АКАДЕМИЯ АЙТИ

academyit.ru

Общий порядок организации обеспечения безопасности персональных данных в ИСПДн

Организация обеспечения безопасности ПДн - формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн.

Статья 19.

Меры по обеспечению безопасности персональных данных при их обработке

1. Оператор при обработке ПДн **обязан** принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн , а также от иных неправомерных действий в отношении ПДн.

152-ФЗ от 25 июля 2006

Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами

- назначить ответственного за организацию обработки ПДн
- разработать и утвердить необходимые документы
- принять правовые, организационные и технические меры по обеспечению безопасности персональных данных
- выполнить требования, установленные постановлением Правительства РФ от № 687 от 15 сентября 2008 г
- организовать проведение периодических проверок условий обработки ПДн
- знакомить служащих, непосредственно осуществляющих обработку ПДн, с положениями законодательства РФ о персональных данных
- уведомить Роскомнадзор об обработке (намерении осуществлять обработку) ПДн
- осуществить обезличивание персональных данных
- опубликовать документы, определяющие политику в отношении обработки персональных данных

Постановление правительства РФ № 211 от 21 марта 2012

Обеспечение безопасности персональных данных достигается

- определением угроз безопасности
- применением организационных и технических мер
- применением сертифицированных СрЗИ
- оценкой эффективности принимаемых мер
- учетом машинных носителей
- обнаружением фактов НСД и принятием мер
- восстановлением персональных данных
- установлением правил доступа
- обеспечением регистрации и учета всех действий
- контролем за принимаемыми мерами

152-ФЗ от 25 июля 2006

Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке ИСПДн

Устанавливает состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн для каждого из уровней защищенности ПДн, определяемых в соответствии с постановлением Правительства РФ от 1 ноября 2012 г. № 1119.

ЗАРЕГИСТРИРОВАНО
Регистрационный № 28375
от 14 мая 2013

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«18» февраля 2013 г. Москва № 21

Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

В соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2009, № 48, ст. 5716, № 52, ст. 6439; 2010, № 27, ст. 3407; № 31, ст. 4173, ст. 4196; № 49, ст. 6409; 2011, № 23, ст. 3263; № 31, ст. 4701) и Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818),

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемые Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

2. Признать утратившим силу приказ ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» (зарегистрирован Минюстом России 19 февраля 2010 г., регистрационный № 16456).

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.Селин

Приказ ФСТЭК России от 18 февраля 2013 г. № 21

Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке ИСПДн

Безопасность ПДн при их обработке в ИС **обеспечивает оператор** или **лицо, осуществляющее обработку** ПДн **по поручению** оператора.

Для выполнения работ по обеспечению безопасности ПДн при их обработке в информационной системе **могут привлекаться** на договорной основе юридическое лицо или индивидуальный предприниматель, имеющие лицензию на деятельность по ТЗКИ.

Приказ ФСТЭК России от 18 февраля 2013 г. № 21

Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке ИСПДн

Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных (СЗПДн), создаваемой в соответствии с **Требованиями** к защите персональных данных и должны быть направлены на нейтрализацию **актуальных угроз** безопасности ПДн.



Приказ ФСТЭК России от 18 февраля 2013 г. № 21

Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке ИСПДн

Меры по обеспечению безопасности ПДн реализуются **в том числе** посредством применения в ИСПДн СрЗИ, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации **актуальных угроз** безопасности персональных данных.

Приказ ФСТЭК России от 18 февраля 2013 г. № 21

Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке ИСПДн

Оценка эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности ПДн проводится

- оператором самостоятельно
- или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по ТЗКИ.

Указанная оценка проводится **не реже 1 раза в 3 года**.

Приказ ФСТЭК России от 18 февраля 2013 г. № 21

Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке ИСПДн

Меры по обеспечению безопасности персональных данных при их обработке в **государственных информационных системах** принимаются в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, устанавливаемыми ФСТЭК России в пределах своих полномочий в соответствии с **частью 5 статьи 16** Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Приказ ФСТЭК России от 18 февраля 2013 г. № 21

Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

Разработаны в соответствии с ФЗ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с учетом национальных стандартов РФ в области ЗИ и в области создания АС.

Устанавливаются требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от утечки по ТК, НСД, специальных воздействий на такую информацию (носители информации) в целях защита информации при обработке указанной информации в государственных информационных системах.

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

Могут применяться для защиты общедоступной информации, содержащейся в государственных информационных системах (ГИС).

Не рассматриваются требования о защите информации, связанные с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации.

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

Являются **обязательными** при обработке информации в ГИС, функционирующих на территории РФ, а также в муниципальных информационных системах, если иное не установлено законодательством Российской Федерации о местном самоуправлении.

Не распространяются на ГИС:

- Администрации Президента Российской Федерации,
- Совета Безопасности Российской Федерации,
- Федерального Собрания Российской Федерации,
- Правительства Российской Федерации,
- Конституционного Суда Российской Федерации,
- Верховного Суда Российской Федерации,
- Высшего Арбитражного Суда Российской Федерации
- Федеральной службы безопасности Российской Федерации.

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

При обработке в ГИС информации, содержащей **ПДн**, настоящие Требования применяются наряду с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

По решению обладателя информации (заказчика) или оператора настоящие Требования **могут** применяться для защиты информации, содержащейся в негосударственных информационных системах.

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах

Защита информации, содержащейся в ГИС, обеспечивается путем выполнения обладателем информации (заказчиком) и (или) оператором **требований к организации защиты информации**, содержащейся в информационной системе, и требований к мерам защиты информации, содержащейся в информационной системе.

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

В ИС **объектами защиты** являются:

- информация, содержащаяся в ИС
- технические средства **(СВТ, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации)**
- **ПО (общесистемное, прикладное, специальное)**
- информационные технологии
- средства защиты информации

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования к **организации ЗИ**, содержащейся в ИС

Для обеспечения ЗИ, содержащейся в ИС, оператором **назначается** структурное подразделение или должностное лицо (работник), **ответственные за защиту информации**.

Для проведения работ по защите информации в ходе создания и эксплуатации ИС обладателем информации (заказчиком) и оператором **при необходимости** привлекаются организации, имеющие лицензию на деятельность по ТЗКИ.

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Для обеспечения защиты информации, содержащейся в ИС, **применяются** СрЗИ, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации.

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- формирование требований к защите информации
- разработка системы защиты информации (СЗИ)
- внедрение системы защиты информации
- аттестация информационной системы по требованиям защиты информации и ввод ее в действие
- обеспечение ЗИ в ходе эксплуатации аттестованной ИС
- обеспечение ЗИ при выводе из эксплуатации аттестованной ИС

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- формирование требований **к защите информации**
- разработка системы защиты информации (СЗИ)
- внедрение системы защиты информации
- аттестация информационной системы по требованиям защиты информации и ввод ее в действие
- обеспечение ЗИ в ходе эксплуатации аттестованной ИС
- обеспечение ЗИ при выводе из эксплуатации аттестованной ИС

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Формирование требований **Осуществляется**

- обладателем информации (заказчиком)
- с учетом
  - ГОСТ Р 51583 «Защита информации. Порядок создания АС в защищенном исполнении. Общие положения»
  - ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования к **организации ЗИ**, содержащейся в ИС

Формирование требований
Включает:

- принятие решения о необходимости защиты информации
- классификацию информационной системы
- определение угроз безопасности информации, и разработку на их основе модели угроз безопасности информации
- определение требований к системе защиты информации

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Формирование требований Включает:

- **принятие решения** о необходимости защиты информации

  Осуществляется:
  - анализ целей создания и задач, решаемых ИС
  - определение информации, подлежащей обработке в ИС
  - анализ НМД и стандартов, которым должна соответствовать ИС
  - принятие решения о необходимости создания СЗИ, а также определение целей и задач защиты информации в ИС, основных этапов создания СЗИ и функций по обеспечению ЗИ, содержащейся в ИС, обладателя информации (заказчика), оператора и уполномоченных лиц

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования к **организации ЗИ**, содержащейся в ИС

Формирование требований
Включает:

- **классификация** информационной системы
  - проводится в зависимости от значимости информации и масштаба ИС
  - определяется в соответствии с приложением № 1 к настоящим Требованиям
  - определяется для ИС в целом и, при необходимости, для сегментов
  - требование к классу защищенности включается в ТЗ (ЧТЗ), разрабатываемые с учетом ГОСТ 34.602 «ИТ. Комплекс стандартов на АС. ТЗ на создание АС»
  - подлежит пересмотру при изменении масштаба ИС или значимости обрабатываемой в ней информации
  - результаты классификации ИС оформляются актом классификации

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Формирование требований Включает:

- определение **угроз** безопасности информации, и разработку на их основе модели угроз безопасности информации

Основа:

- оценка возможности (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей
- анализ возможных уязвимостей информационной системы
- анализ возможных способов реализации угроз безопасности информации
- анализ последствий от нарушения свойств безопасности информации (КЦД)

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Формирование требований
Включает:

- определение **угроз** безопасности информации, и разработку на их основе модели угроз безопасности информации

Учитываются:

- структурно-функциональные характеристики ИС **(структура и состав ИС, физические, логические, функциональные и технологические взаимосвязи между сегментами ИС, с иными ИС и ИТС)**
- режимы обработки информации в ИС и в ее отдельных сегментах
- иные характеристики ИС
- применяемые ИТ
- особенности функционирования ИС

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Формирование требований
Включает:

- определение **угроз** безопасности информации, и разработку на их основе модели угроз безопасности информации

По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик ИС, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Формирование требований
Включает:

- определение **угроз** безопасности информации, и разработку на их основе модели угроз безопасности информации

Модель угроз безопасности информации **должна** содержать описание**:**

- ИС и ее структурно-функциональных характеристик
- угроз безопасности информации, включающее описание:
  - возможности нарушителей (модель нарушителя)
  - возможные уязвимости ИС
  - способы реализации угроз безопасности информации
  - последствия от нарушения свойств безопасности информации

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Формирование требований включает:

- определение **требований** к системе защиты информации

определяются в зависимости от

- класса защищенности ИС
- угроз безопасности информации

включаются в ТЗ на создание ИС и (или) ТЗ (ЧТЗ) на создание СЗИ

- ГОСТ 34.602, ГОСТ Р 51583 и ГОСТР 51624

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Формирование требований Включает:

- определение **требований** к системе защиты информации

Должны содержать:

- цель и задачи обеспечения ЗИ в ИС
- класс защищенности ИС
- перечень НМД, которым должна соответствовать ИС
- перечень объектов защиты ИС
- требования к мерам и средствам ЗИ, применяемым в ИС
- требования к ЗИ при информационном взаимодействии с иными ИС и ИТС, в том числе с ИС уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- формирование требований к защите информации
- разработка системы защиты информации (СЗИ)
- внедрение системы защиты информации
- аттестация информационной системы по требованиям защиты информации и ввод ее в действие
- обеспечение ЗИ в ходе эксплуатации аттестованной ИС
- обеспечение ЗИ при выводе из эксплуатации аттестованной ИС

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- разработка системы защиты информации (СЗИ)
  - организуется обладателем информации (заказчиком)
  - осуществляется
    - в соответствии с ТЗ на создание ИС и (или) ТЗ (ЧТЗ) на создание СЗИ информационной системы
    - с учетом ГОСТ 34.601 «ИТ. Комплекс стандартов на АС. АС. Стадии создания», ГОСТ Р 51583 и ГОСТ Р 51624

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- разработка системы защиты информации (СЗИ)

  Включает:

  - проектирование СЗИ информационной системы
  - разработку эксплуатационной документации на СЗИ
  - макетирование и тестирование СЗИ (при необходимости)

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- разработка системы защиты информации (СЗИ)

Включает:

- проектирование СЗИ информационной системы
- разработку эксплуатационной документации на СЗИ
- макетирование и тестирование СЗИ (при необходимости)

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Проектирование СЗИ

- определяются типы субъектов доступа **(пользователи, процессы и иные субъекты доступа)** и объектов доступа, являющихся объектами защиты **(устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным ПО, иные объекты доступа)**

- определяются методы управления доступом **(дискреционный, мандатный, ролевой или иные методы)**, типы доступа **(чтение, запись, выполнение или иные типы доступа)** и правила разграничения доступа субъектов доступа к объектам доступа **(на основе списков, меток безопасности, ролей и иных правил)**, подлежащие реализации в ИС

- выбираются меры защиты информации, подлежащие реализации в системе защиты информации информационной системы

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Проектирование СЗИ

- определяются виды и типы СрЗИ, обеспечивающие реализацию технических мер защиты информации
- определяется структура СЗИ информационной системы, включая состав (количество) и места размещения ее элементов
- осуществляется выбор СрЗИ, **сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы**

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования к **организации ЗИ**, содержащейся в ИС

Проектирование СЗИ

- определяются параметры настройки ПО, включая ПО СрЗИ, обеспечивающие реализацию мер ЗИ, а также устранение возможных уязвимостей ИС, приводящих к возникновению угроз безопасности

- определяются меры ЗИ при информационном взаимодействии с иными ИС и ИТС, в том числе с ИС уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Проектирование СЗИ

Результаты отражаются в **проектной документации** ГОСТ 34.201 «ИТ. Комплекс стандартов на АС. Виды, комплектность и обозначение документов при создании автоматизированных систем».

Проектная документация подлежит согласованию с оператором ИС При отсутствии необходимых сертифицированных СрЗИ:

- организуется разработка (доработка) СрЗИ и их сертификация
- производится корректировка проектных решений с учетом функциональных возможностей имеющихся сертифицированных СрЗИ

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Разработка эксплуатационной документации

- осуществляется в соответствии с ТЗ (ЧТЗ) на создание СЗИ
- с учетом ГОСТ 34.601, ГОСТ 34.201 и ГОСТ Р 51624

- должна содержать описание:
  - структуры СЗИ
  - состава, мест установки, параметров и порядка настройки СрЗИ, ПО и технических средств
  - правил эксплуатации СЗИ

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Макетирование и тестирование СЗИ

- проверка работоспособности и совместимости СрЗИ с ИТ и ТСр
- проверка выполнения выбранными СрЗИ требований к СЗИ
- корректировка проектных решений
- корректировка проектной и эксплуатационной документации на СЗИ

Может проводиться с использованием средств и методов моделирования информационных систем и технологий виртуализации.

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- формирование требований к защите информации
- разработка системы защиты информации (СЗИ)
- внедрение системы защиты информации
- аттестация информационной системы по требованиям защиты информации и ввод ее в действие
- обеспечение ЗИ в ходе эксплуатации аттестованной ИС
- обеспечение ЗИ при выводе из эксплуатации аттестованной ИС

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- внедрение системы защиты информации

Включает:

- установку и настройку СрЗИ
- разработку ОРД по ЗИ внедрение организационных мер ЗИ
- предварительные испытания СЗИ
- опытную эксплуатацию СЗИ
- анализ уязвимостей ИС и принятие мер ЗИ по их устранению
- приемочные испытания СЗИ

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- внедрение системы защиты информации

Включает:

установку и настройку СрЗИпроводится в соответствии с эксплуатационной документацией

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- внедрение системы защиты информации

Включает:

- разработку **ОРД** по ЗИ внедрение организационных мер ЗИ

Должны определять правила и процедуры:

– управления (администрирования) СЗИ
– выявления инцидентов и реагирования на них
– управления конфигурацией аттестованной ИС и СЗИ
– контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС
– защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- внедрение системы защиты информации

Включает:

- разработку **ОРД** по ЗИ внедрение организационных мер ЗИ

Осуществляются:

– реализация ПРД и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения

– проверка полноты и детальности описания в ОРД по ЗИ действий пользователей и администраторов ИС по реализации организационных мер

– отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- внедрение системы защиты информации

Включает:

- предварительные испытания СЗИ

  – проводятся с учетом ГОСТ 34.603 «Информационная технология. Виды испытаний автоматизированных систем»

  – включают:
    - проверку работоспособности СЗИ
    - принятие решения о возможности опытной эксплуатации СЗИ

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- внедрение системы защиты информации

Включает:

- опытную эксплуатацию СЗИ

  – проводится с учетом ГОСТ 34.603
  – включает
    - проверку функционирования СЗИ
    - готовность пользователей и администраторов к эксплуатации

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- внедрение системы защиты информации

Включает:

- анализ уязвимостей ИС и принятие мер ЗИ по их устранению

  Включает:

  – анализ уязвимостей СрЗИ, ТСр и ПО

  Проверяется:

  – отсутствие известных уязвимостей СрЗИ, ТСр и ПО
  – корректность работы СрЗИ при их взаимодействии с ТСр и ПО

  В случае выявления уязвимостей ИС:

  – проводится уточнение модели угроз безопасности информации
  – принимаются дополнительные меры ЗИ (при необходимости)

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- внедрение системы защиты информации

Включает:

- приемочные испытания СЗИ

Проводятся:
с учетом ГОСТ 34.603

Включают:
проверку выполнения требований к СЗИ в соответствии с ТЗ (ЧТЗ)

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- формирование требований к защите информации
- разработка системы защиты информации (СЗИ)
- внедрение системы защиты информации
- аттестация информационной системы по требованиям защиты информации и ввод ее в действие
- обеспечение ЗИ в ходе эксплуатации аттестованной ИС
- обеспечение ЗИ при выводе из эксплуатации аттестованной ИС

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- аттестация ИС по требованиям ЗИ и ввод ее в действие

  - комплекс организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие СЗИ ИС настоящим Требованиям.
  - организуется обладателем информации или оператором

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- аттестация ИС по требованиям ЗИ и ввод ее в действие

  Исходные данные для аттестации ИС:

  – модель угроз безопасности информации
  – акт классификации ИС (акт определения уровней защищённости ПДн)
  – ТЗ на создание ИС и (или) ТЗ (ЧТЗ) на создание СЗИ (СЗПДн)
  – проектная и эксплуатационная документация на СЗИ ИС
  – ОРД по защите информации
  – результаты анализа уязвимостей информационной системы
  – материалы предварительных и приемочных испытаний СЗИ ИС
  – иные документы

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- аттестация ИС по требованиям ЗИ и ввод ее в действие

Исходные данные для аттестации ИС:

– модель угроз безопасности информации
– акт классификации ИС (акт определения уровней защищённости ПДн)
– ТЗ на создание ИС и (или) ТЗ (ЧТЗ) на создание СЗИ (СЗПДн)
– проектная и эксплуатационная документация на СЗИ ИС
– ОРД по защите информации
– результаты анализа уязвимостей информационной системы
– материалы предварительных и приемочных испытаний СЗИ ИС
– иные документы

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- аттестация ИС по требованиям ЗИ и ввод ее в действие

  - проводится всоответствии с программой и методиками аттестационных испытаний
  - до начала обработки информации, подлежащей защите в ИС
  - по результатам аттестационных испытаний оформляются:
    – протоколы аттестационных испытаний
    – заключение о соответствии ИС требованиям о ЗИ
    – аттестат соответствия

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- аттестация ИС по требованиям ЗИ и ввод ее в действие

допускается на основе результатов аттестационных испытаний выделенного набора сегментов ИС, реализующих полную технологию обработки информации

распространение аттестата соответствия на другие сегменты ИС осуществляется при условии их соответствия сегментам ИС, прошедшим аттестационные испытания

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- аттестация ИС по требованиям ЗИ и ввод ее в действие

  Сегмент считается соответствующим сегменту ИС, в отношении которого были проведены аттестационные испытания, если:
  - установлены одинаковые классы защищенности
  - определены одинаковые угрозы безопасности информации
  - реализованы одинаковые проектные решения по ИС и её СЗИ

  Соответствие сегмента, подтверждается в ходе приемочных испытаний ИС или сегментов информационной системы.

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- аттестация ИС по требованиям ЗИ и ввод ее в действие
  - в сегментах ИС, на которые распространяется аттестат соответствия, **оператором** обеспечивается соблюдение эксплуатационной документации на СЗИ ИС и ОРД по ЗИ

  - особенности аттестации ИС на основе результатов аттестационных испытаний выделенного набора ее сегментов, а также условия и порядок распространения аттестата соответствия на другие сегменты ИС определяются в:
    - программе и методиках аттестационных испытаний
    - заключении
    - аттестате соответствия

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- аттестация ИС по требованиям ЗИ и ввод ее в действие
  повторная аттестация ИС осуществляется в случае

  - окончания срока действия аттестата соответствия
  - повышения класса защищенности ИС

  при увеличении состава угроз безопасности информации **или** изменения проектных решений, реализованных при создании СЗИ ИС, проводятся

  - дополнительные аттестационные испытания в рамках действующего аттестата соответствия

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- обеспечение ЗИ в ходе эксплуатации аттестованной ИС

включает

1. управление (администрирование) СЗИ ИС
2. выявление инцидентов и реагирование на них
3. управление конфигурацией аттестованной ИС и ее СЗИ
4. контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в ИС

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования к **организации ЗИ**, содержащейся в ИС

1. управление (администрирование) СЗИ ИС

- заведение и удаление учетных записей пользователей, управление полномочиями пользователей ИС и поддержание правил разграничения доступа в ИС
- управление СрЗИ в ИС, в том числе параметрами настройки ПО, включая ПО СрЗИ, управление учетными записями пользователей, восстановление работоспособности СрЗИ, генерация, смена и восстановление паролей
- установка обновлений ПО, включая ПО СрЗИ, выпускаемых разработчиками (производителями) средств защиты информации или по их поручению
- централизованное управление СЗИ ИС (при необходимости)
- регистрация и анализ событий в ИС, связанных с ЗИ
- информирование пользователей об угрозах безопасности информации, о правилах эксплуатации СЗИ ИС и отдельных СрЗИ, а также их обучение
- сопровождение функционирования СЗИ ИС в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и ОРД по ЗИ

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования к **организации ЗИ**, содержащейся в ИС

2. выявление инцидентов и реагирование на них
   - определение лиц, ответственных за выявление инцидентов и реагирование на них
   - обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе ТСр, ПО и СрЗИ, нарушений ПРД, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов
   - своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами
   - анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий
   - планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИС и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения ПРД, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов
   - планирование и принятие мер по предотвращению повторного возникновения инцидентов

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования к **организации ЗИ**, содержащейся в ИС

3. управление конфигурацией аттестованной ИС и ее СЗИ

- поддержание конфигурации ИС и ее СЗИ (структуры СЗИ ИС, состава, мест установки и параметров настройки СрЗИ, ПО и ТСр) в соответствии с эксплуатационной документацией на СЗИ (поддержание базовой конфигурации ИС и ее СЗИ)
- определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию ИС и ее СЗИ
- управление изменениями базовой конфигурации ИС и ее СЗИ, в том числе:
  - определение типов возможных изменений
  - санкционирование внесения изменений
  - документирование действий по внесению изменений
  - сохранение данных об изменениях
  - контроль действий по внесению изменений

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

3. управление конфигурацией аттестованной ИС и ее СЗИ

- анализ потенциального воздействия планируемых изменений в базовой конфигурации ИС и ее СЗИ на обеспечение ЗИ, возникновение дополнительных угроз безопасности информации и работоспособность ИС
- определение параметров настройки ПО, включая ПО СрЗИ, состава и конфигурации ТСр и ПО до внесения изменений в базовую конфигурацию ИС и ее СЗИ
- внесение информации (данных) об изменениях в базовой конфигурации ИС и ее СЗИ в эксплуатационную документацию на СЗИ ИС
- принятие решения по результатам управления конфигурацией о повторной аттестации ИС или проведении дополнительных аттестационных испытаний

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

4. контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в ИС

- контроль за событиями безопасности и действиями пользователей в ИС
- контроль (анализ) защищенности информации, содержащейся в ИС
- анализ и оценка функционирования СЗИ ИС, включая выявление, анализ и устранение недостатков в функционировании СЗИ ИС
- периодический анализ изменения угроз безопасности информации в ИС, возникающих в ходе ее эксплуатации, и принятие мер ЗИ в случае возникновения новых угроз безопасности информации
- документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС
- принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) СЗИ ИС, повторной аттестации ИС или проведении дополнительных аттестационных испытаний

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования
к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- обеспечение ЗИ при выводе из эксплуатации аттестованной ИС

Включает

1. архивирование информации, содержащейся в ИС
2. уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

Требования к **организации ЗИ**, содержащейся в ИС

Основные мероприятия:

- обеспечение ЗИ при выводе из эксплуатации аттестованной ИС
  - **архивирование** информации, содержащейся в ИС, должно осуществляться при необходимости дальнейшего использования информации в деятельности оператора
  - **уничтожение** (стирание) данных и остаточной информации с машинных носителей производится при необходимости передачи машинного носителя другому пользователю ИС или в сторонние организации для ремонта, ТО или дальнейшего уничтожения
  - при выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется **физическое уничтожение** этих носителей

Приказ ФСТЭК России от 11 февраля 2013 г. № 17

АКАДЕМИЯ АЙТИ

Спасибо за внимание!

Центральный офис:
Москва, Варшавское шоссе 47, корп. 4, 7 этаж
Тел: +7 (495) 150-96-00 доб. 4
edu-it@academyit.ru