песочница")			
ЗИС.8 (ЗИС.28)	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы	+	+	+
ЗИС.9 (ЗИС.25)	Создание гетерогенной среды			
ЗИС.10 (ЗИС.26)	Использование программного обеспечения, функционирующего в средах различных операционных систем			
ЗИС.11 (ЗИС.2)	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом			
ЗИС.12 (ЗИС.19)	Изоляция процессов (выполнение программ) в выделенной области памяти			

Меры защиты в Приказе ФСТЭК России № 31

Меры защиты в Приказе ФСТЭК России № 17, Приказе ФСТЭК России № 21, Приказе ФСТЭК России № 31

ЗИС.13 (ЗИС.15)	Защита неизменяемых данных		+	+
ЗИС.14	Использование неперезаписываемых машинных носителей информации			
ЗИС.15	Реализация электронного почтового обмена с внешними сетями через ограниченное количество контролируемых точек			
ЗИС.16 (ОЦЛ.4)	Защита от спама		+	+
ЗИС.17	Защита информации от утечек			
ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию			
ЗИС.19 (ЗИС.3)	Защита информации при ее передаче по каналам связи	+	+	+
ЗИС.20 (ЗИС.4)	Обеспечение доверенных канала, маршрута	+	+	+
ЗИС.21 (ЗИС.5)	Запрет несанкционированной удаленной активации периферийных устройств	+	+	+
ЗИС.22 (ЗИС.6)	Управление атрибутами безопасности при взаимодействии с иными информационными (автоматизированными) системами			
ЗИС.23 (ЗИС.7)	Контроль использования мобильного кода		+	+
ЗИС.24 (ЗИС.8)	Контроль передачи речевой информации		+	+
ЗИС.25 (ЗИС.9)	Контроль передачи видеоинформации		+	+
ЗИС.26 (ЗИС.10)	Подтверждение происхождения источника информации			
ЗИС.27 (ЗИС.11)	Обеспечение подлинности сетевых соединений		+	+

ЗИС.28 (ЗИС.12)	Исключение возможности отрицания отправки информации		+	+
ЗИС.29 (ЗИС.13)	Исключение возможности отрицания получения информации		+	+
ЗИС.30 (ЗИС.14)	Использование устройств терминального доступа			
ЗИС.31 (ЗИС.16)	Защита от скрытых каналов передачи информации			+
ЗИС.32 (ЗИС.20)	Защита беспроводных соединений	+	+	+
ЗИС.33 (ЗИС.21)	Исключение доступа через общие ресурсы			+
ЗИС.34 (ЗИС.22)	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	+	+	+
ЗИС.35 (ЗИС.24)	Управление сетевыми соединениями		+	+
ЗИС.36 (ЗИС.27)	Создание (эмуляция) ложных компонентов информационных (автоматизированных) систем			
ЗИС.37 (ЗИС.29)	Перевод информационной (автоматизированной) системы в безопасное состояние при возникновении отказов (сбоев)			
ЗИС.38 (ЗИС.30)	Защита информации при использовании мобильных устройств	+	+	+
ЗИС.39 (ЗСВ.6)	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	+	+	+

Меры защиты в Приказе ФСТЭК России № 31

Меры защиты в Приказе ФСТЭК России № 17, Приказе ФСТЭК России № 21, Приказе ФСТЭК России № 31

XII. Реагирование на компьютерные инциденты (ИНЦ)				
ИНЦ.0	Разработка политики реагирования на компьютерные инциденты	+	+	+
ИНЦ.1 (ИНЦ.2)	Выявление компьютерных инцидентов	+	+	+
ИНЦ.2 (ИНЦ.3)	Информирование о компьютерных инцидентах	+	+	+
ИНЦ.3 (ИНЦ.4)	Анализ компьютерных инцидентов	+	+	+
ИНЦ.4 (ИНЦ.5)	Устранение последствий компьютерных инцидентов	+	+	+
ИНЦ.5 (ИНЦ.6))	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	+	+	+
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах			+

Меры защиты в Приказе ФСТЭК России № 31

Меры защиты в Приказе ФСТЭК России № 21, Приказе ФСТЭК России № 31

XIII. Управление конфигурацией (УКФ)				
УКФ.0	Разработка политики управления конфигурацией информационной (автоматизированной) системы	+	+	+
УКФ.1	Идентификация объектов управления конфигурацией			
УКФ.2	Управление изменениями	+	+	+
УКФ.3 (АН3.2)	Установка (инсталляция) только разрешенного к использованию программного обеспечения	+	+	+
УКФ.4	Контроль действий по внесению изменений			

Меры защиты в Приказе ФСТЭК России № 31

Меры защиты в Приказе ФСТЭК России № 21, Приказе ФСТЭК России № 31

XIV. Управление обновлениями программного обеспечения (ОПО)				
ОПО.0	Разработка политики управления обновлениями программного обеспечения	+	+	+
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	+	+	+
ОПО.2	Контроль целостности обновлений программного обеспечения	+	+	+
ОПО.3	Тестирование обновлений программного обеспечения	+	+	+
ОПО.4	Установка обновлений программного обеспечения	+	+	+

Меры защиты в Приказе ФСТЭК России № 31

XV. Планирование мероприятий по обеспечению безопасности (ПЛН)				
ПЛН.0	Разработка политики планирования мероприятий по обеспечению защиты информации	+	+	+
ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации	+	+	+
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации	+	+	+

Меры защиты в Приказе ФСТЭК России № 31

XVI. Обеспечение действий в нештатных ситуациях (ДНС)				
ДНС.0	Разработка политики обеспечения действий в нештатных ситуациях	+	+	+
ДНС.1	Разработка плана действий в нештатных ситуациях	+	+	+
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях	+	+	+
ДНС.3	Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций		+	+
ДНС.4	Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций		+	+
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	+		+
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения	+	+	+

Меры защиты в Приказе ФСТЭК России № 31

XVII. Информирование и обучение персонала (ИПО)				
ИПО.0	Разработка политики информирования и обучения персонала	+	+	+
ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы	+	+	+
ИПО.2	Обучение персонала правилам безопасной работы	+	+	+
ИПО.3	Проведение практических занятий с персоналом по правилам безопасной работы		+	+
ИПО.4	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы	+	+	+

Меры защиты в Приказе ФСТЭК России № 31

Соответствие категории объекта КИИ и класса средств защиты информации (СЗИ)

Категория КИИ	Классы СЗИ в КИИ
1	4
2	5
3	6

Объект КИИ

В значимых объектах КИИ **1, 2, и 3 категории** – СВТ не ниже **5 класса** защиты от НСД;

В значимых объектах КИИ **1 и 2 категории** - применяются сертифицированные СЗИ, прошедшие проверку не ниже, чем **по 4 уровню** контроля отсутствия недекларированных возможностей

Внедрение организационных и технических мер по обеспечению безопасности значимого объекта

Этапы работ:
(приказ № 239 от 25.12.2017)

- Установка и настройка средств защиты информации.
- Разработка документов по безопасности.
- Внедрение организационных мер.
- Предварительные испытания.
- Опытная эксплуатация.
- Выявление уязвимостей.
- Приемочные испытания.

Государственный контроль в области обеспечения безопасности значимых объектов КИИ

Государственный контроль в области обеспечения безопасности значимых объектов КИИ

соблюдение требований № 187–ФЗ и принятых в соответствии с ним НПА

ФСТЭК России

ПЛАНОВАЯ ПРОВЕРКА

истечение **3-х лет** со дня **внесения** сведений об объекте КИИ в реестр значимых объектов КИИ

истечение **3-х лет** со дня **окончания** осуществления последней плановой проверки в отношении значимого объекта КИИ

ВНЕПЛАНОВАЯ ПРОВЕРКА

истечение срока выполнения субъектом КИИ **предписания** об устранении выявленного нарушения

возникновение **компьютерного инцидента,** повлекшего негативные последствия

приказ директора ФСТЭК России на основании:
поручения Президента РФ;
поручения Правительства РФ;
требования прокурора.

Приказы ФСБ РФ по обеспечению безопасности объекта КИИ

1	№ 366 от 24.07.2018 "О Национальном координационном центре по компьютерным инцидентам"	03.08.2018
2	№ 367 от 24.07.2018 "Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА"	03.08.2018
3	"Об утверждении порядка информирования ФОИВ, уполномоченного в области обеспечения функционирования ГосСОПКА, о КИ, реагировании на них, принятия мер по ликвидации последствий КА, проведенных в отношении ЗО КИИ" (Приложение)	Проект
4	№ 368 от 24.07.2018 "Об утверждении Порядка обмена информацией о КИ между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на КИ, и Порядка получения субъектами КИИ РФ информации о средствах и способах проведения КА и о методах их предупреждения и обнаружения"(Приложение 1), (Приложение 2)	03.08.2018
5	"Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ" (Приложение)	Проект
6	"Об утверждении порядка, ТУ установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий КА и реагирования на КИ, за исключением средств, предназначенных для поиска признаков КА в сетях электросвязи, используемых для организации взаимодействия объектов КИИ РФ"(Приложение)	Проект

Требования к системе безопасности значимого объекта КИИ

Деркач Сергей Александрович

Начальник отдела аттестации

Главного управления информационных технологий и связи Омской области