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____ 201_6_г.

Дополнительная профессиональная программа
повышения квалификации специалистов
в области информационной безопасности

«Техническая защита конфиденциальной информации»

г. Королев
201_6_ г.

Перечень сокращений

АС	- автоматизированная система
ИС	- информационная система
НСД	- несанкционированный доступ
ОИ	- объект информатизации
СЗИ	- средства защиты информации
СЗИ от НСД	- средства защиты информации от несанкционированного доступа
СВТ	- средства вычислительной техники
ТЗКИ	- техническая защита конфиденциальной информации

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 является совершенствование уровня знаний, умений, профессиональных навыков и компетенций специалистов в области защиты информации, в отношении которой законодательством установлено требование обеспечения ее конфиденциальности.

1.3. Категории обучающихся:

- руководители и специалисты организаций, оказывающих услуги по ТЗКИ;
-руководители и специалисты структурных подразделений технической защиты информации;
-пользователи информационных систем, обрабатывающих информацию конфиденциального характера.

1.4. Характеристика вида профессиональной деятельности

1.4.1. Область профессиональной деятельности

Область профессиональной деятельности слушателя, освоившего программу повышения квалификации, включает выполнение работ по технической защите информации конфиденциального характера при ее обработке в АС (ИС), СВТ, защищаемых помещениях.

1.4.2. Объекты профессиональной деятельности

- объекты информатизации, включая автоматизированные системы обработки, хранения и передачи информации конфиденциального характера;
- технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах;
- информационные системы, телекоммуникационные системы, автоматизированные системы, системы управления информационной безопасностью, информационные технологии в условиях воздействия угроз информационной безопасности.
- инструментальные средства контроля эффективности защиты информации от НСД.

1.4.3. Вид и задачи профессиональной деятельности

Виды профессиональной деятельности: организационно-управленческая, эксплуатационная, исследовательская.

Задачи (функции) профессиональной деятельности:

- организация аттестации АС (ИС) по требованиям безопасности информации;
- оценка правильности классификации АС (ИС)
- определение уровня защищенности информации;
- разработка программы и методик аттестационных испытаний АС (ИС);
- проверка состояния организации работ и выполнения организационно-технических требований по защите информации в АС (ИС);
- оценка полноты и уровня разработки организационно-распорядительной, проектной и эксплуатационной документации;
- проведение испытаний АС и ИС на соответствие требованиям по защите информации от НСД;
- контроль соответствия системы защиты информации АС (ИС) требованиям безопасности в процессе ее эксплуатации.

1.5. Планируемые результаты обучения

Процесс освоения обучающимися дополнительной профессиональной программы повышения квалификации направлен на качественное изменение следующих компетенций:

а) общепрофессиональных:

- разработка технических проектов и технических заданий на защищенные информационные (автоматизированные) системы;
- осуществление организационно-правового и инженерно-технического обеспечения защиты информации в ИС;
- сопоставительный анализ данных результатов проверок и испытаний систем защиты информации, анализ возможных источников и каналов утечки информации.

б) профильных профессиональных:

- разработка моделей угроз безопасности информации в ИС;
- разработка предложений по совершенствованию и повышению эффективности принимаемых технических мер и организационных мероприятий по защите информации;
- разработка политик информационной безопасности организаций, эксплуатирующих информационные системы.

В результате освоения дополнительной профессиональной программы повышения квалификации обучающиеся должны получить знания, умения и навыки, которые позволят качественно изменить соответствующие компетенции.

Комплекс знаний, умений и навыков, получаемых обучающимися в результате освоения дополнительной профессиональной программы повышения квалификации должен формироваться из приведенного ниже списка.

Обучающиеся должны:

знать:

- нормативно-правовые и организационные основы обеспечения безопасности информации конфиденциального характера в Российской Федерации;
- порядок организации и проведения лицензирования деятельности в области защиты информации;
- требования основных нормативных правовых актов, регламентирующих вопросы обеспечения безопасности информации;
- основные виды угроз безопасности информации при ее обработке информационных (автоматизированных) системах;
- содержание и порядок организации работ по выявлению угроз безопасности информации;

- организационные и технические меры обеспечения безопасности информации, порядок их выбора и реализации в ИС (АС).

уметь:

- планировать мероприятия по обеспечению безопасности информации;
- разрабатывать необходимые документы в интересах организации работ по обеспечению безопасности информации;
- обосновывать и задавать требования по обеспечению безопасности информации в информационных (автоматизированных) системах;
- проводить оценку актуальных угроз безопасности информации при ее обработке в информационных (автоматизированных) системах;
- определять состав и содержание мер по обеспечению безопасности информации при ее обработке в информационных (автоматизированных) системах, необходимых для блокирования угроз безопасности информации.

обладать навыками:

- определения уровня защищенности информации;
- выявления актуальных угроз безопасности информации в информационных (автоматизированных) системах.

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 и тем	Всего часов	В том числе, час				
		Л	СЗ	ПЗ	Зач	К, СР
1	2	3	4	5	6	7
Раздел 1. Организационно-правовые основы обеспечения защиты информации в Российской Федерации	8	8	-	-		-
Тема: Структура нормативно-правовых актов РФ в области защиты информации.	2	2	-	-		-

Наименование разделов и тем	Всего часов	В том числе, час				
		Л	СЗ	ПЗ	Зач	К, СР
1	2	3	4	5	6	7
Тема: Нормативно-методические документы государственных регуляторов по защите информации.	2	2				
Тема: Государственная система защиты информации.	2	2				
Тема: Лицензирование деятельности по технической защите конфиденциальной информации.	2	2				
Раздел 2. Основы организации работ по защите конфиденциальной информации	**8**	**3**	**2**			**3**
Тема: Требования к организации защиты конфиденциальной информации.	2	2				
Тема: Структура и задачи подразделений по защите информации.	2	1				1
Тема: Структура и содержание локальных нормативных актов по защите информации в государственных и муниципальных органах.	4		2			2
Раздел 3. Способы и средства защиты конфиденциальной информации	**16**	**8**		**4**		**4**
Тема: Классификация угроз безопасности информации.	2	2				
Тема: Средства защиты информации от утечки по техническим каналам и порядок их применения.	6	3		1		2
Тема: Средства защиты информации от несанкционированного доступа. Порядок выбора СЗИ.	8	3		3		2
Раздел 4. Защита конфиденциальной информации при межсетевом взаимодействии	**9**	**3**		**3**		**1**
Тема: Особенности обеспечения безопасности информации при межсетевом взаимодействии.	3	2				1
Тема: Межсетевые экраны: типы, функционал и порядок их применения.	6	2		4		
Раздел 5. Создание системы защиты информации в организации (на предприятии)	**20**	**9**		**10**		**1**
Тема: Порядок анализа информационных ресурсов и информационных потоков организации (предприятия).	2	1				1
Тема: Методика разработки моделей угроз и нарушителя безопасности информации.	6	2		4		
Тема: Порядок формирования требований к системе защиты информации.	2	2				
Тема: Аттестация объектов информатизации по требованиям безопасности информации.	10	4		6		
Раздел 6. Эксплуатация системы защиты конфиденциальной информации.	9	3		6		
Тема: Администрирование системы защиты информации.	8	2		6		
Тема: Организация контроля защищенности информации. Виды и способы контроля.	1	1				
Итоговая аттестация (зачет)	**2**				**2**	
Итого:	**72**	**35**	**2**	**24**	**2**	**9**

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	8	8							
Раздел 2. Основы организации работ по защите конфиденциальной информации	8	1	7						
Раздел 3. Способы и средства защиты конфиденциальной информации	16		2	9	5				
Раздел 4. Защита конфиденциальной информации при межсетевом взаимодействии	9				4	5			
Раздел 5. Создание системы защиты информации в организации (на предприятии)	20					4	9	7	
Раздел 6. Эксплуатация системы защиты конфиденциальной информации.	9							2	7
Итоговая аттестация (зачет)	2								2

2.3. Содержание разделов и тем
Содержание разделов, тем курса и изучаемых вопросов

Наименование разделов и тем (основные вопросы)	
Раздел 1. Организационно-правовые основы обеспечения защиты информации в Российской Федерации	
Тема	**Структура нормативно-правовых актов РФ в области защиты информации.** Федеральные законы и постановления Правительства РФ, осуществляющие правовое регулирование обработки и защиты информации. Порядок ограничения доступа к информации. Виды информации ограниченного доступа. Государственные информационные системы. Государственные регуляторы в сфере защиты информации, их функции и полномочия.
Тема	**Нормативно-методические документы государственных регуляторов по защите информации.** Виды документов, издаваемых государственными регуляторами. Структура и назначение документов в области защиты информации, сфера их применения. Обзор национальных и

	международных стандартов в области защиты информации. Понятие сертификации средств защиты информации.
Тема	**Государственная система защиты информации.** Структура и задачи государственной системы защиты информации. Система мероприятий по защите информации в РФ. Задачи подразделений и специалистов по защите информации.
Тема	**Лицензирование деятельности по технической защите конфиденциальной информации.** Лицензируемые виды деятельности в области защиты конфиденциальной информации. Нормативно-правовые документы по вопросам лицензирования. Лицензионные требования. Функции участников системы лицензирования. Общий порядок получения лицензии. Заявительные документы.
Раздел 2. Основы организации работ по защите конфиденциальной информации.	
Тема	**Требования к организации защиты КИ.** Требования к организации защиты конфиденциальной информации на предприятии (организации). Составные части (основы) системы защиты конфиденциальной информации.
Тема	**Структура и задачи подразделений по защите информации.** Типовая структура и функции органов (подразделений, служб) системы защиты информации на предприятии. Решаемые задачи. Требования к руководителям и специалистам подразделений и уровню их образования.
Тема	**Структура и содержание локальных нормативных актов по защите информации в государственных и муниципальных органах.** Структура, базовый состав и содержание организационно-распорядительной документации по защите информации. Порядок привлечения специализированных сторонних организаций к разработке системы защиты конфиденциальной информации.
Раздел 3. Способы и средства защиты конфиденциальной информации.	
Тема	**Классификация угроз безопасности информации.** Угрозы несанкционированного доступа к конфиденциальной информации. Источники угроз. Классификация угроз. Модель нарушителя. Основы анализа рисков.
Тема	**Средства защиты информации от утечки по техническим каналам и порядок их применения.** Правовые, организационные и технические способы защиты конфиденциальной информации от утечки по техническим каналам. Средства защиты конфиденциальной информации от утечки по техническим каналам. Общие требования к способам и средствам защиты.
Тема	**Средства защиты информации от несанкционированного доступа. Порядок выбора СЗИ.** Организационные меры и программно-технические средства защиты информации от НСД. Классификация СЗИ от НСД. Классы и функционал СЗИ от НСД.
Раздел 4. Защита конфиденциальной информации при межсетевом взаимодействии.	
Тема	**Особенности обеспечения безопасности информации при межсетевом взаимодействии.** Особенности обеспечения безопасности конфиденциальной информации при межсетевом взаимодействии. Основные проблемы защиты конфиденциальной информации при взаимодействии с сетью Интернет. Технологии безопасного использования ресурсов и услуг сети Интернет.
Тема	**Межсетевые экраны и средства анализа защищенности: типы, функционал и порядок их применения.** Межсетевые экраны – как средства защиты информации при межсетевом взаимодействии. VPN – как технология построения защищенных корпоративных сетей. Другие средства защиты конфиденциальной информации при взаимодействии с Интернет. Средства анализа защищенности сетей (сканеры уязвимостей). Средства обнаружения атак.
Раздел 5. Создание системы защиты информации в организации (на предприятии).	
Тема	**Порядок анализа информационных ресурсов и информационных потоков организации (предприятия).** Информационные ресурсы организации (предприятия). Методика анализа информационных ресурсов. Разработка плановых и организационно-распорядительных документов. Требования к содержанию документов. Анализ технологического процесса обработки конфиденциальной информации в организации (предприятии).
Тема	**Методика разработки модели угроз и нарушителя безопасности информации.** Анализ угроз несанкционированного доступа к защищаемой информации. Методика формирования моделей угроз и потенциального нарушителя.

Тема	**Порядок формирования требований к системе защиты информации.** Методология формирования требований к системам защиты конфиденциальной информации. Формы задания требований. Концепция обеспечения информационной безопасности организации (предприятия). Политика безопасности. Техническое задание на работы и системы защиты конфиденциальной информации. Приемка работ по защите конфиденциальной информации. Виды работ и особенности их приемки.
Тема	**Аттестация объектов информатизации по требованиям безопасности информации.** Общий порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Исходные документы для проведения аттестации. Порядок проведения аттестационных работ. Особенности проверки подсистем защиты от УИТК и НСД. Документы, оформляемые по результатам аттестации: состав, структура и формы. Особенности эксплуатации аттестованных объектов информатизации.
Раздел 6. Эксплуатация системы защиты конфиденциальной информации.	
Тема	**Администрирование системы защиты информации.** Общий порядок эксплуатации системы защиты конфиденциальной информации. Виды контроля. Меры контроля. Администрирование штатных средств защиты операционных систем. Настройка, характеристика уязвимых мест. Администрирование СЗИ от НСД. Особенности эксплуатации средств защиты и контроля защищенности информации от утечки по техническим каналам.
Тема	**Организация контроля защищенности информации. Виды и способы контроля.** Требования к периодичности контроля. Формы контроля. Специалисты, привлекаемые к проведению контроля. Государственный, межведомственный и внутренний контроль. Способы проведения контроля. Инструментальные средства контроля эффективности защиты информации.

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 аттестационных испытаний.

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

3.4. Учебно-методическое и информационное обеспечение программы

3.4.1. Средства обеспечения освоения программы

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

3.4.2. Основная литература

Законодательные и правовые акты

№ п/п	Наименование
1.	Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»
2.	Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»
3.	Федеральный закон от 07.07.2003 г. № 126-ФЗ «О связи»
4.	Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»
5.	Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
6.	Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»
7.	Федеральный закон от 26 июня 2008 г. № 102-ФЗ «Об обеспечении единства измерений»
8.	Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
9.	Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»
10.	Указ Президента Российской Федерации от 06 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»
11.	Доктрина информационной безопасности Российской Федерации. (утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895)
12.	Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «Об утверждении Положения о сертификации средств защиты информации»
13.	Постановление Правительства Российской Федерации от 26 июня 1995 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
14.	Постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79 «Об утверждении Положения о лицензировании деятельности по технической защите конфиденциальной информации»
15.	Постановление Правительства Российской Федерации от 02 марта 2012 г. № 171 «Об утверждении Положения о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»
16.	Постановление Правительства Российской Федерации от 03 ноября 1994 г. № 1233 «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»

Нормативно-методические документы

№ п/п	Наименование
1.	Приказ ФСТЭК от 11 февраля 2013г №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
2.	Приказ ФСТЭК от 18 февраля 2013г №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
3.	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.)
4.	Приказ ФСТЭК от 14 июня 2014г №31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»
5.	Методика определения актуальных угроз безопасности персональных при их обработке в информационных системах персональных данных данных (утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.)
6.	Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30.08.2002 г. № 282
7.	Положение о сертификации средств защиты информации по требованиям безопасности информации (утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199)
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 председателем Гостехкомиссии России 25 ноября 1994 г.)
10.	Типовое положение об испытательной лаборатории (утверждено председателем Гостехкомиссии России 25 ноября 1994 г.)
11.	Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации (утверждено председателем Гостехкомиссии России 25 ноября 1994 г.)
12.	Типовое положение об органе по сертификации средств защиты информации по требованиям безопасности информации (утвержденное председателем Гостехкомиссии России 25 ноября 1994 г.)
13.	«Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации», Гостехкомиссия России, Москва, 2001 г.
14.	«Временная методика оценки защищённости конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации», Гостехкомиссия России, Москва, 2001 г.
15.	«Временная методика оценки защищенности речевой конфиденциальной информации от утечки по акустическому и виброакустическому каналам», Гостехкомиссия России, Москва, 2001 г.
16.	«Временная методика оценки защищенности речевой конфиденциальной информации от утечки за счет электроакустических преобразований в вспомогательных технических средствах и системах», Гостехкомиссия России, Москва, 2001 г.

№ п/п	Наименование
17.	Методический документ «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК от 11 февраля 2014 г)
18.	«Сборник руководящих документов по защите информации от несанкционированного доступа», Гостехкомиссия России, Москва, 1998 г.
19.	РД Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей», Москва, 1999г.
20.	Административный регламент ФСТЭК по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации (утвержден Приказом ФСТЭК от 12 июля 2012 г №83)

Национальные стандарты

№ п/п	Наименование
1	ГОСТ Р 51583-2014. «Порядок создания автоматизированных систем в защищенном исполнении»
2	ГОСТ Р50922-96. «Защита информации. Основные термины и определения»
3	ГОСТ РО 0043-003 2012г «Защита информации. Аттестация объектов информатизации»
4	ГОСТ РО 0043-004 2013г «Защита информации. Программа и методики аттестационных испытаний»
5	ГОСТ Р 51275-99. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»
6	Рекомендации по стандартизации Р 50.1.053-2005. «Информационные технологии. Основные термины и определения в области технической защиты информации»
7	ГОСТ Р 51241-98. «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний»
8	ГОСТ 34.201-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»
9	ГОСТ 34.602-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированных систем»
10	ГОСТ 34.003-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»
11	ГОСТ 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадия создания»
12	ГОСТ Р 6.30-2003. «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов»
13	ГОСТ 28195-89. «Оценка качества программных средств. Общие положения»
14	ГОСТ Р ИСО\МЭК 9126-90. «Информационная технология. Оценка программной продукции. Характеристика качества и руководства по их применению»
15	ГОСТ Р 50739-95. «Средства вычислительной техники. Защита от несанкционированного доступа к информации»

3.4.3. Дополнительная литература

№ п/п	Наименование
1	Семкин С.Н., СемкинА.Н.Основы информационной безопасности объектов обработки информации, 2000 г.
2	Б. Шнайер. Секреты и ложь. Безопасность данных в цифровом мире, 2003 г.
3	Д. Скляров. Искусство защиты и взлома информации, 2004 г.
4	С.С. Корт. Теоретические основы защиты информации, 2004 г.
5	В.В. Домарев. Безопасность информационных технологий. Системный подход, 2004 г.
6	С.Н. Семкин и др. Основы организационного обеспечения информационной безопасности объектов информатизации, 2005 г.
7	В.В. Домарев. Защита информации и безопасность компьютерных систем, 1999 г.
8	В.В. Мельников. Безопасность информации в автоматизированных системах, 2003 г.
9	А.Ю. Щеглов. Защита компьютерной информации от несанкционированного доступа, 2004 г.
10	Т.Л. Партыка, Попов И.И. Информационная безопасность, 2004 г.
11	В.И. Ярочкин. Информационная безопасность. Учебник для вузов, 2004 г.
12	Г.Н. Устинов. Основы информационной безопасности систем и сетей передачи данных, 2000г.
13	В.А. Галатенко. Основы информационной безопасности. Курс лекций, 2004 г.
14	Теоретические основы компьютерной безопасности. Учебное пособие для вузов, 2000 г.
15	Соколов А.В., Степанюк О.М. Шпионские штучки. Методы информационной защиты объектов и компьютерных систем, 2000 г.
16	А.В. Петраков. Основы практической защиты информации. Учебное пособие, 2005г.
17	А.А. Губенков, В.Б. Байбурин. Информационная безопасность, Учебное пособие, 2005г.
18	С.В. Лебедь. Межсетевое экранирование. Теория и практика защиты внешнего периметра, 2002г.
19	В.Г. Проскурин, С.В. Крутов, И.В. Мацкевич. Защита в операционных системах, 2000г.
20	А.А. Снытников. Лицензирование и сертификация в области ЗИ, 2003г
21	Скотт Бармен. Разработка правил информационной безопасности, 2002г.
22	А.В. Ильичев. Начала системной безопасности, 2003г.
23	Г.Ф. Конахович. Защита информации в телекоммуникационных системах, 2005г.
24	Научно-практический сборник. Технические средства защиты информации, 2002г.
25	Вильям Столлинг. Основы защиты сетей. Приложения и стандарты, 2002г.
26	А.А. Соколов, О.М. Степанюк. Защита от компьютерного терроризма, 2002г.
27	В. Зима, А. Молдовян. Безопасность глобальных сетевых технологий, 2003г.
28	П. Девянин. Анализ безопасности управления доступом и информационными потоками в компьютерных системах, 2006г.
29	А.А. Садердинов, В.А. Трайнев и др. Учебное пособие. Информационная безопасность предприятия, 2006г.
30	Стивен Норткат, Мери Купер и др. Анализ типовых нарушений безопасности в сетях, 2001г.
31	Н.А. Гайдамакин. Разграничение доступа к информации в компьютерных системах, 2003г.
32	В.Я. Асанович, Т.Г. Маньшин. Информационная безопасность: анализ и прогноз информационного воздействия, 2006г.
33	Ю.К. Меньшаков. Защита объектов и информации от технических средств разведки, 2002г.
34	В.А. Конявский, С.В. Лопаткин. Компьютерная преступность, том 1, 2006г.
35	С.А. Запечников, Н.Г. Милославская. Учебник Информационная безопасность открытых систем, том 1, 2006г.
36	А.А. Малюк, Учебное пособие. Информационная безопасность: концептуальные и

№ п/п	Наименование
	методологические основы защиты информации, 2004г.
37	А.Н. Прохода. Обеспечение Интернет-безопасности, Учебное пособие, 2007г.
38	Учебное пособие. Защита информации в системах мобильной связи, 2006г.
39	А.А. Малюк. Введение в защиту информации в автоматизированных системах, 2005г.
40	Е.Б. Белов, В.П. Лось. Учебное пособие. Основы информационной безопасности, 2006г.
41.	С.В. Запечников и др. Основы построения виртуальных частных сетей, 2003г.

3.4.4. Программное обеспечение

Пакет программ фирмы Microsoft.

Инструментальные средства для проведения аттестационных испытаний: «Ревизор-1XP», «Ревизор-2XP», «ФИКС», «Терьер», «Агент инвентаризации» и др.

Средства защиты информации от НСД: SecretNet, DallasLock, Аккорд, Страж и др.

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 «Техническая защита конфиденциальной информации»;
- документацию на инструментальные средства, используемые для аттестационных испытаний;
- документацию на средства защиты информации от НСД;
- пакет типовых документов, разрабатываемых в ходе аттестации ОИ.

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

Порядок проведения тестирования разрабатывается Частным учреждением ДПО «УЦ ЦБИ» самостоятельно и доводится до обучаемых на установочном занятии.

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%. Слушателям, успешно сдавшим зачет, выдаются Удостоверения о повышении квалификации установленного образца

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

Сведения, составляющие государственную тайну, в учебном процессе не используются.

Начальник учебно-методической группы В.И. Крук