Основные понятия:

1. Информация – любые сведения вне зависимости от их формата представления.
2. Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
3. Информационная безопасность – защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий.
4. Безопасность информации – состояние информации, при котором обеспечены её конфиденциальность, целостность и доступность.
5. Конфиденциальность информации – такое состояние информации, при котором доступ к ней могут получить только те лица, которые имеют на это право.
6. Информационная система – совокупность баз данных, технических и информационных средств для её обработки.

Ответы на вопросы:

1. Предназначение и основное содержание ПП РФ от 01.11.2012 г. № 1119.

Утверждает требования к защите персональных данных при их обработке в информационной системе. Делит ИС на виды, путём разделения их на использующие ПД и не использующие. Первым соответственно выделяются 3 типа угроз безопасности ПД. Также выделяется 4 уровня защищённости. Также определяется контроль за выполнением указанных требований.

1. Предназначение и основное содержание ПП РФ от 06.07.2008 N 512

Определяет требования к материальным носителям биометрических ПД, обязанности оператора а также условия хранения биометрических носителей ПД.

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

Включает подробное описание большинства угроз.

1. Предназначение и основное содержание Методики оценки угроз безопасности информации.

Из перечня угроз позволяет определить актуальные. Моделированием угроз занимаются органы власти.

1. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К).

Распространяются на всю конфи, для гос. ресурсов обязательны, для остальных рекомендательны. Регламентирует взаимоотношения при оказании услуг по ТЗКИ, содержит образцы нек. док-тов.

1. Предназначение и основное содержание Приказа ФСТЭК России от 18.02.2013 N 21.

Определяет состав и меры для каждого из уровня защищённости, порядок выбора мер.

1. Предназначение и основное содержание Приказа ФСТЭК России от 11 февраля 2013 г. № 17.

В целом, очень похож на 21, однако распространяется также и на другую конфи а не только ПД. Предписывает проводить аттестацию системы.

1. Лицензиат – юр. или физ. лицо, имеющее лицензию на осуществление деятельности.
2. Лицензируемый вид деятельности – деятельность, на осуществление которого требуется лицензия.
3. Лицензионные требования и условия – совокупность требований, необходимых для выполнения лицензиатом (специалисты, помещения, оборудование, автомат. систем, программы, документы).
4. Лицензирующие органы – органы исполнительной власти, осуществляющие лицензирование.
5. Какие лицензируемые виды деятельности связаны с защитой конфи и ПДн?

Техническая защита конфи, применение средств криптографической защиты информации

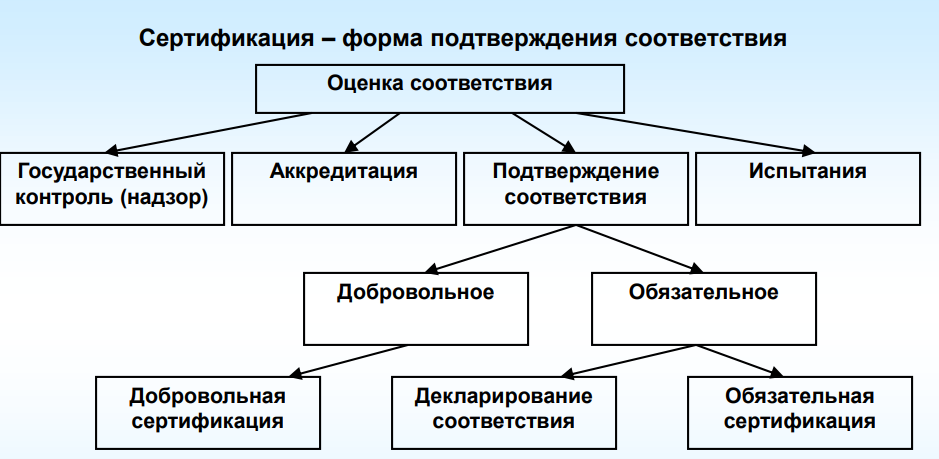
1. В каком документе определены виды деятельности, подлежащие обязательному лицензированию?

ФЗ 99 О лицензировании отдельных видов деятельности

1. Системы сертификации в РФ.

Совокупность участников сертификации, включающая ФСТЭК; центральный орган системы сертификации; органы, проводящие сертификацию; испытательные лаборатории; изготовители

1. Классификация форм оценки соответствия.



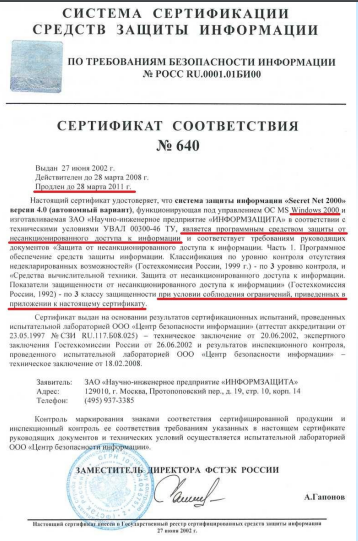
1. Обязательная система сертификации.

Включает декларирование соответствия и обязательную сертификацию

1. Добровольная система сертификации

Я хз чё сказать, она есть, в слайдах больше ничего про это не сказано лол.

1. Сертификация – форма подтверждения объектов требованиям технических регламентов.
2. Сертификация СЗИ – деятельность по подтверждению соответствия требованиям.
3. Сертификат соответствия – я хз, что он хотел, но вот картинка



1. В каких случаях обязательно применение сертифицированных средств защиты информации?

Для обеспечения защиты в информационных системах.

1. Состав участников системы сертификации средств защиты информации.

ФСТЭК, центральный орган системы сертификации, орган проводящий сертификацию, лаборатории, производители

1. Функции органа по сертификации средств защиты информации.

Сертифицируют средства, приостанавливают сертификат, проводят повторные сертификации, формируют фон документов, предоставление информации производителям.

1. Функции испытательных лабораторий.

Проводят сертификационные испытания средств защиты информации.

1. Порядок проведения сертификации.



1. Особенности сертификации средств защиты информации.

Реестр сертификатов есть на ФСТЭК, сертификация может производится для одного товара и для множества, производства. 8 органов сертификации и 44 испытательные лаборатории. В сертификате могут быть условия. Сертификат имеет ограниченный срок.