

Ключевые шаги

по выполнению требований закона № 187-ФЗ
о безопасности критической информационной
инфраструктуры

0. Определение принадлежности организации к субъектам КИИ



до начала
категорирования

- + Составить перечень ИС, АСУ, ИТС организации с определением сферы функционирования каждой ИС, АСУ, ИТС
- + Сделать вывод о необходимости (или отсутствии необходимости) выполнения требований закона № 187-ФЗ

1. Категорирование объектов КИИ



до 01.09.2020

- + Создать комиссию по категорированию объектов КИИ
- + Определить перечень процессов деятельности организации и выявить критические процессы
- + Разработать перечень объектов КИИ, подлежащих категорированию, и направить во ФСТЭК России
- + Определить угрозы безопасности для объектов КИИ
- + Определить категории значимости для объектов КИИ
- + Подготовить и направить во ФСТЭК России на согласование 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)

2. Разработка мероприятий по взаимодействию с ФСБ России



с момента
определения
организации
как субъекта КИИ

- + Разработать и утвердить регламент информирования ФСБ России (НКЦКИ) о компьютерных инцидентах
- + Организовать взаимодействие с ФСБ России (НКЦКИ)

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
- + Разработать план реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак*

3. Создание системы безопасности значимых объектов КИИ

- + Разработать и утвердить приказ о создании системы безопасности значимых объектов КИИ
- + Установить требования к обеспечению безопасности значимых объектов КИИ — разработать техническое задание на создание системы безопасности
- + Разработать организационные и технические меры по обеспечению безопасности значимого объекта КИИ
 - Провести анализ угроз безопасности информации и разработать модель угроз
 - Спроектировать систему безопасности значимого объекта КИИ
 - Разработать рабочую (эксплуатационную) документацию на систему безопасности

* Для организаций, имеющих значимые объекты КИИ

- + Внедрить организационные и технические меры и ввести систему безопасности в действие
 - Установить и настроить средства защиты информации, программные и программно-аппаратные средства
 - Разработать организационно-распорядительные документы о правилах и процедурах обеспечения безопасности значимого объекта КИИ
 - Внедрить организационные меры по обеспечению безопасности значимого объекта КИИ (утвердить приказ о внедрении организационных мер)
 - Провести предварительные испытания значимого объекта КИИ и его системы безопасности
 - Провести опытную эксплуатацию системы безопасности в составе значимого объекта КИИ
 - Провести анализ уязвимостей значимого объекта КИИ и принять меры по их устранению
 - Провести приемочные испытания значимого объекта КИИ и его системы безопасности
 - Аттестовать значимый объект КИИ — если он является ГИС или обрабатывает гостайну

4. Обеспечение безопасности значимого объекта КИИ в ходе его эксплуатации



в течение всего срока эксплуатации объекта КИИ

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

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



в случае вывода объекта из эксплуатации

- + 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, организационно-распорядительные документы по безопасности значимого объекта



Подробный план по выполнению требований закона № 187-ФЗ вы можете скачать на [сайте Positive Technologies](https://www.ptsecurity.com)

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.