



План мероприятий

по выполнению требований Федерального закона
от 26.07.2017 № 187-ФЗ «О безопасности критической
информационной инфраструктуры
Российской Федерации»

Содержание

Перечень сокращений	2
0. Определение принадлежности организации к субъектам КИИ	3
1. Категорирование объектов КИИ — до 01.09.2020	3
2. Разработка мероприятий по взаимодействию с ФСБ России	5
3. Создание системы безопасности значимых объектов КИИ	6
4. Обеспечение безопасности значимого объекта КИИ в ходе его эксплуатации.....	12
5. Обеспечение безопасности значимого объекта КИИ при выводе его из эксплуатации	12

Перечень сокращений

АСУ	Автоматизированная система управления
ЗОКИИ	Значимый объект КИИ
ИБ	Информационная безопасность
ИС	Информационная система
ИТ	Информационная технология
ИТС	Информационно-телекоммуникационная сеть
КИИ	Критическая информационная инфраструктура
НКЦКИ	Национальный координационный центр по компьютерным инцидентам
НМД	Нормативно-методический документ
НПА	Нормативно-правовой акт
ОКИИ	Объект КИИ
ОРД	Организационно-распорядительная документация
ПП	Постановление правительства
СБЗОКИИ	Система безопасности значимого объекта КИИ
ТЗКИ	Техническая защита конфиденциальной информации
ФЗ	Федеральный закон
ФСБ	Федеральная служба безопасности
ФСТЭК	Федеральная служба по техническому и экспортному контролю

0. Определение принадлежности организации к субъектам КИИ

Что делать

Составить перечень ИС, АСУ, ИТС организации с определением сферы функционирования каждой ИС, АСУ, ИТС

Результаты

- Сводный перечень ИС, АСУ, ИТС организации с информацией о сфере деятельности для каждой ИС, АСУ, ИТС
- Вывод о необходимости (или отсутствии необходимости) выполнения требований закона № 187-ФЗ (в первом случае может быть задокументирован актом (приказом, распоряжением) о приведении системы безопасности организации в соответствие с требованиями закона № 187-ФЗ)

Примечание

Если в перечне есть хотя бы одна ИС, АСУ или ИТС, функционирующая в одной из следующих сфер:

- здравоохранения;
- науки;
- транспорта;
- связи;
- энергетики;

- банковской сфере и иных сферах финансового рынка;
- топливно-энергетического комплекса;
- в области атомной энергии;
- оборонной промышленности;
- ракетно-космической промышленности;
- горнодобывающей промышленности;
- металлургической промышленности;
- химической промышленности —

Сроки проведения

До начала категорирования объектов КИИ

Кто проводит (организует)

Руководство, подразделение ИБ, подразделение ИТ, специалисты-технологи

Ссылка на НПА, НМД

187-ФЗ, ст. 2, п. 7, 8

или обеспечивающая взаимодействие таких ИС, АСУ или ИТС является объектом КИИ, а следовательно, организация является субъектом КИИ.

1. Категорирование объектов КИИ — до 01.09.2020

1.1. Создание комиссии по категорированию объектов КИИ

Что делать

Разработать и утвердить приказ (распоряжение) о создании комиссии по категорированию объектов КИИ

Результаты

Распоряжение о создании комиссии по категорированию объектов КИИ

Сроки проведения

—

Кто проводит (организует)

Руководитель организации

Ссылка на НПА, НМД

ПП № 127, п. 11

Примечание

В состав комиссии включаются:

- руководитель (или уполномоченное руководителем лицо);
- работники — специалисты в области осуществляемых видов деятельности;
- работники — специалисты в области информационных технологий;
- работники — специалисты по эксплуатации основного технологического (производственного) оборудования;

- работники — специалисты в области промышленной безопасности;
- работники — специалисты по обеспечению информационной безопасности;
- работники — специалисты по защите государственной тайны (в случае обработки на объекте КИИ информации, составляющей государственную тайну);
- работники структурного подразделения по гражданской обороне и защите от чрезвычайных ситуаций.

В состав комиссии могут быть включены (по согласованию с соответствующими госорганами и организациями) представители госорганов или организаций в установленной сфере деятельности.

В состав комиссии могут быть включены работники других подразделений, в том числе финансово-экономического подразделения.

Если субъект КИИ имеет филиалы, то в этих филиалах могут создаваться отдельные комиссии, координацию деятельности которых осуществляет комиссия по категорированию субъекта КИИ.

1.2. Определение перечня процессов деятельности организации и выявление критических процессов

Что делать	Сроки проведения
<ul style="list-style-type: none"> Определить управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности организации Выявить критические процессы деятельности организации 	—
Результаты	Кто проводит (организует)
Перечень критических процессов организации	Комиссия по категорированию объектов КИИ
	Ссылка на НПА, НМД
	ПП № 127, п. 14 (а, б)
Примечание	
Перечень критических процессов организации должен содержать:	<ul style="list-style-type: none"> наименование процесса; тип процесса (управленческий, технологический, производственный и т. п.); указание на сферу деятельности, которую поддерживает процесс.

1.3. Разработка перечня объектов КИИ, подлежащих категорированию

Что делать	Сроки проведения
<ul style="list-style-type: none"> Определить объекты КИИ (ИС, АС, ИТС), которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов Разработать перечень объектов КИИ, подлежащих категорированию Согласовать перечень объектов КИИ, подлежащих категорированию, с отраслевым регулятором Утвердить перечень объектов КИИ, подлежащих категорированию, у руководителя организации 	До 01.09.2019 ¹
<ul style="list-style-type: none"> Направить перечень объектов КИИ, подлежащих категорированию, во ФСТЭК России 	В течение десяти рабочих дней после утверждения перечня
Результаты	Кто проводит (организует)
Перечень объектов КИИ, подлежащих категорированию (определению категории значимости)	Комиссия по категорированию объектов КИИ
	Ссылка на НПА, НМД
	ПП № 127, п. 5 (г), п. 14 (в, г), п. 15
Примечание	
Перечень объектов КИИ, подлежащих категорированию, должен содержать следующую информацию:	<ul style="list-style-type: none"> наименование субъекта КИИ; наименование объекта КИИ; указание на сферу (область) деятельности, в которой функционирует объект; адрес размещения объекта КИИ; ориентировочный срок категорирования.

¹ Срок обязателен для государственных органов и учреждений и рекомендован для юридических лиц и ИП.

1.4. Определение угроз безопасности для объектов КИИ

Что делать

- Проанализировать возможные действия нарушителей в отношении объектов КИИ, а также иных источников угроз безопасности информации
- Провести анализ угроз безопасности информации, которые могут привести к возникновению компьютерных инцидентов на объектах КИИ

Результаты

Перечень угроз безопасности информации и уязвимостей для каждого объекта КИИ

Сроки проведения

—

Кто проводит (организует)

Комиссия по категорированию объектов КИИ

Ссылка на НПА, НМД

ПП № 127, п. 14 (г, д)

1.5. Определение категории значимости для объектов КИИ

Что делать

- В соответствии с перечнем показателей критериев значимости (ПП № 127) для каждого объекта КИИ определить возможное значение по каждому показателю
- Присвоить каждому из объектов КИИ одну из категорий значимости либо принять решение об отсутствии необходимости присвоения им одной из категорий значимости
- Оформить акты категорирования объектов КИИ

Результаты

Акт категорирования объекта КИИ (для каждого объекта КИИ)

Сроки проведения

—

Кто проводит (организует)

Комиссия по категорированию объектов КИИ

Ссылка на НПА, НМД

ПП № 127, п. 14 (е, ж)

1.6. Подготовка сведений о категорировании объектов КИИ

Что делать

Подготовить и направить во ФСТЭК России сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

Результаты

Сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий (отдельно для каждого объекта КИИ)

Сроки проведения

В течение 10 рабочих дней после утверждения акта категорирования объекта КИИ

Кто проводит (организует)

Комиссия по категорированию объектов КИИ

Ссылка на НПА, НМД

ПП № 127, п. 17, приказ ФСТЭК России № 236

2. Разработка мероприятий по взаимодействию с ФСБ России

2.1. Разработка регламента информирования ФСБ России

Что делать

Разработать и утвердить руководителем организации регламент информирования ФСБ России (НКЦКИ) о компьютерных инцидентах

Результаты

- Регламент информирования ФСБ России (НКЦКИ) о компьютерных инцидентах
- Перечень информации о компьютерных инцидентах, связанных с функционированием объектов КИИ
- Приказ (распоряжение) об утверждении регламента информирования ФСБ России (НКЦКИ) о компьютерных инцидентах

Сроки проведения

С момента определения организации как субъекта КИИ

Кто проводит (организует)

Подразделение (ответственный) ИБ организации, лицензиат (ТЗКИ) ФСТЭК России²

Ссылка на НПА, НМД

187-ФЗ (ст. 9, ч. 2, п. 1), приказ ФСБ России № 367

² Привлечение лицензиатов ФСТЭК России является необязательным, решение об их привлечении принимает сам субъект КИИ.

2.2. Организация взаимодействия с ФСБ России (НКЦКИ)

Что делать	Кто проводит (организует)
<ul style="list-style-type: none"> В случае подключения к технической инфраструктуре НКЦКИ направить в НКЦКИ по адресу gov-cert@gov-cert.ru запрос о необходимости организации технической возможности незамедлительного информирования об инцидентах в соответствии с ч. 2 ст. 9 закона № 187-ФЗ Подключиться к технической инфраструктуре НКЦКИ в соответствии с установленным порядком 	Подразделение (ответственный) ИБ организации, субъекты (центры) ГосСОПКА (при необходимости)
	Ссылка на НПА, НМД
	Приказ ФСБ России № 367, приказ ФСБ России № 368

Для организаций, имеющих значимые объекты КИИ

2.3. Разработка плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак

Что делать	Сроки проведения
<ul style="list-style-type: none"> Разработать план реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак самостоятельно или совместно с НКЦКИ³ Направить План на согласование в ФСБ России⁴ и в Банк России⁵ 	Не позднее 90 календарных дней после включения объекта КИИ в реестр значимых объектов КИИ
Результаты	Кто проводит (организует)
План реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак	Подразделение (ответственный) ИБ организации
Примечание	Ссылка на НПА, НМД
<p>План реагирования должен содержать:</p> <ul style="list-style-type: none"> технические характеристики и состав значимых объектов КИИ; события (условия), при наступлении которых начинается реализация предусмотренных Планом мероприятий; мероприятия, проводимые в ходе реагирования на инциденты и принятия мер по ликвидации последствий атак, а также время на их реализацию; описание состава подразделений и должностных лиц субъекта КИИ, ответственных за проведение мероприятий. 	<p>Для субъектов КИИ, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты КИИ в банковской сфере и в иных сферах финансового рынка, в План дополнительно включаются условия привлечения Банка России к проведению мероприятий.</p> <p>При необходимости в План включаются:</p> <ul style="list-style-type: none"> условия привлечения ФСБ России к проведению мероприятий; порядок проведения мероприятий в отношении значимых объектов КИИ совместно с ФСБ России.

3. Создание системы безопасности значимых объектов КИИ

3.1. Разработка и утверждение руководителем организации приказа (распоряжения) о создании системы безопасности значимых объектов КИИ

Что делать	Сроки проведения
Разработать и утвердить приказ (распоряжение) о создании системы безопасности значимых объектов КИИ	—
Результаты	Кто проводит (организует)
Приказ (распоряжение) о создании системы безопасности значимых объектов КИИ	Руководитель организации, подразделение (ответственный) ИБ организации
Примечание	Ссылка на НПА, НМД
<p>В приказе (распоряжении) должны быть указаны по меньшей мере:</p> <ul style="list-style-type: none"> цели создания СБЗОКИИ; структурные подразделения (работники), ответственные за обеспечение безопасности значимых объектов КИИ, и их функции по обеспечению безопасности значимых объектов КИИ; 	187-ФЗ (ст. 10, ч. 1), приказ ФСТЭК России № 235 (раздел II, п. 8, 9, 10)

³ Участие НКЦКИ обязательно, если есть необходимость привлечения ФСБ России к проведению мероприятий по реагированию на инциденты и принятию мер по ликвидации последствий атак.

⁴ Согласование с ФСБ России обязательно, если есть необходимость привлечения ФСБ России к проведению мероприятий по реагированию на инциденты и принятию мер по ликвидации последствий атак.

⁵ Для субъектов КИИ со значимыми объектами КИИ, осуществляющих деятельность в банковской сфере и в иных сферах финансового рынка.

3.2. Установление требований к обеспечению безопасности значимых объектов КИИ

3.2.1. Разработка технического задания на создание СБЗОКИИ

<p>Что делать</p> <ul style="list-style-type: none"> Определить базовый набор мер по обеспечению безопасности значимого объекта на основе установленной категории значимости значимого объекта Адаптировать базовый набор мер по обеспечению безопасности значимого объекта в соответствии с угрозами безопасности информации, применяемыми информационными технологиями и особенностями функционирования значимого объекта Разработать компенсирующие меры, обеспечивающие блокирование (нейтрализацию) угроз безопасности информации с необходимым уровнем защищенности значимого объекта (при необходимости) Разработать техническое задание на создание СБЗОКИИ 	<p>Сроки проведения</p> <p>—</p>
<p>Результаты</p> <p>Техническое задание на создание СБЗОКИИ</p>	<p>Кто проводит (организует)</p> <p>Подразделение (ответственный) ИБ организации, лицензиат (ТЗКИ) ФСТЭК России</p> <p>Ссылка на НПА, НМД</p> <p>Приказ ФСТЭК России № 239, раздел II, п. 10</p>
<p>Примечание</p> <p>В техническом задании на создание СБЗОКИИ должны быть описаны:</p> <ul style="list-style-type: none"> цель и задачи обеспечения безопасности значимого объекта или системы безопасности значимого объекта; категория значимости значимого объекта; перечень нормативных правовых актов, методических документов и национальных стандартов, которым должен соответствовать значимый объект; перечень типов объектов защиты значимого объекта; организационные и технические меры, применяемые для обеспечения безопасности значимого объекта; стадии (этапы работ) создания системы безопасности значимого объекта; требования к применяемым программным и программно-аппаратным средствам, в том числе средствам защиты информации; требования к защите средств и систем, обеспечивающих функционирование значимого объекта (обеспечивающей инфраструктуре); требования к информационному взаимодействию значимого объекта с иными объектами КИИ, а также иными ИС, АСУ или ИТС. 	

3.3. Разработка организационных и технических мер по обеспечению безопасности значимого объекта КИИ

<p>Ссылка на НПА, НМД</p> <p>Приказ ФСТЭК России № 239, раздел II, п. 11</p>	<p>Сроки проведения</p> <p>—</p>
---	---

3.3.1. Анализ угроз безопасности информации и разработка модели угроз безопасности информации или ее уточнение при ее наличии

<p>Что делать</p> <ul style="list-style-type: none"> Выявить источники угроз безопасности информации и оценить возможности (потенциал) внешних и внутренних нарушителей Проанализировать возможные уязвимости значимого объекта и его программных, программно-аппаратных средств Определить возможные способы (сценарии) реализации (возникновения) угроз безопасности информации Оценить возможные последствия от реализации (возникновения) угроз безопасности информации 	<p>Сроки проведения</p> <p>—</p>
<p>Результаты</p> <p>Модель угроз безопасности информации значимого объекта КИИ (для каждого объекта КИИ или для нескольких объектов в случае одинаковых целей их создания и архитектуры)</p>	<p>Кто проводит (организует)</p> <p>Подразделение (ответственный) ИБ организации, лицензиат (ТЗКИ) ФСТЭК России</p> <p>Ссылка на НПА, НМД</p> <p>Приказ ФСТЭК России № 239, раздел II, п. 11.1, приказ ФСТЭК России № 235, п. 25</p>
<p>Примечание</p> <p>Модель угроз безопасности информации должна содержать:</p> <ul style="list-style-type: none"> краткое описание архитектуры значимого объекта; характеристику источников угроз безопасности информации, в том числе модель нарушителя; описание всех угроз безопасности информации, актуальных для значимого объекта. Описание каждой угрозы безопасности информации должно включать указания: <ul style="list-style-type: none"> на источник угрозы безопасности информации; уязвимости (ошибки), которые могут быть использованы для реализации (способствовать возникновению) угрозы безопасности информации; возможные способы (сценарии) реализации угрозы безопасности информации; возможные последствия от реализации угрозы безопасности информации. 	

3.3.2. Проектирование системы безопасности значимого объекта КИИ

Что делать	Сроки проведения
<ul style="list-style-type: none"> Разработать документацию технического проекта Макетировать СБЗОКИИ (при необходимости) 	—
	Кто проводит (организует) Подразделение (ответственный) ИБ организации, лицензиат (ТЗКИ) ФСТЭК России
Результаты Документация технического проекта	Ссылка на НПА, НМД Приказ ФСТЭК России № 239, раздел II, п. 11.3, приказ ФСТЭК России № 235, п. 25
Примечание <div> <div> Состав технического проекта: <ul style="list-style-type: none"> ведомость технического проекта; пояснительная записка к техническому проекту; схема структурная комплекса технических средств; описание комплекса технических средств; описание программного обеспечения; </div> <div> <ul style="list-style-type: none"> схема функциональной структуры; схема организационной структуры; описание организационной структуры; план расположения; сметы на создание системы. </div> </div> <p>Состав и содержание документации технического проекта определяются в соответствии с ГОСТ 34.201, РД 50-34.698-90.</p>	

3.3.3. Разработка рабочей (эксплуатационной) документации на СБЗОКИИ

Что делать	Сроки проведения
Разработать рабочую (эксплуатационную) документацию	—
	Кто проводит (организует) Подразделение (ответственный) ИБ организации, лицензиат (ТЗКИ) ФСТЭК России
Результаты Комплект рабочей (эксплуатационной) документации	Ссылка на НПА, НМД Приказ ФСТЭК России № 239, раздел II, п. 11.3
Примечание <div> <div> Рабочая (эксплуатационная) документация на значимый объект должна содержать: </div> <div> <ul style="list-style-type: none"> описание архитектуры системы безопасности значимого объекта; описание параметров и порядка настройки программных и программно-аппаратных средств, в том числе средств защиты информации; </div> <div> <ul style="list-style-type: none"> правила эксплуатации программных и программно-аппаратных средств, в том числе средств защиты информации (правила безопасной эксплуатации). </div> </div>	

3.4. Внедрение организационных и технических мер по обеспечению безопасности значимого объекта КИИ и ввод СБЗОКИИ в действие

Ссылка на НПА, НМД

Приказ ФСТЭК России № 239, раздел II, п. 12

Сроки проведения

—

3.4.1. Установка и настройка средств защиты информации, настройка программных и программно-аппаратных средств

Что делать

- Закупить программные и технические средства для СБЗОКИИ
- Поставить программные и технические средства для СБЗОКИИ на объекты КИИ
- Установить и настроить программные и программно-технические средства

Сроки проведения

Рекомендовано до 01.09.2019¹

Кто проводит (организует)

Подразделение (ответственный)
ИБ организации, лицензиат (ТЗКИ)
ФСТЭК России

Результаты

- Товарные накладные
- Акты передачи прав на ПО
- Акты проведения монтажных и пуско-наладочных работ (акты установки-настройки средств защиты)

Ссылка на НПА, НМД

Приказ ФСТЭК России № 239,
раздел II, п. 12.1

3.4.2. Разработка организационно-распорядительных документов о правилах и процедурах обеспечения безопасности значимого объекта КИИ

Что делать

Разработать комплект организационно-распорядительных документов по ИБ ЗОКИИ

Сроки проведения

—

Результаты

- Комплект ОРД ИБ ЗОКИИ:
- Политика идентификации и аутентификации
 - Политика управления доступом
 - Разрешительная система доступа к защищаемым ресурсам (матрица доступа)
 - Политика ограничения программной среды
 - Политика защиты машинных носителей
 - Журнал учета машинных носителей информации
 - Политика аудита безопасности
 - Политика антивирусной защиты
 - Политика предотвращения вторжений (компьютерных атак)
 - Политика обеспечения целостности
 - Политика обеспечения доступности
 - Политика защиты технических средств и систем
 - План контролируемой зоны
 - Политика защиты информационной (автоматизированной) системы и ее компонентов
 - Политика реагирования на компьютерные инциденты
 - Политика управления конфигурацией информационной (автоматизированной) системы
 - Технический паспорт ОККИ
 - Перечень разрешенного к использованию программного обеспечения
 - Политика управления обновлениями программного обеспечения
 - Политика планирования мероприятий по обеспечению защиты информации
 - План мероприятий по обеспечению безопасности значимых ОККИ
 - Политика обеспечения действий в нештатных ситуациях
 - Политика информирования и обучения персонала

Кто проводит (организует)

Подразделение (ответственный)
ИБ организации, лицензиат (ТЗКИ)
ФСТЭК России

Ссылка на НПА, НМД

Приказ ФСТЭК России № 239,
раздел II, п. 12.2, приказ ФСТЭК
России № 235, п. 25

3.4.3. Внедрение организационных мер по обеспечению безопасности значимого объекта КИИ

Что делать	Сроки проведения
Разработать и утвердить приказ (распоряжение) о внедрении организационных мер по обеспечению безопасности значимого объекта КИИ в организации	—
	Кто проводит (организует)
	Подразделение (ответственный) ИБ организации
Результаты	Ссылка на НПА, НМД
<ul style="list-style-type: none"> Приказ (распоряжение) о внедрении организационных мер по обеспечению безопасности значимого объекта КИИ в организации Комплект ОРД ЗОКИИ (в части ИБ) — приложение к приказу (распоряжению) 	Приказ ФСТЭК России № 239, раздел II, п. 12.3
Примечание	
Приказ (распоряжение) о внедрении организационных мер по обеспечению безопасности значимого объекта КИИ в организации должен содержать:	<ul style="list-style-type: none"> имя и должность лица (лиц), назначенного администратором безопасности значимого объекта КИИ; имя и должность лица, на которое возлагается контроль за выполнением приказа (распоряжения); комплект вводимой в действие ОРД ЗОКИИ в части ИБ (в приложении).

3.4.4. Предварительные испытания значимого объекта КИИ и его системы безопасности

Что делать	Сроки проведения
Провести предварительные испытания в соответствии с программой и методикой предварительных испытаний	—
Результаты	Кто проводит (организует)
<ul style="list-style-type: none"> Программа и методика предварительных испытаний Приказ (распоряжение) о проведении предварительных испытаний СБЗОКИИ Протокол проведения предварительных испытаний СБЗОКИИ Акт приемки СБЗОКИИ в опытную эксплуатацию 	Подразделение (ответственный) ИБ организации, лицензиат (ТЗКИ) ФСТЭК России Ссылка на НПА, НМД Приказ ФСТЭК России № 239, раздел II, п. 12.4

3.4.5. Опытная эксплуатация СБЗОКИИ в составе значимого объекта КИИ

Что делать	Сроки проведения
Проверить функционирование системы безопасности значимого объекта, в том числе реализованных организационных и технических мер, а также знаний и умений пользователей и администраторов, необходимых для эксплуатации значимого объекта и его системы безопасности	—
	Кто проводит (организует)
	Подразделение (ответственный) ИБ организации, лицензиат (ТЗКИ) ФСТЭК России
Результаты	Ссылка на НПА, НМД
<ul style="list-style-type: none"> Программа и методика опытной эксплуатации Журнал опытной эксплуатации 	Приказ ФСТЭК России № 239, раздел II, п. 12.5

3.4.6. Анализ уязвимостей значимого объекта КИИ и принятие мер по их устранению

Что делать

- Провести анализ уязвимостей значимого объекта
- Оформить результаты анализа уязвимостей значимого объекта

Сроки проведения

—

Кто проводит (организует)

Подразделение (ответственный)
ИБ организации, лицензиат (ТЗКИ)
ФСТЭК России

Результаты

Протокол проведения анализа уязвимостей значимого объекта КИИ

Ссылка на НПА, НМД

Приказ ФСТЭК России № 239,
раздел II, п. 12.6

Примечание

По результатам анализа уязвимостей должно быть подтверждено, что в значимом объекте отсутствуют по крайней мере уязвимости, содержащиеся в банке данных угроз безопасности информации ФСТЭК России.

3.4.7. Приемочные испытания значимого объекта КИИ и его системы безопасности

Что делать

Провести приемочные испытания значимого объекта КИИ и его системы безопасности

Сроки проведения

—

Результаты

- Программа и методика приемочных испытаний
- Приказ (распоряжение) организации о проведении приемочных испытаний СБЗОКИИ
- Протокол проведения приемочных испытаний СБЗОКИИ
- Акт приемки СБЗОКИИ в эксплуатацию

Кто проводит (организует)

Подразделение (ответственный)
ИБ организации, лицензиат (ТЗКИ)
ФСТЭК России

Ссылка на НПА, НМД

Приказ ФСТЭК России № 239,
раздел II, п. 12.7

3.4.8. Аттестация значимого объекта КИИ

Что делать

- Разработать программу и методику аттестационных испытаний
- Провести комплексные испытания значимого объекта КИИ в реальных условиях эксплуатации
- Оформить результаты аттестационных испытаний

Сроки проведения

—

Кто проводит (организует)

Лицензиат (ТЗКИ) ФСТЭК России
с аттестатом аккредитации⁶

Результаты

- Приказ (распоряжение) о внедрении организационных мер по обеспечению безопасности значимого объекта КИИ в организации
- Комплект ОРД ЗОКИИ (в части ИБ) — приложение к приказу (распоряжению)

Ссылка на НПА, НМД

Приказ ФСТЭК России № 239,
раздел II, п. 12.7

Примечание

Аттестация ЗОКИИ проводится обязательно, если:

- ЗОКИИ является ГИС;
- ЗОКИИ обрабатывает гостайну.

По решению руководителя организации оценка соответствия ОКИИ требованиям по ЗИ может быть проведена в форме аттестации.

⁶ В данном случае участие лицензиата обязательно.

4. Обеспечение безопасности значимого объекта КИИ в ходе его эксплуатации

Что делать

- Актуализировать модель угроз безопасности
- Актуализировать документацию технического проекта
- Актуализировать организационно-распорядительную документацию
- Выполнять требования политик, инструкции, регламенты по управлению и эксплуатации СБЗОКИИ

Сроки проведения

В течение всего срока эксплуатации ЗОКИИ

Кто проводит (организует)

Подразделение (ответственный)
ИБ организации, лицензиат (ТЗКИ)
ФСТЭК России

Ссылка на НПА, НМД

Приказ ФСТЭК России № 239,
раздел II, п. 13

5. Обеспечение безопасности значимого объекта КИИ при выводе его из эксплуатации

Что делать

- Заархивировать информацию, содержащуюся в значимом объекте
- Уничтожить данные, остаточную информацию с машинных носителей информации и (или) машинные носители
- Уничтожить данные об архитектуре и конфигурации значимого объекта
- Заархивировать или уничтожить эксплуатационную документацию на значимый объект и его систему безопасности и организационно-распорядительные документы по безопасности значимого объекта

Сроки проведения

—

Кто проводит (организует)

Подразделение (ответственный) ИБ организации

Результаты

- Акты уничтожения информации с машинных носителей
- Акты уничтожения носителей информации
- Акты архивирования (уничтожения) документации на ЗОКИИ

Ссылка на НПА, НМД

Приказ ФСТЭК России № 239,
раздел II, п. 14

О компании

ptsecurity.com
pt@ptsecurity.com

facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.