Частное учреждение
дополнительного профессионального образования «Учебный центр ЦБИ»
(Частное учреждение ДПО «УЦ ЦБИ»)

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат:
036F578B0083ADDAA4449D09419C08873B
Владелец: Радионов Владимир Витальевич
Действителен: с 13.08.2021 до 13.11.2022

УТВЕРЖДАЮ
Директор
Частного учреждения ДПО «УЦ ЦБИ»
В.В. Радионов
«06» 06 2016 г.

Дополнительная профессиональная программа
повышения квалификации специалистов
в области информационной безопасности

«Аттестация объектов информатизации по требованиям безопасности информации. Защита от утечки по техническим каналам»

г. Королев
2016 г.

Перечень сокращений

АС	- автоматизированная система
ВП	- выделенное помещение
ВТ	- вычислительная техника
ВТСС	- вспомогательные технические средства и системы
ВЧ-навязывание	- высокочастотное навязывание
НСД	- несанкционированный доступ
ОИ	- объект информатизации
ОТСС	- основные технические средства и системы
ПЭМИ	- побочные электромагнитные излучения
ПЭМИН	- побочные электромагнитные излучения и наводки
СВТ	- средства вычислительной техники
СЗИ	- средства защиты информации
СИ	- специальные исследования
ТК	- технические каналы
ФСТЭК	- Федеральная служба по техническому и экспортному контролю

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1. 1. Общие положения

Настоящая программа повышения квалификации разработана на основании Федерального закона от 29.12.2012г. № 273-ФЗ «Об образовании в Российской Федерации», приказа Минобрнауки России от 05.12.2013г. № 1310 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности» и приказа Минобрнауки России от 01.07.2013г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам».

Программа повышения квалификации реализуется в Частном учреждении дополнительного профессионального образования «Учебный центр ЦБИ».

1.2. Цель реализации программы

Целью реализации дополнительной профессиональной программы по курсу «Аттестация объектов информатизации по требованиям безопасности информации. Защита от утечки по техническим каналам» является совершенствование уровня знаний, умений, профессиональных навыков и компетенций специалистов в области защиты информации, содержащей сведения государственной тайны.

1.3. Категории обучающихся:

- руководители и специалисты аттестационных центров;
- эксперты органов по аттестации объектов информатизации и сертификации средств защиты информации.

1.4. Характеристика вида профессиональной деятельности

1.4.1.Область профессиональной деятельности

Область профессиональной деятельности слушателя, освоившего программу повышения квалификации, включает совокупность задач, связанных с аттестацией объектов информатизации и средств вычислительной техники по требованиям безопасности информации.

1.4.2. Объекты профессиональной деятельности

Объектами профессиональной деятельности являются:

- объекты информатизации;
- средства вычислительной техники;
- средства защиты информации от утечки по техническим каналам;
- средства контроля эффективности защиты информации от утечки по техническим каналам.

1.4.3. Вид и задачи профессиональной деятельности

Вид профессиональной деятельности:

организация и проведение работ по аттестации объектов информатизации, а также оценке соответствия требованиям по безопасности информации средств вычислительной техники, используемых для обработки сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, сведения о которой составляют государственную тайну.

Задачи профессиональной деятельности:

– организация работ по проведению атестационных испытаний средств вычислительной техники по требованиям безопасности информации;

– разработка программ и методик аттестационных испытаний средств вычислительной техники по требованиям безопасности информации;

– проведение аттестационных испытаний средств вычислительной техники в соответствии с утвержденными программами и методиками;

– разработка отчетных материалов по результатам аттестационных испытаний средств вычислительной техники.

1.5.Планируемые результаты обучения

Процесс освоения обучающимися дополнительной профессиональной программы повышения квалификации направлен на качественное изменение компетенций в области аттестации объектов информатизации по требованиям безопасности информации от утечки по техническим каналам.

Перечень профессиональных компетенций, качественное изменение которых осуществляется в результате обучения:

– способность организовать работы по аттестации объектов информатизации;

– способность разрабатывать программы и методики аттестационных испытаний испытаний средств вычислительной техники;

– способность разрабатывать отчетную документацию по результатам аттестационных испытаний.

Слушатель, освоивший программу должен,

знать:

основы российского и международного законодательства и нормативно-правовых актов в области защиты информации;

правовые, нормативно-технические и организационные основы информационной безопасности;

теоретические основы информационной безопасности;

нормативную базу, регламентирующую аттестацию объектов информатизации;

классификацию, характеристики и методики оценки защищенности от утечки информации по техническим каналам.

уметь:

проводить анализ информационных систем и технологических процессов обработки информации на объектах защиты;

оценивать уровень защищенности информации на объектах защиты;

анализировать модели угроз и технических каналов утечки информации на объектах информатизации;

разрабатывать основные организационно-распорядительные документы и рекомендации по обеспечению безопасности информации на аттестованных объектах информатизации.

владеть:

методиками оценки защищенности информации от утечки по техническим каналам;

навыками проведения измерительных процедур на объектах защиты;

навыками применения, монтажа и контроля эффективности применяемых мер и средств защиты.

В результате обучения на курсе у слушателей должен быть сформирован объем специальных теоретических и практических знаний, позволяющих проводить аттестационные испытания объектов информатизации по требованиям безопасности информации от утечки по техническим каналам на уровне, соответствующем требованиям ФСТЭК России.

1.6. Трудоемкость программы

Общая трудоемкость освоения данной программы повышения квалификации составляет 72 (семьдесят два) академических часа.

1.7. Форма и сроки обучения

Обучение по данной программе повышения квалификации осуществляется в очной (с отрывом от работы) форме.

Срок освоения данной программы повышения квалификации при очной форме обучения составляет 8 дней.

1.8. Режим занятий

Учебные занятия проводятся в соответствии с расписанием, утверждаемым директором.

Продолжительность одного занятия – 45 минут.

Перерыв между занятиями 10 минут.

Перерыв на обед – 1 час.

Учебная нагрузка – не более 9 академических часов в день, включая все виды аудиторной и внеаудиторной учебной работы слушателя.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный план

Наименование разделов (тем)	Всего часов	В том числе, час				
		Л	СЗ	ПЗ	Зач	К, СР
Раздел 1. Организационно-правовые основы обеспечения защиты информации в Российской Федерации	**4**	**4**				**1**
Тема: Актуальность проблемы защиты информации. Нормативно-правовая база в области защиты информации.	1	1				
Тема: Основные понятия, термины и определения в области защиты информации.	1	1				
Тема: Структура, задачи и основные функции Государственной системы защиты информации.	1	1				
Тема: Лицензирования деятельности в области защиты государственной тайны. Сертификации средств защиты информации.	1	1				
Раздел 2. Система аттестации объектов информатизации по требованиям безопасности информации	5	4				
Тема: Организация, содержание и порядок проведения аттестационных испытаний объектов вычислительной техники	2	2				
Тема: Технические каналы утечки информации. Общие положения. Характеристика каналов. Основы организации исследований технических средств	2	2				
Самостоятельная подготовка	1					1
Раздел 3. Организация аттестационных испытаний объектов информатизации на соответствие требованиям безопасности информации	**9**	**5**		**3**		**1**
Тема: Нормативно-методическая база специальных исследований	1	1				
Тема: Канал утечки речевой информации за счет электроакустических преобразований (микрофонный эффект). Канал утечки речевой информации за счет ВЧ - навязывания (облучения)	1	1				
Тема: Канал утечки речевой информации за счет электроакустических преобразований (микрофонный эффект). Канал утечки речевой информации за счет ВЧ - навязывания (облучения)	1			1		
Тема: Канал утечки речевой информации за счет модулированных высокочастотных колебаний, возникающих при работе генераторов технических средств	1	1				
Тема: Канал утечки речевой информации за счет модулированных высокочастотных колебаний, возникающих при работе генераторов технических средств	1			1		

Наименование разделов (тем)	Всего часов	В том числе, час				
		Л	СЗ	ПЗ	Зач	К, СР
Тема: Паразитная генерация в технических средствах. Каналы утечки речевой информации за счет побочных электромагнитных излучений средств аналоговой обработки речи	1	1				
Тема: Паразитная генерация в технических средствах. Каналы утечки речевой информации за счет побочных электромагнитных излучений средств аналоговой обработки речи	1			1		
Тема: Основные способы блокирования каналов утечки речевой информации	1	1				
Самостоятельная подготовка	1					1
Раздел 4. Аттестационные испытания выделенных помещений (ВП) на соответствие требованиям по безопасности акустической речевой информации	**9**	**5**		**4**		
Л: Акустический и виброакустический каналы утечки речевой информации	2	2				
Тема: Оценка защищенности помещения от утечки речевой информации по акустическому и виброакустическому каналам». Теоретические положения.	2	2				
Тема: Оценка защищенности помещения от утечки речевой информации по акустическому и виброакустическому каналам». Измерения. Проведение расчетов. Обработка результатов	4			4		
Тема: Меры противодействия акустической речевой разведке. Основные характеристики систем виброакустической защиты и способы их установки в помещении.	1	1				
Раздел 5. Аттестационные испытания объектов вычислительной техники (ВТ) по требованиям безопасности информации от утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН)	**40**	**22**		**18**		
Тема: Общая характеристика технических каналов утечки информации при обработке ее средствами вычислительной техники	2	2				
Тема: Методы кодирования информации при обработке ее средствами вычислительной техники	1	1				
Тема: Условия проведения специальных исследований средств вычислительной техники. Общие требования при проведении измерений побочных электромагнитных излучений и наводок	2	2				
Тема: Условия проведения специальных исследований средств вычислительной техники. Тестовые режимы и примеры их применения	2	2				
Тема: Условия проведения специальных исследований средств вычислительной техники. Тестовые режимы и примеры их применения	1			1		
Тема: Условия проведения специальных исследований средств вычислительной техники. Требования к измерительному и вспомогательному оборудованию	2	2				
Тема: Контроль защищенности средств вычислительной техники от утечки информации по каналу побочных электромагнитных излучений. Лабораторные исследования. Теоретические положения.	2	2				
Тема: Контроль защищенности средств вычислительной техники от утечки информации по каналу побочных электромагнитных излучений. Лабораторные исследования. Измерения. Проведение расчетов. Оценка результатов.	5			5		
Тема: Контроль защищенности средств вычислительной техники от утечки информации по каналу побочных электромагнитных излучений. Объектовые исследования. Теоретические положения.	3	3				

Наименование разделов (тем)	Всего часов	В том числе, час				
		Л	СЗ	ПЗ	Зач	К, СР
Тема: Контроль защищенности средств вычислительной техники от утечки информации по каналу побочных электромагнитных излучений. Объектовые исследования. Измерения. Проведение расчетов. Оценка результатов.	5			5		
Тема: Каналы утечки информации на объекте вычислительной техники за счет наводок на цепи электропитания, заземления, отходящие от средств вычислительной техники линии, линии вспомогательных технических средств и систем и другие токопроводящие коммуникации	2	2				
Тема: Контроль защищенности средств вычислительной техники от утечки информации за счет наводок на цепи электропитания, заземления, отходящие от средств вычислительной техники линии, линии вспомогательных технических средств и систем и другие токопроводящие коммуникации. Теоретические положения.	3	3				
Тема: Контроль защищенности средств вычислительной техники от утечки информации за счет наводок на цепи электропитания, заземления, отходящие от средств вычислительной техники линии, линии вспомогательных технических средств и систем и другие токопроводящие коммуникации. Измерения. Проведение расчетов. Оценка результатов.	5			5		
Тема: Методы и средства защиты информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок	1	1				
Тема: Порядок построения пространственной системы активной защиты информации распределённого объекта информатизации, обеспечивающей защищённость по каналу побочных электромагнитных излучений и наводок от основных технических средств и систем, и оценки её эффективности	2	2				
Тема: Пример построения пространственной системы активной защиты информации распределённого объекта информатизации, обеспечивающей защищённость по каналу побочных электромагнитных излучений и наводок от основных технических средств и систем	2			2		
Самостоятельная подготовка	2					2
Раздел 6. Основы проведения поисковых мероприятий по выявлению закладочных устройств и предназначенных для несанкционированного съема информации	**2**	**2**				
Тема: Каналы утечки информации за счет внедренных специальных электронных устройств негласного получения информации. Специальные проверки и специальные обследования	2	2				
Итоговая аттестация (зачет)	**2**				**2**	
Итого (часов):	**72**	**41**		**25**	**2**	**4**

Примечание: «Л» - лекция, «СЗ» - семинарское занятие, «ПЗ» - практическое занятие, «К» - консультация, «СР» - самостоятельная работа, «Зач» - зачет.

Наименование тем занятий, их виды и объем могут корректироваться в пределах объема программы повышения квалификации с учетом обновления законодательной и нормативно-методической базы в области информационной безопасности, появления новых средств защиты информации и инструментальных средств контроля.

2.2. Календарный учебный график

Занятия по программе повышения квалификации проводятся, как правило, ежемесячно в соответствии с утвержденным графиком проведения курсов на текущий год. Продолжительность реализации программы повышения квалификации составляет 8 (восемь) дней.

Наименование раздела программы	Объем нагрузки, час	Учебные дни							
		1 9ч	2 9ч	3 9ч	4 9ч	5 9ч	6 9ч	7 9ч	8 9ч
Раздел 1. Организационно-правовые основы обеспечения защиты информации в Российской Федерации	4	4							
Раздел 2. Система аттестации объектов информатизации по требованиям безопасности информации	5	5							
Раздел 3. Организация аттестационных испытаний объектов информатизации на соответствие требованиям безопасности информации	9		9						
Раздел 4. Аттестационные испытания выделенных помещений (ВП) на соответствие требованиям по безопасности акустической речевой информации	9			9					
Раздел 5. Аттестационные испытания объектов вычислительной техники (ВТ) по требованиям безопасности информации от утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН)	41				9	9	9	9	5
Раздел 6. Основы проведения поисковых мероприятий по выявлению закладочных устройств и предназначенных для несанкционированного съема информации	2								2
Итоговая аттестация	2								2

2.3. Содержание разделов и тем

Содержание разделов, тем курса и изучаемых вопросов

Раздел 1. Организационно-правовые основы обеспечения защиты информации в Российской Федерации.

Виды информации по категориям доступа. Особенности видов информации с ограниченным доступом. Законодательные и нормативно-правовые акты Российской Федерации по защите информации. Их структура, основные положения. Государственная система защиты информации. Ее структура, задачи и основные функции. Нормативно-методические документы по защите информации (концепции, нормы, требования, положения, методики, ГОСТы и др.). Руководящие документы ФСТЭК России по защите информации. Лицензирование и сертификация в области защиты информации. Требования к специалистам органов по аттестации ОИ.

Раздел 2. Система аттестации объектов информатизации по требованиям безопасности информации.

Понятие аттестации ОИ по требованиям безопасности информации. Виды объектов информатизации. Объекты информатизации аттестуемые по требованиям безопасности информации. Необходимость, цель и задачи аттестации ОИ по требованиям безопасности информации. Аттестат соответствия. Организационная структура системы аттестации ОИ по требованиям безопасности информации. Функции субъектов процесса аттестации ОИ.

Раздел 3. Организация аттестационных испытаний объектов информатизации на соответствие требованиям безопасности информации.

Общие требования по аттестации ОИ. Порядок организации работ по аттестации ОИ по требованиям безопасности информации. Основные направления аттестации ОИ: НСД, ПЭМИН, вирусы, спецустройства. Этапы аттестационных испытаний их содержание и особенности реали-

зации. Схемы аттестации. Нормативные документы, определяющие порядок и объем аттестационных испытаний ОИ. Стандарты, нормативные и руководящие документы ФСТЭК России по требованиям безопасности информации. Условия, виды и методы проведения аттестационных испытаний АС. Программа и методики аттестационных испытаний. Требования к нормативным и методическим документам по аттестации ОИ, выбору измерительной аппаратуры и тестовых средств. Особенности аттестации современных автоматизированных систем. Оценка результатов испытаний и оформление отчетных материалов. Государственный контроль и надзор, инспекционный контроль за соблюдением правил аттестации и эксплуатации аттестованных объектов информатизации.

Раздел 4. Аттестационные испытания выделенных помещений (ВП) на соответствие требованиям по безопасности акустической речевой информации.

Технические каналы утечки речевой информации. Модели каналов утечки речевой информации по техническим каналам. Основные способы блокирования каналов утечки речевой информации.

Технические средства защиты речевой информации. Содержание и порядок проведения аттестационных испытаний выделенных помещений. Методика проведения инструментального контроля защищенности ВП от утечки акустической речевой информации. Нормативно-методическая база. Требования к измерительной аппаратуре. Особенности аттестационных испытаний ВП, оснащенных системами звукового усиления речи. Методика проведения акустического и виброакустического контроля при аттестации ВП. Проведение измерений и обработка результатов. Содержание отчетных документов.

Раздел 5. Аттестационные испытания объектов вычислительной техники (ВТ) по требованиям безопасности информации от утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

Каналы утечки информации. Модель и источники каналов утечки информации. Механизм возникновения каналов ПЭМИ СВТ. Классификация технических каналов утечки за счет ПЭМИН. Основные характеристики средств разведки ПЭМИН. Основные способы блокирования каналов утечки информации за счет ПЭМИН. Технические средства защиты информации. Специальные исследования технических средств и объектов. Виды специальных исследований. Нормативно-методическая база специальных исследований. Условия проведения специальных исследований. Требования к тестовым режимам работы технических средств. Требования к измерительным средствам.

Методика проведения специальных исследований СВТ на ПЭМИ. Расчет зоны 2 и зоны 1. Содержание предписания на эксплуатацию СВТ и протокола с результатами исследований. Особенности проведения специальных исследований сетей передачи данных и каналообразующей аппаратуры.

Методика проведения специальных объектовых исследований типового объекта ВТ в части оценки защищенности информации от утечки по каналу ПЭМИ. Расчет показателя защищенности. Оценка защищенности информации по методу «реальных затуханий». Содержание протокола с результатами исследований.

Методика проведения специальных объектовых исследований типового объекта ВТ в части оценки защищенности информации от утечки по цепям электропитания, заземления, совместно расположенным линиям ВТСС и инженерным коммуникациям. Рекомендуемая измерительная и вспомогательная аппаратура. Расчет показателей защищенности. Оценка защищенности информации по методу «реальных затуханий». Содержание протоколов с результатами исследований.

Порядок построения пространственной системы активной защиты информации распределённого объекта информатизации, обеспечивающей защищённость по каналу побочных электромагнитных излучений и наводок от основных технических средств и систем, и оценки её эффективности.

Пример построения пространственной системы активной защиты информации распределённого объекта информатизации, обеспечивающей защищённость по каналу побочных электромагнитных излучений и наводок от основных технических средств и систем.

Программно-аппаратные комплексы для проведения оценки защищенности технических средств в части ПЭМИН, защищенности помещений в части акустической речевой разведки и аку-

стоэлектрических преобразований. Назначение и основные режимы работы. Реализуемые функции. Основные технические характеристики. Принцип работы. Варианты комплектации. Особенности применения.

Раздел 6. Основы проведения поисковых мероприятий по выявлению закладочных устройств и предназначенных для несанкционированного съема информации.

Каналы утечки информации за счет внедренных специальных электронных устройств негласного получения информации. Специальные проверки и специальные обследования

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Требования к уровню подготовки слушателя, необходимому для освоения программы

К освоению программы повышения квалификации допускаются лица, имеющие среднее профессиональное и (или) высшее образование и лица, получающие среднее профессиональное и (или) высшее образование.

3.2. Требования к кадровым условиям реализации программы

Реализация программы повышения квалификации обеспечивается руководящими и научно-педагогическими работниками Учебного центра, а также лицами, привлекаемыми к реализации программы на условиях гражданско-правового договора.

Все научно-педагогические работники, участвующие в реализации программы повышения квалификации, должны иметь высшее техническое образование, конкретный опыт реализации научно-прикладных разработок или иной формы практической деятельности в области защиты информации.

3.3. Требования к материально-техническим условиям реализации программы

Для проведения занятий используются учебные аудитории и специализированные классы. Учебные аудитории оборудованы учебными досками, компьютерами, экранами и мультимедийными проекторами. Специализированные классы оборудованы стендами и компьютерами с установленным лицензионным программным обеспечением, средствами защиты информации, инструментальными средствами контроля эффективности защиты информации, а также инструментальными средствами, позволяющими отрабатывать практические навыки проведения сертификационных испытаний.

Лабораторные классы, оснащены средствами измерений и вспомогательным оборудованием для стендовых специсследований, контроля защищенности информации на объектах вычислительной техники и оценки эффективности установленных СЗИ.

Слушателям обеспечивается доступ в помещения, оснащенные компьютерами и другой оргтехникой, для самостоятельной работы и возможностью доступа в Интернет.

3.4. Требования к информационному и учебно-методическому обеспечению программы

3.4.1. Средства обеспечения освоения программы

1. Презентационные материалы лекций и практических занятий.
2. Типовые формы программ, методик и протоколов аттестационных испытаний.
3. Документация на средства защиты информации от НСД и инструментальные средства контроля защищенности.
4. Доступ к сети Интернет.

3.4.2. Основная литература

№ п/п	Наименование
1.	А.А. Голяков, В.С. Горбатов и др. Контроль защищенности информации от утечки по техническим каналам за счет ПЭМИН. Аттестационные испытания по требованиям безопасности информации. МИФИ, Москва, 2014г.
2.	В.С. Горбатов, А.П. Дураковский и др. Контроль защищенности речевой информации в помещениях. Аттестационные испытания выделенных помещений по требованиям безопасности информации. МИФИ, Москва, 2014г.

3.	В.П. Аминов, И.В. Коровин, В.И. Рыбальченко. Блокировка акустоэлектрических преобразователей в электронных ТС и системах общего применения. Гелиос АРВ, Москва, 2010г.
4.	Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. Защита от утечки информации по техническим каналам. Учебное пособие. Телеком, Москва, 2005г.
5.	В.Г. Герасименко, Ю.Н. Лаврухин, В.И. Тупота. Методы защиты акустической речевой информации от утечки по техническим каналам. РЦИБ «Факел», 2008г.
6.	А.В. Кондратьев. Организация и содержание работ по выявлению и оценке основных видов ТКУИ, защита информации от утечки. МАСКОМ, Москва, 2011г.
7.	В.К. Железняк. Защита информации от утечки по техническим каналам. Учебное пособие, Санкт-Петербург, 2006г.
8.	Системы виброакустической защиты семейства «Соната-АВ». Руководящий технический материал по выбору, монтажу и применению. ЗАО «Анна», Москва, 2008г.
9.	Ю.К. Меньшаков. Защита объектов и информации от технических средств разведки. Учебное пособие. Москва, 2002г.
10.	Ю.К. Меньшиков. Виды и средства иностранных технических разведок. Учебное пособие, 2009г.
11.	А.А. Торокин. Основы инженерно-технической защиты информации. Ось, Москва,1998г.
12.	А.А. Хорев. Техническая защита информации. Учебное пособие. В 3-х томах, 2008г.

3.4.3. Дополнительная литература

Законодательно-правовые акты	
№ п/п	**Наименование**
1.	Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»
2.	Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»
3.	Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»
4.	Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
5.	Федеральный закон от 28 декабря 2013 г. N 412-ФЗ «Об аккредитации в национальной системе аккредитации»
6.	Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895)
7.	Указ Президента Российской Федерации от 12 мая 2009 г. № 537 «О стратегии национальной безопасности Российской Федерации до 2020г.»
8.	Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»
9.	Постановление Правительства РФ от 15.05.2010г. №330 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг)»
10.	Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «Об утверждении Положения о сертификации средств защиты информации»
11.	Постановление Госстандарта РФ от 17 марта 1998 г. N 11 «Об утверждении Положения о Системе сертификации ГОСТ Р»
12.	Постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79 «Об утверждении Положения о лицензировании деятельности по технической защите конфиденциальной информации»
13.	Постановление Правительства Российской Федерации от 02 марта 2012 г. № 171 «Об утверждении Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»

14.	Постановление Правительства Российской Федерации от 21.04.2010г. № 266 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг), и о внесении изменения в положение о сертификации средств защиты информации
15.	Постановление Правительства Российской Федерации от 3 ноября 2014 г. N 1149 г. «Об аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по оценке (подтверждению) соответствия в отношении оборонной продукции (работ, услуг), поставляемой по государственному оборонному заказу, продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, а также о внесении изменений в некоторые акты Правительства Российской Федерации в части оценки соответствия указанной продукции (работ, услуг)».

Нормативно-методические документы	
№ п/п	**Наименование**
1.	Положение о государственной системе защиты информации в РФ от ИТР и от ее утечки по техническим каналам. Постановление СМ-Правительства РФ от 15.09.1993г. № 912-51.
2.	Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР), Гостехкомиссия России, 1997г.
3.	Сборник норм защиты информации от утечки за счет побочных электромагнитных излучений и наводок, Гостехкомиссия России, 1998 г.
4.	Сборник НМД АРР, введен в действие с 1.09.2000 г. приказом председателя Гостехкомиссии России № 304 от 26.07.2000г.
5.	Сборник НМД по ТЗИ ВОСП, утвержден и введен в действие с 1.03.2006 г. приказом ФСТЭК России от 15.11.2005г. 3№ 448
6.	Сборник методических документов по контролю защищенности информации, обрабатываемой СВТ, от утечки за счет ПЭМИН, утвержден приказом ФСТЭК России от 30.12.2005 г. № 075
7.	Модель ИТР-2020.
8.	Положение по аттестации объектов информатизации по требованиям безопасности информации (утверждено председателем Гостехкомиссии России 25 ноября 1994 г.)
9.	Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации (утверждено приказом председателя Гостехкомиссии России 25 ноября 1994 г.)
10.	Типовое положение об испытательной лаборатории (утверждено приказом председателя Гостехкомиссии России 25 ноября 1994г.)
11.	Положение о сертификации средств защиты информации по требованиям безопасности информации (утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199)
12.	Типовое положение об органе по сертификации средств защиты информации по требованиям безопасности информации (утверждено приказом председателя Гостехкомиссии России 05 января 1996 г., № 3)
13.	Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации (утверждено приказом председателя Гостехкомиссии России 05 января 1996г, № 3)
14.	Приказ ФСТЭК от 28 января 2015 г. № 5 «Об утверждении формы аттестата аккредитации»
15.	Приказ ФСТЭК от 10 апреля 2015 г. № 33 «Об утверждении правил выполнения отдельных работ по аккредитации органов по сертификации и испытательных лабораторий, выполняющих работы по оценке (подтверждению) соответствия в отношении продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в

	соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, в установленной ФСТЭК России сфере деятельности»
16.	Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок), утверждены приказом ФСТЭК России № 033 от 3.10 2014 г.
17.	Требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа (требования к средствам акустической и виброакустической защиты речевой информации), утверждены приказом ФСТЭК России № 03 от 4.02 2015 г.
18.	Сборник методических материалов по проведению специальных исследований технических средств АСУ и ЭВМ, предназначенных для работы с секретной информацией. НИИАА МРП СССР, 1978 г.
19.	Руководящий документ. Средства защиты информации. Специальные и общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам. Гостехкомиссия России, 2000 г.
20.	Руководящий документ. Временные специальные требования по проведению сертификационных испытаний по требованиям безопасности информации средств вычислительной техники, используемых при осуществлении международного информационоого обмена, включая международную ассоциацию сетей «Интернет», размещаемых в выделенных помещениях, и защите информации от утечки по техническим каналам. ФСТЭК России, 2006 г.

Национальные стандарты

№ п/п	Наименование
1.	ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения
2.	ГОСТ Р 56093-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства обнаружения преднамеренных силовых электромагнитных воздействий. Общие требования.
3.	ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения.
4.	ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования.
5.	ГОСТ Р 52863-2007 Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования.
6.	ГОСТ Р 53113.1-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.
7.	ГОСТ Р 53113.2-2009 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов.
8.	ГОСТ 12.1.050-86. Методы измерения шума на рабочих местах.
9.	СниП 23-03-2003. Защита от шума.
10.	ГОСТ 27296-87. Защита от шума в строительстве. Звукоизоляция ограждающих конструкций. Методы измерения.
11.	ГОСТ Р 53112-2008. Защита информации. Комплексы для измерений параметров ПЭМИН. Технические требования и методы испытаний.
12.	ГОСТ Р 51320-99. Совместимость технических средств электромагнитная. Радиопомехи индустриальные. Методы испытаний ТС – источников индустриальных помех.

13.	ГОСТ Р 51319-99. Совместимость технических средств электромагнитная. Приборы для измерения индустриальных помех. Технические требования и методы испытаний.
14.	ГОСТ Р 8.563-2009. Государственная система обеспечения единства измерений. Методики (методы) измерений.
15.	ГОСТ Р 52448-2005. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения.
16.	ГОСТ Р 52447-2005. Защита информации. Техника защиты информации. Номенклатура показателей качества.
17.	ГОСТ Р50922-2006. «Защита информации. Основные термины и определения»
18.	ГОСТ РО 0043-003 2012 «Защита информации. Аттестация объектов информатизации. Общие положения»
19.	ГОСТ РО 0043-004 2013 «Защита информации. Программа и методики аттестационных испытаний»
20.	ГОСТ Р 51275-2006. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»
21.	ГОСТ Р 51241-98. «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний»
22.	ГОСТ Р 54011-2010. Оценка соответствия. Общие правила отбора образцов продукции при проведении обязательного подтверждения соответствия третьей стороной.
23.	ГОСТ 22505-97. Совместимость технических средств электромагнитная. Радиопомехи индустриальные от радиовещательных приемников, телевизоров и другой бытовой радиоэлектронной аппаратуры. Нормы и методы испытаний.
24.	ГОСТ CISPR 16-1-4-2013 Совместимость технических средств электромагнитная. Требования к аппаратуре для измерения параметров индустриальных радиопомех и помехоустойчивости и методы измерений.
25.	ГОСТ Р 29339-92. Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Общие технические требования.
26.	ГОСТ Р 50752-95. Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Методы испытаний.
Научно-техническая литература	
1.	Г.А. Ерохин, О.В. Чернов и др. Антенно-фидерные устройства и распространение радиоволн. Учебное пособие. Телеком. Москва, 2007г.
2.	Э.Л. Портнов. Оптические кабели связи и пассивные компоненты волоконно-оптических линий связи. Учебное пособие. Телеком. Москва, 2007г.
3.	О.В. Головин. Радиоприемные устройства. Учебное пособие. Телеком, Москва, 2004г.
4.	С.С. Анцыферов, Б.И. Голубь. Общая теория измерений. Учебное пособие. Телеком, Москва,2007г.
5.	А.Н. Денисенко. Сигналы. Теоретическая радиотехника. Справочное пособие. Телеком, Москва, 2005г.
6.	А.А. Кучумов. Электроника и схемотехника. Учебное пособие. Гелиос АРВ. Москва, 2004г.
7.	Р.Е. Быков. Основы телевидения и видеотехники. Учебное пособие. Телеком, Москва,2006г.
8.	И.А. Алдошина, Э.И. Вологдин и др. Электроакустика и звуковое вещание. Учебное пособие. Телеком. Москва, 2007г.
9.	Е.А. Колосовский. Устройства приема и обработки сигналов. Учебное пособие., Телеком, Москва,2007г.
10.	В.В. Шубин. Информационная безопасность волоконно-оптических систем. Саров, 2015г.
11.	А.И. Болдырев, И.В. Василевский, С.Е. Сталенков. Методические рекомендации по поиску и нейтрализации средств негласного съема информации. Практическое пособие. Москва, 2001г.
12.	С.В. Лебедь. Межсетевое экранирование. Теория и практика защиты внешнего периметра, 2002г.
13.	Ю.К. Меньшаков. Защита объектов и информации от технических средств разведки, 2002г.

3.4.4. Программное обеспечение

Пакет программ фирмы Microsoft.

Программа «ПЭМИН-2005» - для расчета показателей защищенности информации, обрабатываемой СВТ, от утечки за счет ПЭМИН.

Сборник тестовых программ для СИ средств ЭВТ.

Программа расчета показателей защищенности конфиденциальной информации «ГРОЗА-К» версия 1.0

3.4.5. Пакет слушателя

Пакет слушателя (раздаточный материал) включает:

- конспект лекций (презентаций) для слушателя по дополнительной профессиональной программе повышения квалификации специалистов в области информационной безопасности по курсу «Аттестация объектов информатизации по требованиям безопасности информации. Защита от утечки по техническим каналам»;
- приложение к конспекту лекций (презентаций), содержащее справочные и дополнительные материалы по изучаемым темам.

3.5. Порядок передачи программы повышения квалификации другой организации

Данная программа повышения квалификации может быть передана другой организации на основании и в соответствии с требованиями действующего Законодательства Российской Федерации.

4. ФОРМЫ АТТЕСТАЦИИ

Итоговая аттестация обучающихся завершается зачетом в форме тестирования. В ходе зачета слушатели отвечают на вопросы, изложенные в билетах. Слушатель считается аттестованным, если по результатам зачета (тестирования) количество правильных ответов составляет не менее 80%.

Для проведения итоговой аттестации создается аттестационная комиссия, состав которой утверждается директором Частного учреждения ДПО «УЦ ЦБИ».

В целях обеспечения объективной оценки знаний, умений и уровня приобретенных компетенций слушателем по результатам обучения в состав аттестационной комиссии могут включаться представители ФСТЭК России, потенциальные работодатели, профильные специалисты и представители заказчика обучения.

5. ПЕРЕЧЕНЬ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ, ИСПОЛЬЗУЕМЫХ В УЧЕБНОМ ПРОЦЕССЕ

№ п/п	Сведения, отнесенные к государственной тайне*	Сведения, подлежащие засекречиванию**	№ раздела (темы), при изучении которых доводятся сведения, составляющие государственную тайну
1	п.102.	п.42, п.55.	Раздел 4. Раздел 5.

* В соответствии с Перечнем сведений, отнесенных к государственной тайне, утвержденным Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203.

** В соответствии с Перечнем сведений, подлежащих засекречиванию, Федеральной службы по техническому и экспортному контролю, утвержденным приказом ФСТЭК России от 12 октября 2012 г. № 033.

Начальник учебно-методической группы В.И. Крук