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
«___» _____201_г.

Дополнительная профессиональная программа
повышения квалификации специалистов
в области информационной безопасности

«Аттестация объектов информатизации по требованиям безопасности информации. Защита от несанкционированного доступа»

г. Королев
201_г.

Перечень сокращений

АС	- автоматизированная система
НСД	- несанкционированный доступ
ОИ	- объект информатизации
ОС	- операционная система
ПО	- программное обеспечение
ПРД	- правила разграничения доступа
ПЭВМ	- персональная электронно-вычислительная машина
РД	- руководящий документ
СЗИ	- система защиты информации
СрЗИ	- средства защиты информации
СрЗИ от НСД	- средства защиты информации от несанкционированного доступа
СВТ	- средства вычислительной техники
ФСБ	- Федеральная служба безопасности
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 является: совершенствование и получение новых компетенций необходимых для выполнения профессиональной деятельности в области аттестации объектов информатизации по требованиям безопасности информации в части несанкционированного доступа.

1.3. Категории обучающихся:

- руководители и специалисты испытательных лабораторий;
- 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

- объекты информатизации, включая автоматизированные системы обработки, хранения и передачи информации определенного уровня конфиденциальности;
- технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах;
- нормативно-правовые акты РФ в области защиты информации;
- нормативно- методические документы по защите информации от НСД;
- методы и средства обеспечения информационной безопасности АС;
- методы проведения аттестационных испытаний;
- средства защиты информации от НСД;
- организационно-распорядительная, проектная и эксплуатационная документация ОИ;
- инструментальные средства контроля эффективности защиты информации от НСД.

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 (функции) профессиональной деятельности:

- организация аттестации АС по требованиям безопасности информации;
- оценка правильности категорирования и классификации АС (определение уровня защищенности информации);
- анализ исходных данных и документации по защите информации и проверка их соответствия реальным условиям размещения и эксплуатации АС;
- разработка программы и методик аттестационных испытаний АС;
- проверка состояния организации работ и выполнения организационно-технических требований по защите информации в АС;
- оценка полноты и уровня разработки организационно-распорядительной, проектной и эксплуатационной документации;
- оценка уровня подготовки кадров, обеспечивающих защиту информации, и распределения ответственности должностных, эксплуатирующих АС, за выполнение требований по защите информации в АС;
- проведение испытаний АС на соответствие требованиям по защите информации от НСД;
- подготовка отчетной документации и оценка результатов испытаний аттестуемой АС;
- контроль соответствия системы защиты информации аттестованной АС 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:

- способность понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны;
- способность выявлять и анализировать возможные угрозы информационной безопасности объектов информатизации;
- способность проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов;
- способность использовать нормативные правовые акты и нормативно-методические документы ФСБ России и ФСТЭК России в области информационной безопасности и защиты информации;
- способность ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность;
- способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью;
- способность организации защиты информации на объектах информатизации.

б) профильных профессиональных:

- способность проводить экспертный анализ уровня защищённости автоматизированных систем обработки информации ограниченного доступа от различного вида угроз и оценку соответствия автоматизированных систем международным и отечественным стандартам и нормативно-методическим документам ФСБ России и ФСТЭК России в области защиты информации;
- способность организовать процесс проведения и сопровождения аттестации объекта информатизации на соответствие требованиям безопасности информации;
- способность разрабатывать программы и методики аттестационных испытаний по оценке защищенности информации от несанкционированного доступа;
- умение применять способы и средства защиты информации от несанкционированного доступа к информации;

- самостоятельно проводить аттестационные испытания с использованием инструментальных средств контроля защищенности;
- способность разрабатывать организационно-распорядительные документы, регламентирующие работу по защите информации на объекте информатизации;
- способность осуществлять классификацию СВТ и АС по уровню защищенности от несанкционированного доступа к обрабатываемой информации;
- способность проводить аттестационные испытания АС по оценке защищенности информации от несанкционированного доступа;
- способность оформлять протоколы и заключения по результатам аттестационных испытаний.
- способность применять методы и средства контроля эффективности защиты СВТ и АС от несанкционированного доступа к информации;

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

В результате освоения учебной программы обучаемые должны

знать:

- нормативно-правовые и организационные основы обеспечения безопасности информации ограниченного доступа в РФ;
- виды информационных ресурсов по категориям доступа;
- свойства, характеризующие защищенность информации;
- основные способы НСД к информации;
- основные направления защиты информации от НСД;
- возможности и характеристики технических, программно-технических и программных средств защиты информации от НСД;
- архитектуру современных автоматизированных систем;
- характеристики информации, циркулирующей в средствах и системах информатизации;
- типовые угрозы информации и ресурсам автоматизированных систем;
- этапы и критерии классификации АС;
- требования существующих законов, стандартов и нормативно-методических документов по защите информации от НСД для АС;
- организационную структуру Системы аттестации ОИ по требованиям безопасности информации и функции субъектов процесса аттестации;
- порядок организации и проведения работ по аттестации ОИ по требованиям безопасности информации;
- нормативные документы, определяющие содержание и объем аттестационных испытаний;
- условия, виды и методы проведения аттестационных испытаний;
- возможные схемы аттестации ОИ;
- порядок разработки программы и методик аттестационных испытаний и требования к их содержанию;
- этапы аттестационных испытаний, их содержание и особенности реализации;
- инструментальные средства проведения аттестационных испытаний ОИ на соответствие требованиям по защите информации от НСД и условия их применения;

уметь:

- применять действующую законодательную базу в области информационной безопасности;
- организовать работу по аттестации, обеспечить соблюдение правил и процедур аттестационных испытаний и обоснованность выдачи «Аттестата соответствия», в том числе:

определять перечень охраняемых сведений ОИ;

провести анализ и оценку исходных данных и документации, представленных заявителем для аттестации ОИ;

оценить правильность классификации и категорирования ОИ;

разработать программу и методику проведения аттестационных испытаний ОИ;

провести анализ и оценку технологического процесса обработки информации на ОИ;
провести оценку достаточности мероприятий по защите информации на ОИ;
провести анализ результатов аттестационных испытаний;
оформить протоколы, заключение и «Аттестат соответствия» по результатам аттестационных испытаний ОИ;
организовать и провести контроль и надзор за соблюдением правил аттестации и эксплуатацией аттестованных ОИ;

- разрабатывать положения, инструкции и другие организационно-распорядительные документы по защите информации от НСД;

обладать навыками:

- применения инструментальных средств аттестации ОИ на соответствие требованиям по защите информации от НСД;
- настройки и администрирования встроенных механизмов защиты ОС;
- настройки и администрирования специализированных средств защиты информации от НСД.

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. Государственная система защиты информации	**9**	**6**				**3**
Тема: Основные определения. Актуальность проблемы защиты информации	1	1				
Тема: Структура, задачи и основные функции Государственной системы защиты информации.	1	1				
Тема: Система лицензирования деятельности в области защиты государственной тайны.	2	1				1
Тема: Система лицензирования деятельности в области защиты конфиденциальной информации.	2	1				1
Тема: Система сертификации средств защиты информации в	1	1				

Наименование разделов и тем	Всего часов	В том числе, час				
		Л	СЗ	ПЗ	Зач	К, СР
РФ.						
Тема: Система аттестации объектов информатизации (ОИ) по требованиям безопасности информации.	2	1				1
Раздел 2. Система нормативно – правового регулирования деятельности в области защиты информации в РФ	**11**	**9**				**2**
Тема: Структура нормативно-правовых актов РФ в области защиты информации по уровню и назначению.	1	1				
Тема: Законы РФ в области защиты информации. Основные положения.	2	2				
Тема: Постановления Правительства РФ в области защиты информации. Основные положения	2	2				
Тема: Основные национальные стандарты и технические регламенты в области защиты информации. Основные положения	1	1				
Тема: Основные руководящие документы и нормативно-методические документы в области защиты информации. Назначение. Основные положения	2	1				1
Тема: Основные организационно-распорядительные документы организации (предприятия) в области защиты информации. Назначение. Регламентируемые положения	1	1				
Тема: Ответственность за правонарушения в области защиты информации. Нормативно-правовые акты, устанавливающие ответственность	2	1				1
Раздел 3. Автоматизированные системы. Защита информации от несанкционированного доступа	**12**	**5**		**5**		**2**
Тема: Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа.	2	1				1
Тема: Классификация автоматизированных систем, подлежащих защите от несанкционированного доступа к информации	2	1		1		
Тема: Система защиты информации от несанкционированного доступа в АС. Требования по защите информации от несанкционированного доступа в АС.	3	2				1
Тема: Средства защиты информации от несанкционированного доступа – основа системы защиты информации в АС.	5	1		4		
Раздел 4. Аттестация объектов информатизации по требованиям безопасности информации	**16**	**11**	**2**			**3**
Тема: Порядок организации работ по аттестации объектов информатизации по требованиям безопасности информации.	1	1				
Тема: Исходные данные и документация, представляемые для проведения аттестации объектов информатизации. Особенности исходных данных для различных типов аттестуемых объектов информатизации.	2	1				1
Тема: Условия и порядок проведения аттестационных испытаний объектов информатизации. Методы проверок и испытаний. Возможные схемы аттестации объектов информатизации.	1	1				
Тема: Методическое обеспечение и инструментальные средства для проведения аттестационных испытаний (общий обзор).	1	1				
Тема: Анализ и оценка исходных данных и документации по защите информации на объекте информатизации. Проверка	2	2				

Наименование разделов и тем	Всего часов	В том числе, час				
		Л	СЗ	ПЗ	Зач	К, СР
соответствия исходных данных реальным условиям размещения и эксплуатации объекта информатизации.						
Тема: Программа и методики аттестационных испытаний объектов информатизации.	5	2	2			1
Тема: Проверка состояния технологического процесса обработки информации	1	1				
Тема: Проверка состояния организации работ и выполнения организационно-технических требований по защите информации.	2	1				1
Тема: Государственный контроль и надзор, инспекционный контроль за соблюдением правил аттестации и эксплуатации аттестованных объектов.	1	1				
Раздел 5. Аттестационные испытания автоматизированных систем на соответствие требованиям по защите информации от несанкционированного доступа	**22**	**9**		**13**		
Тема: Анализ и оценка технологического процесса обработки информации в части несанкционированного доступа.	1	1				
Тема: Испытания подсистемы управления доступом.	4	2		2		
Тема: Испытания подсистемы регистрации и учета.	3	1		2		
Тема: Испытания подсистемы обеспечения целостности.	3	1		2		
Тема: Испытания подсистемы антивирусной защиты.	3	1		2		
Тема: Испытания подсистемы криптографической защиты.	3	1		2		
Тема: Особенности аттестации автоматизированных систем, использующих сетевую технологию обработки информации.	3	1		2		
Тема: Оценка результатов испытаний. Подготовка отчетных документов.	2	1		1		
Итоговая аттестация (зачет)	**2**				**2**	
Итого:	**72**	**40**	**2**	**18**	**2**	**10**

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. Государственная система защиты информации	9	9							

Раздел 2. Система нормативно – правового регулирования деятельности в области защиты информации в Российской Федерации	**11**		**9**	**2**					
Раздел 3. Автоматизированные системы. Защита информации от несанкционированного доступа	**12**			**7**	**5**				
Раздел 4. Аттестация объектов информатизации по требованиям безопасности информации	**16**				**4**	**9**	**3**		
Раздел 5. Аттестационные испытания автоматизированных систем на соответствие требованиям по защите информации от несанкционированного доступа	**22**						**6**	**9**	**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. Государственная система защиты информации	
Тема	**Основные определения. Актуальность проблемы защиты информации.** Место информационной безопасности в общей системе безопасности РФ. Место информационной безопасности в общей системе безопасности организации. Структура актуальных угроз информационной безопасности.
Тема	**Структура, задачи и основные функции Государственной системы защиты информации (ГСЗИ).** Понятие ГСЗИ. Цели ГСЗИ. Основные принципы функционирования ГСЗИ. Правовые основы деятельности ГСЗИ. Основные задачи ГСЗИ. Организационная структура ГСЗИ. Функциональная структура (основные элементы) ГСЗИ. Зоны ответственности.
Тема	**Система лицензирования деятельности в области защиты государственной тайны.** Области компетенции лицензирующих органов и лицензируемые ими виды деятельности. Основные нормативные документы системы лицензирования ФСТЭК России. Виды лицензий ФСТЭК России. Общие требования к соискателям лицензий. Лицензионные требования. Заявительные документы. Схема лицензирования. Функции участников.
Тема	**Система лицензирования деятельности в области защиты конфиденциальной информации (ЗКИ).** Области компетенции лицензирующих органов и лицензируемые ими виды деятельности. Виды лицензий. Нормативные документы системы лицензирования в области ЗКИ. Внутренние процедуры ФСТЭК России, определяющие порядок лицензирования в области ЗКИ. Условия лицензирования. Общие принципы лицензирования в области ЗКИ. Схема лицензирования Лицензионные требования. Функции участников. Заявительные документы.
Тема	**Система сертификации средств защиты информации (СрЗИ) в РФ.** Понятие СрЗИ. Понятие сертификации. Структура СрЗИ, подлежащих сертификации. Необходимость сертификации СрЗИ. Цели системы сертификации СрЗИ. Организационная структура системы сертификации СрЗИ ФСТЭК России. Схема проведения сертификации СрЗИ. Нормативные документы, определяющие порядок сертификации СрЗИ. Срок действия сертификатов. Порядок продления срока действия сертификата
Тема	**Система аттестации объектов информатизации (ОИ) по требованиям безопасности информации.** Понятие ОИ. Виды (типы) ОИ. Понятие аттестации ОИ. Необходимость аттестации ОИ. ОИ, подлежащие обязательной аттестации. Общие требования по аттестации ОИ, предназначенных для обработки защищаемой информации. Стандарты, нормативные и руководящие документы ФСТЭК России по требованиям безопасности информации. Организационная структура системы аттестации ФСТЭК России по требованиям безопасности информации.

Раздел 2. Система нормативно-правового регулирования деятельности в области защиты информации в Российской Федерации	
Тема	**Структура нормативно-правовых актов РФ в области защиты информации по уровню и назначению.**
Тема	**Законы РФ в области защиты информации. Основные положения.**
Тема	**Постановления Правительства РФ в области защиты информации. Основные положения.**
Тема	**Основные национальные стандарты и технические регламенты в области защиты информации. Основные положения.**
Тема	**Основные руководящие документы и нормативно-методические документы в области защиты информации. Назначение. Основные положения.**
Тема	**Основные организационно-распорядительные документы организации (предприятия) в области защиты информации. Назначение. Регламентируемые положения.**
Тема	**Ответственность за правонарушения в области защиты информации. Нормативно-правовые акты, устанавливающие ответственность.**
Раздел 3. Автоматизированные системы. Защита информации от несанкционированного доступа	
Тема	**Концепция защиты средств вычислительной техники (СВТ) и автоматизированных систем (АС) от несанкционированного доступа (НСД).** Определение НСД. Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД. Организация работ по защите от НСД. Модель нарушителя в АС.
Тема	**Классификация АС, подлежащих защите от НСД к информации.** Цель классификации. Критерии классификации. Основные этапы классификации. Исходные данные для проведения классификации. Характеристика классов защищенности. Отличительные особенности. Рекомендации по классификации АС.
Тема	**Система защиты информации (СЗИ) от НСД в АС. Требования по защите информации от НСД для АС.** Основные подсистемы СЗИ от НСД. Их назначение и решаемые задачи. Требования к подсистемам СЗИ от НСД в АС. Основные различия и особенности требований в зависимости от конфиденциальности информации. Практическая реализация подсистем СЗИ от НСД.
Тема	**Средства защиты информации от НСД – основа СЗИ от НСД в АС.** Определение СрЗИ от НСД. Классификация СрЗИ от НСД. Функциональное назначение современных СрЗИ от НСД. Основные задачи, решаемые СрЗИ от НСД. Требования к СрЗИ от НСД, применяемым при создании защищенных АС. Характерные признаки сертифицированных СрЗИ от НСД. Рекомендации по анализу содержания Сертификатов на СрЗИ от НСД и условиям применения СрЗИ для создания защищенных АС. Краткий обзор современных сертифицированных СрЗИ от НСД.
Раздел 4. Аттестация объектов информатизации (ОИ) по требованиям безопасности информации	
Тема	**Порядок организации работ по аттестации ОИ по требованиям безопасности информации.** Нормативная база. Схема организации и проведения работ по аттестации ОИ. Функции организации-заявителя, ФСТЭК России и органов по аттестации ОИ. Содержание заявки на проведение аттестации ОИ.
Тема	**Исходные данные и документация, представляемые для проведения аттестации ОИ. Особенности исходных данных для различных типов аттестуемых ОИ.**
Тема	**Условия и порядок проведения аттестационных испытаний ОИ. Методы проверок и испытаний. Возможные схемы аттестации ОИ.** Основные нормативные документы, определяющие условия, порядок, объем, виды и методы проведения аттестационных испытаний ОИ. Общие требования по аттестации ОИ. Цели и задачи аттестационных испытаний и проверок. Стандарты, нормативные и руководящие документы ФСТЭК России по требованиям безопасности информации.
Тема	**Методическое обеспечение и инструментальные средства для проведения аттестационных испытаний (общий обзор).**
Тема	**Анализ и оценка исходных данных и документации по защите информации на объекте**

	информатизации. Проверка соответствия исходных данных реальным условиям размещения и эксплуатации ОИ.
Тема	**Программа и методики аттестационных испытаний ОИ.** Типовое содержание программы аттестационных испытаний ОИ. Основные факторы, определяющие содержание и объем аттестационных испытаний. Рекомендации по разработке.
Тема	**Проверка состояния технологического процесса обработки информации.** Выявление реальных объектов и субъектов доступа и средств обработки и передачи информации. Проверка соответствия описания технологического процесса реальной практике на объекте. Выявление опасных факторов, угроз и критических мест, снижающих уровень защищенности. Практические рекомендации по проведению анализа и применению инструментальных средств.
Тема	**Проверка состояния организации работ и выполнения организационно-технических требований по защите информации.** Объем испытаний (проверок). Объекты испытаний. Цели испытаний. Методы испытаний. Требования к объектам испытаний. Порядок испытаний.
Тема	**Государственный контроль и надзор, инспекционный контроль за соблюдением правил аттестации и эксплуатации аттестованных объектов. Ответственность за правильность аттестации и эксплуатации аттестованных АС.**
Раздел 5. Аттестационные испытания АС на соответствие требованиям по защите информации от НСД	
Тема	**Анализ и оценка технологического процесса обработки информации в части НСД.** Цель анализа (изучение информационных потоков, выявление субъектов и объектов доступа и правил разграничения доступа). Объекты анализа. Порядок действий. Анализ возможных угроз НСД к информационным и техническим ресурсам. Практические рекомендации. Инструментальные средства.
Тема	**Испытания подсистемы управления доступом.** Объект испытаний. Цель испытаний. Метод испытаний. Требования к объекту испытания. Порядок испытаний (проверок). Инструментальные средства. Особенности и рекомендации.
Тема	**Испытания подсистемы регистрации и учета.** Объект испытаний. Цель испытаний. Метод испытаний. Требования к объекту испытания. Порядок испытаний (проверок). Инструментальные средства. Особенности и рекомендации.
Тема	**Испытания подсистемы обеспечения целостности.** Объект испытаний. Цель испытаний. Метод испытаний. Требования к объекту испытания. Порядок испытаний (проверок). Инструментальные средства. Особенности и рекомендации.
Тема	**Испытания подсистемы антивирусной защиты.** Объект испытаний. Цель испытаний. Метод испытаний. Требования к объекту испытания. Порядок испытаний (проверок). Инструментальные средства. Особенности и рекомендации.
Тема	**Испытания подсистемы криптографической защиты.** Объект испытаний. Цель испытаний. Метод испытаний. Требования к объекту испытания. Порядок испытаний (проверок). Инструментальные средства. Особенности и рекомендации.
Тема	**Особенности аттестации АС, использующих сетевую технологию обработки информации.** Объекты испытаний. Цель испытаний. Методы испытаний. Порядок испытаний (проверок). Инструментальные средства. Особенности и рекомендации. Межсетевые экраны. Их настройка и администрирование.
Тема	**Оценка результатов испытаний. Подготовка отчетных документов.** Виды отчетных документов и их содержание. Рекомендации и особенности оформления. Примеры типовых форм отчетных документов.
	Зачет

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

№ п/п	Наименование
1	Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации. Учебное пособие. В.С. Горбатов, С.В. Дворянкин и др., 2014
2	Контроль защищенности речевой информации в помещениях. Аттестационные испытания выделенных помещений по требованиям безопасности информации. Учебное пособие. В.С. Горбатов, А.П. Дураковский и др., 2014
3	Контроль защищенности информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок. Аттестационные испытания по требованиям безопасности информации. Учебное пособие. А.А. Голяков, В.С. Горбатов и др., 2014
4	Организация и содержание работ по выявлению и оценке основных видов ТКУИ, защита информации от утечки. А.В. Кондратьев, 2011
5	Защита объектов и информации от технических средств разведки. Учебное пособие. Ю.К. Меньшаков, 2002
6	Инженерно-техническая защита информации. Учебное пособие. А.А. Торокин, 2005
7	Информационная безопасность предприятия. И. Конеев, А. Беляев, 2003
8	Защита информации и безопасность компьютерных систем. В.В. Домарев, 1999
9	Информационная безопасность открытых систем. Угрозы, уязвимости, атаки и подходы к защите. Учебное пособие. С.В. Запечников, Н.Г. Милославская и др., 2006
10	Информационная безопасность. Учебное пособие. В.И. Ярочкин, 2004

11	Основы информационной безопасности. Учебное пособие. Е.Б. Белов, В.П. Лось и др., 2006
12	Защита компьютерной информации от несанкционированного доступа. А.Ю. Щеглов, 2004
13	Основы информационной безопасности объектов обработки информации. Научно-практическое пособие. С.Н. Семкин, А.Н. Семкин, 2000
14	Разработка правил информационной безопасности. С. Бармен, 2002
15	Основы информационной безопасности. Учебное пособие. В.А. Галатенко, 2004
16	Основы организационного обеспечения информационной безопасности объектов информатизации. Учебное пособие. С.Н. Семкин, Э. В. Беляков и др., 2005
17	Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие. А.А. Малюк, 2004
18	Введение в защиту информации в автоматизированных системах. Учебное пособие. А.А. Малюк, С.В. Пазизин, Н.С. Погожин, 2005
19	Общие критерии оценки безопасности информационных технологий. Учебное пособие. А.А. Сидак, 2004
20	Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. Г.Н. Устинов, 2000
21	Системный анализ в защите информации. Учебное пособие. А.А. Шумский, А.А. Шелупанов, 2005
22	Информационная безопасность. Учебное пособие. А.А. Губенков, В.Б. Байбурин, 2005
23	Теоретические основы защиты информации. Учебное пособие. С.С. Корт, 2004
24	Информационная безопасность автоматизированных систем. Учебное пособие. А.Ф. Чипига, 2010
25	Комплекс СЗИ от НСД «Аккорд-АМДЗ». Учебное пособие. Л.К. Бабенко, Е.А. Ищукова, 2007
26	Система защиты информации VipNet. Курс лекций. Н.В. Кабанова, А.О. Чефранова, 2014
27	Система защиты информации VipNet. Практикум. Н.В. Кабанова, А.О. Чефранова, 2013

3.4.3. Дополнительная литература

Законодательные и правовые акты	
№ п/п	**Наименование**
1.	«Доктрина информационной безопасности Российской Федерации». Утверждена Президентом Российской Федерации 9 сентября 2000г. № Пр-1895
2.	«О стратегии национальной безопасности Российской Федерации до 2020г.». Указ Президента Российской Федерации от 12 мая 2009г. N 537
3.	«О безопасности». Федеральный закон от 28 декабря 2010г. № 390-ФЗ
4.	«О государственной тайне». Закон Российской Федерации от 21 июля 1993г. № 5485-I
5.	«О Федеральной службе безопасности». Федеральный закон от 3 апреля 1995г. № 40-ФЗ
6.	«Об информации, информационных технологиях и о защите информации». Федеральный закон от 27 июля 2006г. № 149-ФЗ
7.	«О техническом регулировании». Федеральный закон от 27 декабря 2002г. № 184-ФЗ
8.	«О персональных данных». Федеральный закон от 27 июля 2006г. № 152-ФЗ
9.	«О лицензировании отдельных видов деятельности». Федеральный закон от 4 мая 2011г. № 99-ФЗ
10.	Вопросы федеральной службы безопасности Российской Федерации. Указ Президента Российской Федерации от 11 августа 2003г. № 960
11.	Вопросы Федеральной службы по техническому и экспортному контролю. Указ Президента Российской Федерации от 16 августа 2004г. № 1085
12.	Вопросы Межведомственной комиссии по защите государственной тайны. Указ Президента Российской Федерации от 06 октября 2004г. № 1286
13.	О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного

	информационного обмена. Указ Президента Российской Федерации от 17 марта 2008г. № 351
14.	Перечень сведений, отнесенных к государственной тайне. Указ Президента Российской Федерации от 30 ноября 1995г. № 1203
15.	О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне. Распоряжение Президента Российской Федерации от 16апреля 2005г. № 151-рп
16.	Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности. Постановление Правительства Российской Федерации от 4 сентября 1995г. № 870 с изменениями и дополнениями от 15 января и 22 мая 2008г.
17.	Об утверждении перечня сведений конфиденциального характера. Указ Президента Российской Федерации от 06 марта 1997г. № 188
18.	Об организации лицензирования отдельных видов деятельности. Постановление Правительства Российской Федерации от 21 ноября 2011г. № 957
19.	Положением о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны. Постановление Правительства Российской Федерации от 15 апреля 1996г. № 333
20.	О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации. Постановление Правительства Российской Федерации от 3 марта 2012г. № 171
21.	О лицензировании деятельности по технической защите конфиденциальной информации. Постановление Правительства Российской Федерации от 3 февраля 2012г. № 79
22.	Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии Постановление Правительства Российской Федерации от 3 ноября 1994г. № 1233
23.	О сертификации средств защиты информации. Постановление Правительства Российской Федерации от 26 июня 1995г. № 608
Нормативно-методические документы	
№ п/п	**Наименование**
1.	Положение по аттестации объектов информатизации по требованиям безопасности информации (утверждено председателем Гостехкомиссии России 25 ноября 1994 г.)
2.	Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации (утверждено председателем Гостехкомиссии России 25 ноября 1994 г.)
3.	Положение о сертификации средств защиты информации по требованиям безопасности информации. Приказ ФСТЭК России от 27 октября 1995г. № 199
4.	Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации (утверждено председателем Гостехкомиссии России 25 ноября 1994 г.)
5.	Типовое положение об испытательной лаборатории (утверждено председателем Гостехкомиссии России 25 ноября 1994 г.)
6.	Типовое положение об органе по сертификации средств защиты информации по требованиям безопасности информации (утвержденное председателем Гостехкомиссии России 25 ноября 1994
7.	Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приказ ФСТЭК России от 11 февраля 2013г. № 17
8.	Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Приказ ФСТЭК России от 18 февраля 2013г. № 21

9.	Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения». Решение председателя Гостехкомиссии России от 30 марта 1992 г.
10.	Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Решение председателя Гостехкомиссии России от 30 марта 1992г.
11.	Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Решение председателя Гостехкомиссии России от 25 июля 1997г.
12.	Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности. Гостехкомиссия России, 2003г.
13.	Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты. Гостехкомиссия России, 2003г.
14.	Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты. Гостехкомиссия России, 2003г.
15.	Руководящий документ. Руководство по разработке профилей защиты и заданий по безопасности. Гостехкомиссия России, 2003г.
16.	Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Приказ председателя Гостехкомиссии России от 4 июня 1999г. № 114.
17.	Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Решение председателя Гостехкомиссии России от 30 марта 1992г.
18.	Методика определения актуальных угроз безопасности персональных при их обработке в информационных системах персональных данных данных (утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.)
19.	Методические документы. Профили защиты средств антивирусной защиты. Утверждены ФСТЭК России 14 июня 2012г.
20.	Методические документы. Профили защиты систем обнаружения вторжений. Утверждены ФСТЭК России 6 марта 2012г.
Национальные стандарты	
№ п/п	**Наименование**
1.	ГОСТ Р50922-96. «Защита информации. Основные термины и определения»
2.	ГОСТ Р 51583-2014. «Порядок создания автоматизированных систем в защищенном исполнении»
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.	ГОСТ Р 51241-98. «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний»
7.	ГОСТ 34.201-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»
8.	ГОСТ 34.602-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированных систем»
9.	ГОСТ 34.003-90. «Информационная технология. Комплекс стандартов на

	автоматизированные системы. Автоматизированные системы. Термины и определения»
10.	ГОСТ 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадия создания»
11.	ГОСТ Р 6.30-2003. «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов»
12.	ГОСТ 28195-89. «Оценка качества программных средств. Общие положения»
13.	ГОСТ Р ИСО\МЭК 9126-90. «Информационная технология. Оценка программной продукции. Характеристика качества и руководства по их применению»
14.	ГОСТ Р 50739-95. «Средства вычислительной техники. Защита от несанкционированного доступа к информации»
15.	Рекомендации по стандартизации Р 50.1.053-2005. «Информационные технологии. Основные термины и определения в области технической защиты информации»
16.	Р 50.1.053-2005. Рекомендации по стандартизации. Информационные технологии. Основные термины и определения в области технической защиты информации.
17.	Р 50.1.056-2005. Рекомендации по стандартизации. Техническая защита информации. Основные термины и определения.
18.	ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.
19.	ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
20.	ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.
21.	ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

Научно-техническая литература

№ п/п	Наименование
1	Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации. Учебное пособие. В.С. Горбатов, С.В. Дворянкин и др., 2014
2	Контроль защищенности речевой информации в помещениях. Аттестационные испытания выделенных помещений по требованиям безопасности информации. Учебное пособие. В.С. Горбатов, А.П. Дураковский и др., 2014
3	Контроль защищенности информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок. Аттестационные испытания по требованиям безопасности информации. Учебное пособие. А.А. Голяков, В.С. Горбатов и др., 2014
4	Организация и содержание работ по выявлению и оценке основных видов ТКУИ, защита информации от утечки. А.В. Кондратьев, 2011
5	Защита объектов и информации от технических средств разведки. Учебное пособие. Ю.К. Меньшаков, 2002
6	Инженерно-техническая защита информации. Учебное пособие. А.А. Торокин, 2005
7	Информационная безопасность предприятия. И. Конеев, А. Беляев, 2003
8	Защита информации и безопасность компьютерных систем. В.В. Домарев, 1999
9	Информационная безопасность открытых систем. Угрозы, уязвимости, атаки и подходы к защите. Учебное пособие. С.В. Запечников, Н.Г. Милославская и др., 2006
10	Информационная безопасность. Учебное пособие. В.И. Ярочкин, 2004
11	Основы информационной безопасности. Учебное пособие. Е.Б. Белов, В.П. Лось и др., 2006
12	Защита компьютерной информации от несанкционированного доступа. А.Ю. Щеглов, 2004
13	Основы информационной безопасности объектов обработки информации. Научно-практическое пособие. С.Н. Семкин, А.Н. Семкин, 2000

14	Разработка правил информационной безопасности. С. Бармен, 2002
15	Основы информационной безопасности. Учебное пособие. В.А. Галатенко, 2004
16	Основы организационного обеспечения информационной безопасности объектов информатизации. Учебное пособие. С.Н. Семкин, Э. В. Беляков и др., 2005
17	Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие. А.А. Малюк, 2004
18	Введение в защиту информации в автоматизированных системах. Учебное пособие. А.А. Малюк, С.В. Пазизин, Н.С. Погожин, 2005
19	Общие критерии оценки безопасности информационных технологий. Учебное пособие. А.А. Сидак, 2004
20	Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. Г.Н. Устинов, 2000
21	Системный анализ в защите информации. Учебное пособие. А.А. Шумский, А.А. Шелупанов, 2005
22	Информационная безопасность. Учебное пособие. А.А. Губенков, В.Б. Байбурин, 2005
23	Теоретические основы защиты информации. Учебное пособие. С.С. Корт, 2004
24	Информационная безопасность автоматизированных систем. Учебное пособие. А.Ф. Чипига, 2010
25	Комплекс СЗИ от НСД «Аккорд-АМДЗ». Учебное пособие. Л.К. Бабенко, Е.А. Ищукова, 2007
26	Система защиты информации VipNet. Курс лекций. Н.В. Кабанова, А.О. Чефранова, 2014
27	Система защиты информации VipNet. Практикум. Н.В. Кабанова, А.О. Чефранова, 2013

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: Secret Net, Dallas Lock, 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 «Аттестация объектов информатизации по требованиям безопасности информации. Защита от несанкционированного доступа»;
- 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