**Название Компании**

**ПЛАН МЕРОПРИЯТИЙ ПО РЕАЛИЗАЦИИ ТРЕБОВАНИЙ**

**187-ФЗ «о БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ»**

ЛИСТОВ 24

ВЕРСИЯ 1

|  |  |  |
| --- | --- | --- |
| **Согласовано** |  | **Согласовано** |
|  |  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2020 г. |  | «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2020 г. |
| **Согласовано** |  | **Согласовано** |
|  |  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2020 г. |  | «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2020 г. |

**ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ**

| **Изм. №** | **Номера листов (страниц)** | | | | **Всего листов (страниц) в документе** | **№ документа** | **Входящий № сопроводительного документа и дата** | **Подпись ответственного за изменения** | **Дата** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Измененных** | **Замененных** | **Новых** | **Аннулированных** |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

**СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ**

|  |  |
| --- | --- |
| **АСУ** | Автоматизированная система управления |
| **ГОСТ** | Государственный стандарт |
| **ЗОКИИ** | Значимый объект критической информационной инфраструктуры |
| **ИБ** | Информационная безопасность |
| **ИС** | Информационная система |
| **ИТС** | Информационно-телекоммуникационная система |
| **КИИ** | Критическая информационная инфраструктура |
| **НКЦКИ** | Национальный координационный центр по компьютерным инцидентам |
| **ОКИИ** | Объект критической информационной инфраструктуры |
| **ОРД** | Организационно-распорядительная документация |
| **ПО** | Программное обеспечение |
| **ПП** | Постановление правительства |
| **РД** | Руководящий документ |
| **СБЗОКИИ** | Система безопасности значимого объекта критической информационной инфраструктуры |
| **СЗИ** | Средства защиты информации |
| **ТЗКИ** | Техническая защита конфиденциальной информации |
| **ФЗ** | Федеральный закон |
| **ФСБ России** | Федеральная служба безопасности Российской Федерации |
| **ФСТЭК России** | Федеральная служба по техническому и экспортному контролю Российской Федерации |

# План мероприятий по реализации требований 187-ФЗ «О критической информационной инфраструктуры Российской Федерации»

| **№** | **Работы** | **Комментарий** | **Нормативный документ** | **Результат** | **Ответственный** | **Рекомендуемые сроки[[1]](#footnote-1)** | **Отметка о выполнении** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Разработка перечня объектов КИИ, подлежащих категорированию | Перечень объектов КИИ, подлежащих категорированию, должен содержать следующую информацию:   * наименование субъекта КИИ; * наименование объекта КИИ; * указание на сферу (область) деятельности, в которой функционирует объект; * адрес размещения объекта КИИ; * ориентировочный срок категорирования. | ПП РФ № 127, п. 5 (г), п. 14 (в, г), п. 15 | Акт формирования перечня объектов КИИ, подлежащих категорированию | Комиссия по категорированию объектов КИИ | - |  |
|  | Утверждение перечня объектов КИИ, подлежащих категорированию | Перечень выявленных объектов критической информационной инфраструктуры утверждается субъектом критической информационной инфраструктуры.  Перечень объектов подлежит согласованию с государственным органом или российским юридическим лицом, выполняющим функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере в части подведомственных им субъектов критической информационной инфраструктуры. | ПП РФ № 127, п. 5 (г), п. 14 (в, г), п. 15 | Утвержденный акт формирования перечня объектов КИИ, подлежащих категорированию | Комиссия по категорированию объектов КИИ | 30.08.2019 |  |
|  | Разработка Регламента информирования ФСБ России | Субъекты КИИ обязаны незамедлительно информировать о компьютерных инцидентах федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. | 187-ФЗ (ст. 9, ч. 2, п. 1), приказ ФСБ России № 367 | 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. | Подразделение (ответственный) ИБ организации, лицензиат (ТЗКИ) ФСТЭК России | С момента определения статуса субъекта КИИ |  |
|  | Информирование о компьютерных инцидентах НКЦКИ | Информация о компьютерном инциденте, связанном с функционированием значимого объекта КИИ, направляется субъектом КИИ в НКЦКИ в срок не позднее 3 часов с момента обнаружения компьютерного инцидента, а в отношении иных объектов КИИ – в срок не позднее 24 часов с момента его обнаружения | Приказ ФСБ России № 282, п. 4 |  | Подразделение (ответственный) ИБ организации | С момента разработки Регламента информирования ФСБ России |  |
|  | Отправка перечня объектов КИИ, подлежащих категорированию во ФСТЭК России | Отправка перечня осуществляется не позднее 10-ти рабочих дней после утверждения.  Рекомендуемая форма перечня ОКИИ, подлежащих категорированию представлена в Приложении 1 к информационному сообщению от 17.04.2020 г. № 240/84/611 | ПП РФ № 127, п. 15 | Форма перечня ОКИИ, подлежащих категорированию | Комиссия по категорированию объектов КИИ | 13.09.2019 |  |
|  | Определение категории значимости объектов КИИ (категорирование), утверждение акта категорирования | 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.  Срок категорирования не должен превышать 1 год с момента утверждения перечня объектов КИИ, подлежащих категорированию (см. пункт 2). | ПП РФ № 127, п. 14 (е, ж) | Акт категорирования объекта КИИ (для каждого объекта КИИ) | Комиссия по категорированию объектов КИИ | 28.08.2020 |  |
|  | Подготовка и утверждение форм направления сведений о присвоении категории объектов КИИ | В рамках подготовки форм направления сведений о категорировании ОКИИ необходимо подготовить сведения о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.  Форма утверждается руководителем субъекта КИИ или уполномоченным им лицом. | ПП РФ № 127, п. 17, приказ ФСТЭК России № 236; 187-ФЗ (ст. 6, ч. 3, п. 3) | Форма направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий (отдельно для каждого объекта КИИ) | Комиссия по категорированию объектов КИИ | 28.08.2020 |  |
|  | Отправка форм направления сведений о присвоении категории объектов КИИ | В рамках подготовки сведений о категорировании ОКИИ необходимо направить сведения во ФСТЭК России в форме, представленной в приказе ФСТЭК России № 236.  Срок отправки формы направления сведений во ФСТЭК России не должен превышать 10 рабочих дней с момента утверждения акта категорирования (см. пункт 6). | ПП РФ № 127, п. 17, приказ ФСТЭК России № 236; 187-ФЗ (ст. 6, ч. 3, п. 3) | Документ, содержащий 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) | Комиссия по категорированию объектов КИИ | 11.09.2020 |  |
|  | Проверка соблюдения порядка категорирования и правильности присвоения ОКИИ одной из категорий значимости либо не присвоения ему ни одной из таких категорий | ФСТЭК России в тридцатидневный срок со дня получения сведений, проверяет соблюдение порядка осуществления категорирования и правильность присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо не присвоения ему ни одной из таких категорий | 187-ФЗ (ст. 7, ч. 6) | Уведомление о внесении сведений об объекте КИИ в реестр ЗОКИИ или возврат сведений в письменном виде с мотивированным обоснованием причин возврата. | Комиссия по категорированию объектов КИИ | - |  |
|  | Получение мотивированного обоснования причин возврата форм, в случае выявления нарушения порядка категорирования | В случае, если ФСТЭК России, выявлены нарушения порядка осуществления категорирования и (или) объекту критической информационной инфраструктуры, принадлежащему на праве собственности, аренды или ином законном основании субъекту критической информационной инфраструктуры, неправильно присвоена одна из категорий значимости и (или) необоснованно не присвоена ни одна из таких категорий и (или) субъектом критической информационной инфраструктуры представлены неполные и (или) недостоверные сведения о результатах присвоения такому объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, ФСТЭК России в десятидневный срок со дня поступления представленных сведений возвращает их в письменном виде субъекту критической информационной инфраструктуры с мотивированным обоснованием причин возврата. | 187-ФЗ (ст. 7, ч. 8) | Возврат сведений в письменном виде с мотивированным обоснованием причин возврата. | Комиссия по категорированию объектов КИИ | - |  |
|  | Исправление выявленных нарушений порядка категорирования и правильности присвоения ОКИИ одной из категорий значимости либо не присвоения ему ни одной из таких категорий | Субъект КИИ после получения мотивированного обоснования причин возврата сведений, не более чем в десятидневный срок устраняет отмеченные недостатки и повторно направляет такие сведения во ФСТЭК России | 187-ФЗ (ст. 7, ч. 9) | Исправленная форма направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий (отдельно для каждого объекта КИИ) | Комиссия по категорированию объектов КИИ | - |  |
|  | Получение уведомления о внесении в реестр ЗОКИИ | ФСТЭК России вносит сведения о таком ОКИИ в реестр ЗОКИИ, о чем в десятидневный срок уведомляется субъект КИИ | 187-ФЗ (ст. 7, ч. 7) | Уведомление о внесении сведений об объекте КИИ в реестр ЗОКИИ | Комиссия по категорированию объектов КИИ | 12.10.2020[[2]](#footnote-2) |  |
|  | Разработка и утверждение руководителем организации приказа (распоряжения) о создании системы безопасности значимых объектов КИИ | В приказе (распоряжении) должны быть указаны по меньшей мере:   * цели создания СБЗОКИИ; * структурные подразделения (работники), ответственные за обеспечение безопасности значимых объектов КИИ, и их функции по обеспечению безопасности значимых объектов КИИ; * сроки создания СБЗОКИИ; * ответственные за создание СБЗОКИИ; * лицо, осуществляющее контроль за созданием СБЗОКИИ. | 187-ФЗ (ст. 10, ч. 1), приказ ФСТЭК России № 235 (раздел II, п. 8, 9, 10) | Приказ (распоряжение) о создании системы безопасности значимых объектов КИИ | Руководитель организации, подразделение (ответственный) ИБ организации | 16.10.2020 |  |
|  | Подготовка к реагированию на компьютерные инциденты | Для подготовки к реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак субъектом критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежит значимый объект критической информационной инфраструктуры, в срок до 90 календарных дней со дня включения данного объекта в реестр значимых объектов критической информационной инфраструктуры Российской Федерации разрабатывается план реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак | Приказ ФСБ России № 282, п. 6 | Проект плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак | Подразделение (ответственный) ИБ организации, субъекты (центры) НКЦКИ (при необходимости) | 12.01.2021 |  |
|  | Согласование плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных инцидентов с ФСБ России | Разработанный проект план реагирования на инциденты направляется в ФСБ России. ФСБ России в течении 30 календарных дней рассматривает проект плана и по результатам рассмотрения согласовывает его или возвращает без согласования для доработки | Приказ ФСБ России № 282, п. 8 | Согласованный план реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак | Подразделение (ответственный) ИБ организации | 12.02.2021 |  |
|  | Тренировки по отработке мероприятий Плана | Субъект критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, не реже одного раза в год организует и проводит тренировки по отработке мероприятий Плана. Объем и содержание тренировки определяются субъектом критической информационной инфраструктуры с учетом мероприятий, содержащихся в Плане.  Организация и проведение тренировок возлагаются на подразделения и должностных лиц субъекта критической информационной инфраструктуры, ответственных за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак. | Приказ ФСБ России № 282, п. 10 | Отчетные документы по результатам отработки мероприятий Плана, аттестация работников | Подразделение (ответственный) ИБ организации | Ежегодно, начиная с 12.02.2021 |  |
|  | Разработка моделей угроз безопасности информации ЗОКИИ или их уточнение при наличии, в том числе модели нарушителя | Модель угроз безопасности информации должна содержать:   * 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:   * 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. | Приказ ФСТЭК России № 239, раздел II, п. 11.1, приказ ФСТЭК России № 235, п. 25 | Модель угроз безопасности информации ЗОКИИ (для каждого объекта КИИ или для нескольких объектов в случае одинаковых целей их создания и архитектуры) | Подразделение (ответственный) ИБ организации, лицензиат (ТЗКИ) ФСТЭК России | Февраль-Март 2021 г. |  |
|  | Формирование требований к системе обеспечения безопасности значимых объектов КИИ | В техническом задании на создание СБЗОКИИ должны быть описаны:   * 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. | Приказ ФСТЭК России № 239, раздел II, п. 10 | Техническое задание на создание СБЗОКИИ | Подразделение (ответственный) ИБ организации, лицензиат (ТЗКИ) ФСТЭК России | Апрель 2021 г. |  |
|  | Эскизное проектирование системы безопасности значимого объекта КИИ | Состав технического проекта:   * ведомость технического проекта; * пояснительная записка к техническому проекту; * схема структурная комплекса технических средств; * описание комплекса технических средств; * описание программного обеспечения; * схема функциональной структуры; * схема организационной структуры; * план расположения серверных стоек; * план расположения оборудования в серверных стойках; * план расположения оборудования и проводок; * спецификация оборудования и ПО. | Приказ ФСТЭК России № 239, раздел II, п. 11.3, приказ ФСТЭК России № 235, п. 25  Состав и содержание документации технического проекта определяются в соответствии с ГОСТ 34.201, РД 50-34.698-90. | Документация технического проекта | Подразделение (ответственный) ИБ организации, лицензиат (ТЗКИ) ФСТЭК России | Май – Июль 2021 г.[[3]](#footnote-3) |  |
|  | Разработка организационно-распорядительных документов о правилах и процедурах обеспечения безопасности значимого объекта КИИ | Разрабатываемая организационно-распорядительная документация должна:   * определять правила и процедуры реализации отдельных организационных и (или) технических мер (политик безопасности); * устанавливать правила безопасной работы работников, эксплуатирующих значимые объекты, и работников, обеспечивающих функционирование значимых объектов, а также действия работников при возникновении нештатных ситуаций, в том числе вызванных компьютерными инцидентами. | Приказ ФСТЭК России № 239, раздел II, п. 12.2, приказ ФСТЭК России № 235, п. 25, приказ ФСТЭК России № 17, п. 25 | Комплект ОРД ИБ ЗОКИИ | Подразделение (ответственный) ИБ организации, лицензиат (ТЗКИ) ФСТЭК России | Июль – Август 2021 г. |  |
|  | Утверждение приказа (распоряжения) о внедрении организационных мер по обеспечению безопасности значимого объекта КИИ | Приказ (распоряжение) о внедрении организационных мер по обеспечению безопасности значимого объекта КИИ в организации должен содержать:   * 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). | Приказ ФСТЭК России № 239, раздел II, п. 12.3 | Приказ (распоряжение) о внедрении организационных мер по обеспечению безопасности значимого объекта КИИ в организации.  Комплект ОРД ЗОКИИ (в части ИБ) — приложение к приказу. | Подразделение (ответственный) ИБ организации | Сентябрь  2021 г. |  |
|  | Пилотирование (макетирование) СЗИ | В целях тестирования подсистемы безопасности значимого объекта в ходе проектирования может осуществляться ее макетирование или создание тестовой среды. Тестирование должно быть направлено на:   * обеспечение работоспособности и совместимости выбранных средств защиты информации с программными и аппаратными средствами значимого объекта; * практическую отработку выполнения средствами защиты информации функций безопасности; * исключение влияния подсистемы безопасности на функционирование значимого объекта. | Приказ ФСТЭК России № 239, раздел II, п. 11.2 | Отчет о тестировании подсистемы безопасности значимого объекта КИИ | Подразделение (ответственный) ИБ организации, лицензиат (ТЗКИ) ФСТЭК России | Сентябрь-Декабрь 2021 г. |  |
|  | Поставка СЗИ | Закупка и поставка программно-аппаратных средств, оборудования, а также средств защиты информации определенных и согласованных в эскизном проекте систем безопасности ЗОКИИ.  При наличии согласия федерального органа исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, за свой счет приобретать, арендовать, устанавливать и обслуживать средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты | 187-ФЗ (ст. 9, ч. 1, п. 3) | Эксплуатационная документация от производителя программно-аппаратных средств, оборудования, а также средств защиты информации.  Комплект поставки.  Финансовая документация. | Подразделение (ответственный) ИБ организации, лицензиат (ТЗКИ) ФСТЭК России | Январь-Март  2022 г. |  |
|  | Разработка технорабочего проекта, рабочей (эксплуатационной) документации на СБЗОКИИ | Рабочая (эксплуатационная) документация на значимый объект должна содержать:   * описание архитектуры системы безопасности значимого объекта; * описание параметров и порядка 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). | Приказ ФСТЭК России № 239, раздел II, п. 11.3 | Комплект рабочей (эксплуатационной) документации | Подразделение (ответственный) ИБ организации, лицензиат (ТЗКИ) ФСТЭК России | Апрель-Август  2022 г. |  |
|  | Пусконаладочные работы - установка и настройка средств защиты информации, настройка программных и программно-аппаратных средств | Для реализации этапа пусконаладочных работ необходимо:   * 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. | Приказ ФСТЭК России № 239, раздел II, п. 12.1 | Товарные накладные.  Акты передачи прав на ПО.  Акты проведения монтажных и пуско-наладочных работ (акты установки-настройки средств защиты). | Подразделение (ответственный) ИБ организации, лицензиат (ТЗКИ) ФСТЭК России | Сентябрь-Октябрь  2022 г. |  |
|  | Предварительные испытания значимого объекта КИИ и его системы безопасности | Предварительные испытания ЗОКИИ и его системы безопасности должны проводиться в соответствии с программой и методиками предварительных испытаний. А также включать проверку работоспособности подсистемы безопасности значимого объекта и отдельных СЗИ, оценку влияния подсистемы безопасности на функционирование значимого объекта при проектных режимах его работы, установленных проектной документацией, а также принятие решения о возможности опытной эксплуатации значимого объекта и его подсистемы безопасности. | Приказ ФСТЭК России № 239, раздел II, п. 12.4 | 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 | Ноябрь  2022 г. |  |
|  | Опытная эксплуатация СБЗОКИИ в составе значимого объекта КИИ | Опытная эксплуатация СБЗОКИИ в составе значимого объекта КИИдолжна проводиться в соответствии с программой и методиками опытной эксплуатации, а также включать проверку функционирования подсистемы безопасности значимого объекта, в том числе реализованных организационных и технических мер | Приказ ФСТЭК России № 239, раздел II, п. 12.5 | Программа и методика опытной эксплуатации.  Журнал опытной эксплуатации. | Подразделение (ответственный) ИБ организации, лицензиат (ТЗКИ) ФСТЭК России | Ноябрь  2022 г. |  |
|  | Анализ уязвимостей значимого объекта КИИ (тестирование на проникновение) и принятие мер по их устранению | В случае выявления уязвимостей значимого объекта, которые могут быть использованы для реализации угроз безопасности информации, принимаются меры, направленные на их устранение или исключающие возможность использования нарушителем выявленных уязвимостей. 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 | Приказ ФСТЭК России № 239, раздел II, п. 12.6 | Протокол проведения анализа уязвимостей значимого объекта КИИ | Подразделение (ответственный) ИБ организации, лицензиат (ТЗКИ) ФСТЭК России | Ноябрь-Декабрь 2022 г. |  |
|  | Приемочные испытания значимого объекта КИИ и его системы безопасности | В качестве исходных данных используется:   * модель угроз безопасности информации; * результаты (акт) категорирования; * техническое задание на создание (модернизацию) значимого объекта и техническое задание на создание подсистемы безопасности значимого объекта; * проектная и рабочая документация на значимый объект; * организационно-распорядительные документы по безопасности значимых объектов; * результаты анализа уязвимостей значимого объекта; * материалы предварительных испытаний и опытной эксплуатации. | Приказ ФСТЭК России № 239, раздел II, п. 12.7 | Программа и методика приемочных испытаний.  Приказ (распоряжение) организации о проведении приемочных испытаний СБЗОКИИ.  Протокол проведения приемочных испытаний СБЗОКИИ.  Акт приемки СБЗОКИИ в эксплуатацию. | Подразделение (ответственный) ИБ организации, лицензиат (ТЗКИ) ФСТЭК России | Декабрь  2022 г. |  |
|  | Обеспечение безопасности значимого объекта КИИ в ходе его эксплуатации | На данном этапе необходима реализация следующих мероприятий:   * 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 работников значимого объекта; * контроль за обеспечением безопасности значимого объекта. | Приказ ФСТЭК России № 239, раздел II, п. 13 | Поддержка и совершенствование уровня процедур (мер) по ИБ значимого объекта КИИ в ходе его эксплуатации | Подразделение (ответственный) ИБ организации, лицензиат (ТЗКИ) ФСТЭК России | В течение всего срока эксплуатации ЗОКИИ |  |
|  | Пересмотр категории значимости объекта КИИ | В случае изменения категории значимости сведения о результатах пересмотра категории значимости направляются в федеральный орган, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры | ПП РФ № 127, п. 21 | Акт категорирования объекта КИИ (для каждого объекта КИИ) | Подразделение (ответственный) ИБ организации | Не позднее 28.08.2025 |  |
|  | Обеспечение безопасности значимого объекта КИИ при выводе его из эксплуатации | Обеспечение безопасности значимого объекта при выводе его из эксплуатации должно предусматривать:   * 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. | Приказ ФСТЭК России № 239, раздел II, п. 14 | Акты уничтожения информации с машинных носителей.  Акты уничтожения носителей информации.  Акты архивирования (уничтожения) документации на ЗОКИИ. | Подразделение (ответственный) ИБ организации | В течение срока вывода из эксплуатации ЗОКИИ |  |
|  | Плановая проверка | Основаниями для осуществления плановой проверки являются истечение 3-х лет со дня:   * внесения сведений об ОКИИ в реестр ЗОКИИ; * окончания осуществления последней плановой проверки в отношении ЗОКИИ.   Ежегодный план проведения плановых проверок утверждается руководителем органа государственного контроля до 20 декабря года, предшествующего году проведения плановых проверок.  Выписки из утвержденного ежегодного плана проведения плановых проверок направляются до 1 января года проведения плановых проверок органом государственного контроля субъектам критической информационной инфраструктуры.  О проведении плановой проверки субъект КИИ уведомляется органом государственного контроля не менее чем за 3 рабочих дня до начала ее проведения посредством направления копии приказа органа государственного контроля о проведении плановой проверки любым доступным способом, обеспечивающим возможность подтверждения факта такого уведомления.  Основаниями для осуществления внеплановой проверки являются:  истечение срока выполнения субъектом КИИ выданного органом государственного контроля предписания об устранении выявленного нарушения требований по обеспечению безопасности;  возникновение компьютерного инцидента на ЗОКИИ, повлекшего негативные последствия;  приказ органа государственного контроля, изданный в соответствии с поручением Президента Российской Федерации или Правительства Российской Федерации либо на основании требования прокурора об осуществлении внеплановой проверки в рамках проведения надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.  О проведении внеплановой проверки (за исключением внеплановой проверки, основание для осуществления которой указано в подпункте «б» пункта 20 настоящих Правил) субъект КИИ уведомляется органом государственного контроля не менее чем за 24 часа до начала ее проведения любым доступным способом, обеспечивающим возможность подтверждения факта такого уведомления. | ПП РФ № 162, раздел II, п. 11 – 18, раздел III, п. 19 – 21. | Акт с результатами проведения плановой проверки | Комиссия, ответственная за проведение плановой проверки | С 28.08.23 |  |

1. На основании Информационного сообщения ФСТЭК России от 17.04.2020 г. № 240/84/611 отправной датой при разработке настоящего Плана установлен срок утверждения перечня объектов КИИ, подлежащих категорированию, - 1 сентября 2019 г., а максимальный срок категорирования КИИ не должен превышать одного года со дня утверждения субъектом КИИ перечня объектов КИИ, подлежащих категорированию (внесения в него изменений). План рассчитан на 3 года с момента внесения значимых объектов КИИ в реестр, т.к. с этого момента возможны плановые проверки ФСТЭК России. Даты адаптированы под рабочие дни. [↑](#footnote-ref-1)
2. На практике ФСТЭК России не успевает проверять формы в регламентированные сроки и процесс согласования форм может затянуться, но если вы определили значимые объекты КИИ, то рекомендуется не останавливать работы по защите КИИ в связи с ожиданием ответа от ФСТЭК России [↑](#footnote-ref-2)
3. Здесь и далее указаны примерные сроки для среднестатистического предприятия (несколько филиалов/подразделений, 5-20 объектов КИИ). В зависимости от масштаба предприятия сроки могут быть существенно продлены. [↑](#footnote-ref-3)