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

«Основы обеспечения защиты информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

г. Королев
2016 г.

Перечень сокращений

ГИС	- государственная информационная система
ИС	- информационная система
ИСПДн	- информационная система персональных данных
НСД	- несанкционированный доступ
ОИ	- объект информатизации
ПО	- программное обеспечение
ПЭМИН	- побочные электромагнитные излучения и наводки
СЗИ	- средства защиты информации
СВТ	- средства вычислительной техники
ТК	- технический канал
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».

2. 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 в области информационной безопасности обладателей информации, заказчиков, заключивших государственный контракт на создание информационной системы (далее - заказчики), операторов государственных информационных систем (далее - операторы), а также организаций, выполняющих работы по разработке, внедрению и аттестации ГИС.

1.3. Категории обучающихся:

- заказчики ГИС;
- разработчики ГИС;
- операторы ГИС;
- 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 разработкой, проектированием, внедрением, аттестацией и эксплуатацией систем защиты информации в ГИС.

1.4.2. Объекты профессиональной деятельности

- государственные информационные системы;
- технологии обеспечения информационной безопасности ГИС;
- нормативно-правовые акты РФ в области защиты информации;
- нормативно- методические документы по защите информации ГИС;
- методы и средства обеспечения информационной безопасности в ГИС;
- методы проведения аттестационных испытаний;
- средства защиты информации от НСД и ТК;
- организационно-распорядительная, проектная и эксплуатационная документация;
- инструментальные средства контроля эффективности защиты информации.

1.4.3. Вид и задачи профессиональной деятельности

Вид профессиональной деятельности:

организация мероприятий по созданию и эксплуатации системы защиты информации ГИС в соответствии с нормативными правовыми актами и методическими документами, устанавливающими требования по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, содержащейся в ГИС.

Задачи (функции) профессиональной деятельности:

- организация защиты информации в ГИС;

- классификация ГИС;
- формирование требований по защите информации в ГИС;
- разработка системы защиты информации в ГИС;
- организация внедрения системы защиты информации в ГИС;
- организация аттестации ГИС и ввода в эксплуатацию;
- разработка организационно-распорядительной, проектной и эксплуатационной документации;
- управление конфигурацией ГИС;
- контроль за обеспечением уровнем защищенности ГИС.

1.5. Планируемые результаты обучения

Планируемый результат обучения по данной программе – качественное изменение профессиональных компетенций, позволяющих организовать мероприятия по созданию и эксплуатации системы защиты информации ГИС в соответствии с нормативными правовыми актами и методическими документами, устанавливающими требования по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, содержащейся в ГИС.

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

- способность формировать требования по защите информации в ГИС;
- способность организовать внедрение системы защиты информации ГИС;
- способность организовать аттестацию ГИС и ввод ее в эксплуатацию;
- способность обеспечить защиту информации при эксплуатации аттестованной ГИС;
- способность обеспечить защиту информации при выводе из эксплуатации аттестованной ГИС или после принятия решения об окончании обработки информации.

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				
		Л	СЗ	ПЗ	Зач	К, СР
Вводная лекция	**1**	**1**				
Раздел 1. Система государственного управления Российской Федерации. Организационно-правовые основы обеспечения безопасности информации	**2**	**1**	**1**			
Тема: Система и структура государственных органов власти, механизмы взаимодействия и принципы разграничения их полномочий. Структура государственной системы защиты информации	0,5	0,5				
Тема: Информационно-телекоммуникационные технологии в государственном управлении. Понятие государственной информационной системы	0,5	0,5				
Тема: Структура законодательной и нормативно-методической базы РФ в области защиты информации	1		1			
Раздел 2. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Основные положения	**8**	**3**	**2**			**3**
Тема: Роль и место Требований в системе нормативных и методических документов по защите информации в информационных системах. Структура Требований	1	1				
Тема: Система понятий, терминов и определений, используемых в Требованиях	2		1			1
Тема: Организация защиты информации, содержащейся в информационных системах. Основные мероприятия, реализуемые в информационных системах для обеспечения защиты информации	2	1				1
Тема: Общая характеристика мер защиты информации, подлежащих реализации в государственной информационной системе. Примеры реализации	3	1	1			1
Раздел 3. Основы формирования требований к защите информации, содержащейся в информационных системах	**5**	**1**	**2**			**2**
Тема: Классификация информационной системы	1	1				
Тема: Определение угроз безопасности информации в информационной системе. Разработка модели угроз	2		1			1
Тема: Определение требований к системе защиты информации в информационной системе. Выбор мер защиты информации, подлежащих реализации в информационной системе. Разработка технического задания	2		1			1
Раздел 4. Основы разработки и внедрения системы защи-	**11**	**2**	**4**	**1**		**4**

Наименование разделов и тем	Всего часов	В том числе				
		Л	СЗ	ПЗ	Зач	К, СР
ты информации информационной системы						
Тема: Основы проектирования системы защиты информации информационной системы	2	1				1
Тема: Эксплуатационная документация на систему защиты информации информационной системы. Основное содержание и виды документов	2		1			1
Тема: Порядок внедрения системы защиты информации информационной системы	2	1				1
Тема: Организационно-распорядительные документы по защите информации. Основное содержание и виды документов	2		1			1
Тема: Анализ уязвимостей информационной системы	3		2	1		
Раздел 5. Основы аттестации информационной системы по требованиям защиты информации и ввода ее в действие	**3**	**1**	**1**			**1**
Тема: Порядок и содержание работ по аттестации информационной системы. Программа и методики аттестационных испытаний	2	1				1
Тема: Особенности аттестации государственной информационной системы. Аттестация на основе типового сегмента системы	1		1			
Раздел 6. Основы защиты информации в ходе эксплуатации информационной системы и при выводе ее из эксплуатации	**8**	**3**	**2**			**3**
Тема: Управление системой защиты информации. Основное содержание работ	1	1				
Тема: Выявление инцидентов и реагирование на них. Основное содержание работ	2	1				1
Тема: Управление конфигурацией информационной системы. Основное содержание работ	2	1				1
Тема: Контроль за обеспечением уровня защищенности информации в информационной системе. Основные процедуры	2		1			1
Тема: Особенности обеспечения защиты информации при принятии решения об окончании обработки информации и выводе из эксплуатации информационной системы	1		1			
Раздел 7. Основное содержание мер защиты информации, содержащейся в информационной системе	**32**	**11**		**12**		**9**
Тема: Идентификация и аутентификация субъектов доступа и объектов доступа. Особенности реализации	3	1		1		1
Тема: Управление доступом субъектов доступа к объектам доступа. Особенности реализации	3	1		1		1
Тема: Ограничение программной среды. Особенности реализации	1	0,5		0,5		

Наименование разделов и тем	Всего часов	В том числе				
		Л	СЗ	ПЗ	Зач	К, СР
Тема: Защита машинных носителей информации. Особенности реализации	3	1		1		1
Тема: Регистрация событий безопасности. Особенности реализации	3	1		1		1
Тема: Антивирусная защита. Особенности реализации	1	0,5		0,5		
Тема: Обнаружение (предотвращение) вторжений. Особенности реализации	1	0,5		0,5		
Тема: Контроль (анализ) защищенности информации. Особенности реализации	3	1		1		1
Тема: Обеспечение целостности информационной системы и информации. Особенности реализации	3	1		1		1
Тема: Обеспечение доступности информации. Особенности реализации	3	1		1		1
Тема: Защита среды виртуализации. Особенности реализации	3	1		1		1
Тема: Защита технических средств. Особенности реализации	1	0,5		0,5		
Тема: Защита информационной системы, ее средств, систем связи и передачи данных. Особенности реализации	4	1		2		1
Итоговая аттестация (зачет)	**2**				**2**	
ИТОГО	**72**	**23**	**12**	**13**	**2**	**22**

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. Система государственного управления Российской Федерации. Организационно-правовые основы обеспечения безопасности информации	3	3							
Раздел 2. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Основные положения	8	6	2						
Раздел 3. Основы формирования требований к защите информации, содержащейся в информационных системах	5		5						
Раздел 4. Основы разработки и внедрения системы защиты информации информационной системы	11		2	9					
Раздел 5. Основы аттестации информационной системы по требованиям защиты информации и ввода ее в действие	3				3				
Раздел 6. Основы защиты информации в ходе эксплуатации информационной системы и при выводе ее из эксплуатации	8				6	2			
Раздел 7. Основное содержание мер защиты информации, содержащейся в информационной системе	32					7	9	9	7
Итоговая аттестация (зачет)	2								2

4.

2.3. Содержание разделов и тем

Содержание разделов, тем курса и изучаемых вопросов

Наименование разделов и тем (основные вопросы)	
Раздел 1. Система государственного управления Российской Федерации. Организационно-правовые основы обеспечения безопасности информации	
Тема	**Система и структура государственных органов власти, механизмы взаимодействия и принципы разграничения их полномочий. Структура государственной системы защиты информации** Понятие государственного управления. Органы государственного управления. Федеральные министерства, службы и агентства, подведомственные Президенту РФ и Правительству РФ (Указ Президента РФ от 21.05.2012г №636). Органы власти субъектов РФ. Органы местного самоуправления. Виды нормативных актов, издаваемых государственными органами. Понятие межведомственного взаимодействия. Постановление Правительства РФ от 19 января 2005 г № 30 «О Типовом регламенте взаимодействия федеральных органов исполнительной власти».

Тема	**Информационно-телекоммуникационные технологии в государственном управлении. Понятие государственной информационной системы** Современные технологии управления и государственные услуги. Концепция электронного правительства. Инфраструктура межведомственного электронного взаимодействия. Понятие государственной ИС.
Тема	**Структура законодательной и нормативно-методической базы РФ в области защиты информации** Федеральные законы и постановления Правительства РФ, осуществляющие правовое регулирование обработки и защиты информации. Виды информации ограниченного доступа. Виды документов, издаваемых государственными регуляторами. Структура и назначение документов в области защиты информации, сфера их применения. Обзор национальных стандартов в области защиты информации.
Раздел 2. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Основные положения	
Тема	**Роль и место Требований в системе нормативных и методических документов по защите информации в информационных системах. Структура Требований** Область действия Требований. Целевая аудитория документа. Роль и место Требований в системе нормативных и методических документов по защите информации в ИС. Структура Требований.
Тема	**Система понятий, терминов и определений, используемых в Требованиях** Система понятий предметной области «Защита информации». Стандартизованные термины и их определения. Схема взаимосвязи стандартизированных терминов. Основные термины и определения в области защиты информации от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации).
Тема	**Организация защиты информации, содержащейся в информационных системах. Основные мероприятия, реализуемые в информационных системах для обеспечения защиты информации** Объекты защиты информации ИС. Задачи и функции структурного подразделения по защите информации или должностного лица (работника), назначенного ответственным за защиту информации в ИС. Основные мероприятия по обеспечению защиты информации ИС.
Тема	**Общая характеристика мер защиты информации, подлежащих реализации в государственной информационной системе. Примеры реализации** Требования к мерам защиты информации, применяемым в ГИС. Состав мер защиты информации и их назначение. Общий порядок действий по выбору мер защиты информации для их реализации в информационной системе. Примеры и особенности реализации технических мер защиты информации ИС.
Раздел 3. Основы формирования требований к защите информации, содержащейся в информационных системах	
Тема	**Классификация информационной системы** Анализ целей создания ИС и задач, решаемых этой системой. Определение информации, подлежащей обработке в ИС. Принятие решения о необходимости создания системы защиты информации в ИС. Порядок классификации ИС. Особенности определения масштаба ИС. Основные подходы к определению уровня значимости информации и степени возможного ущерба. Особенности классификации распределенных и сегментированных ИС.
Тема	**Определение угроз безопасности информации в информационной системе. Разработка модели угроз** Классификация нарушителей безопасности информации. Оценка возможностей внешних и внутренних нарушителей. Анализ возможных уязвимостей ИС. Виды угроз безопасности информации в зависимости от структурно-функциональных характеристик ИС. Способы реализации угроз, оценка последствий от нарушения свойств безопасности информации. Структура и содержание модели угроз безопасности информации.
Тема	**Определение требований к системе защиты информации в информационной системе.**

	Выбор мер защиты информации, подлежащих реализации в информационной системе. Разработка технического задания Порядок формирования требований к системе защиты информации в ИС. Определение перечня объектов защиты информации. Требования к защите информации в ИС при ее информационном взаимодействии с иными ИС. Выбор базового набора мер защиты информации. Адаптация базового набора мер защиты информации. Уточнение адаптированного базового набора мер защиты информации. Дополнение уточненного адаптированного базового набора мер защиты информации. Компенсирующие меры защиты информации. Содержание технического задания на систему защиты информации.
Раздел 4. Основы разработки и внедрения системы защиты информации информационной системы	
Тема	**Основы проектирования системы защиты информации информационной системы** Основные положения по проектированию ИС. Стадии создания. Основные типы субъектов доступа и объектов доступа. Методы и типы управления доступом. Порядок выбора видов и типов СЗИ, определение структуры системы защиты информации. Проектная документация на систему защиты информации в ИС.
Тема	**Эксплуатационная документация на систему защиты информации информационной системы. Основное содержание и виды документов.** Виды, назначение и основное содержание эксплуатационных документов. Рекомендации по подготовке, оформлению, согласованию и утверждению эксплуатационной документации.
Тема	**Порядок внедрения системы защиты информации информационной системы** Состав работ по внедрению системы защиты информации ИС. Организационные меры защиты информации ИС и их содержание. Виды испытаний ИС и их содержание.
Тема	**Организационно-распорядительные документы по защите информации. Основное содержание и виды документов** Правила и процедуры, реализуемые оператором для обеспечения защиты информации ИС. Виды и основное содержание организационно-распорядительных документов по защите информации ИС.
Тема	**Анализ уязвимостей информационной системы** Уязвимости ИС. Методы выявления уязвимостей. Порядок и содержание работ по анализу уязвимостей технических средств, программного обеспечения и средств защиты информации ИС. Средства контроля защищенности информации ИС.
Раздел 5. Основы аттестации информационной системы по требованиям защиты информации и ввода ее в действие	
Тема	**Порядок и содержание работ по аттестации информационной системы. Программа и методики аттестационных испытаний** Порядок проведения аттестационных испытаний. Типовое содержание аттестационных испытаний. Основные факторы, определяющие содержание и объем аттестационных испытаний. Типовое содержание программы и методик аттестационных испытаний. Основные методы аттестационных испытаний. Характеристика работ, проводимых в рамках аттестации. Особенности проверки соответствия реализованных мер защиты информации установленным требованиям. Протоколирование результатов аттестационных испытаний.
Тема	**Особенности аттестации государственной информационной системы. Аттестация на основе типового сегмента системы** Понятие выделенного набора сегментов ИС. Принятие решения о соответствии сегмента ИС выделенному набору сегментов. Условия распространения аттестата на другие сегменты. Особенности аттестации сегмента ИС.
Раздел 6. Основы защиты информации в ходе эксплуатации информационной системы и при выводе ее из эксплуатации	
Тема	**Управление системой защиты информации. Основное содержание работ** Управление средствами защиты информации в ИС. Управление учетными записями и параметрами настройки ПО. Восстановление работоспособности средств защиты информации. Установка обновлений прикладного ПО и СЗИ. Централизованное управление систе-

	мой защиты информации. Регистрация и анализ событий безопасности в ИС.
Тема	**Выявление инцидентов и реагирование на них. Основное содержание работ** Понятие инцидента информационной безопасности. Обнаружение, идентификация и анализ инцидентов, оценка их последствий. Планирование и принятие мер по устранению инцидентов, по восстановлению ИС и ее сегментов в случае отказа в обслуживании или после сбоев. Меры по предотвращению повторного возникновения инцидентов.
Тема	**Управление конфигурацией информационной системы. Основное содержание работ** Процедуры поддержки базовой конфигурации ИС и системы защиты информации в соответствии с эксплуатационной документацией. Управление изменениями базовой конфигурации, определение типов возможных ее изменений. Анализ потенциального воздействия планируемых изменений в ИС на обеспечение защиты информации, на возникновение дополнительных угроз безопасности информации и работоспособность ИС. Определение состава и конфигурации технических средств и ПО до внесения изменений в базовую конфигурацию ИС. Принятие решения по результатам управления конфигурацией о повторной аттестации ИС или проведении дополнительных аттестационных испытаний.
Тема	**Контроль за обеспечением уровня защищенности информации в информационной системе. Основные процедуры** Основные способы контроля за событиями безопасности и действиями пользователей в ИС. Анализ защищенности информации, оценка функционирования системы защиты информации. Устранение недостатков в функционировании системы защиты информации. Способы периодического анализа изменения угроз безопасности информации в ИС, возникающих в ходе ее эксплуатации. Документирование результатов контроля за обеспечением уровня защищенности информации.
Тема	**Особенности обеспечения защиты информации при принятии решения об окончании обработки информации и выводе из эксплуатации информационной системы** Архивирование информации, содержащейся в ИС. Уничтожение данных и остаточной информации с машинных носителей информации. Требования к уничтожению машинных носителей информации.
Раздел 7. Основное содержание мер защиты информации, содержащейся в информационной системе	
Тема	**Идентификация и аутентификация субъектов доступа и объектов доступа. Особенности реализации** Характеристика и содержание мер ИАФ (идентификация и аутентификация субъектов доступа и объектов доступа). Особенности реализации данной группы мер защиты информации, содержащейся в ИС.
Тема	**Управление доступом субъектов доступа к объектам доступа. Особенности реализации** Характеристика и содержание мер УПД (управление доступом субъектов доступа к объектам доступа). Особенности реализации данной группы мер защиты информации, содержащейся в ИС.
Тема	**Ограничение программной среды. Особенности реализации** Характеристика и содержание мер ОПС (ограничение программной среды). Особенности реализации данной группы мер защиты информации, содержащейся в ИС.
Тема	**Защита машинных носителей информации. Особенности реализации** Характеристика и содержание мер ЗНИ (защита машинных носителей информации). Особенности реализации данной группы мер защиты информации, содержащейся в ИС.
Тема	**Регистрация событий безопасности. Особенности реализации** Характеристика и содержание мер РСБ (регистрация событий безопасности). Особенности реализации данной группы мер защиты информации, содержащейся в ИС.
Тема	**Антивирусная защита. Особенности реализации** Характеристика и содержание мер АВЗ (антивирусная защита). Особенности реализации данной группы мер защиты информации, содержащейся в ИС.
Тема	**Обнаружение (предотвращение) вторжений. Особенности реализации** Характеристика и содержание мер СОВ (система обнаружения вторжений). Особенности

	реализации данной группы мер защиты информации, содержащейся в ИС.
Тема	**Контроль (анализ) защищенности информации. Особенности реализации** Характеристика и содержание мер АНЗ (анализ защищенности информации). Особенности реализации данной группы мер защиты информации, содержащейся в ИС.
Тема	**Обеспечение целостности информационной системы и информации. Особенности реализации** Характеристика и содержание мер ОЦЛ (обеспечение целостности информационной системы и информации). Особенности реализации данной группы мер защиты информации, содержащейся в ИС.
Тема	**Обеспечение доступности информации. Особенности реализации** Характеристика и содержание мер ОДТ (обеспечение доступности информации). Особенности реализации данной группы мер защиты информации, содержащейся в ИС.
Тема	**Защита среды виртуализации. Особенности реализации** Характеристика и содержание мер ЗСВ (защита среды виртуализации). Особенности реализации данной группы мер защиты информации, содержащейся в ИС.
Тема	**Защита технических средств. Особенности реализации** Характеристика и содержание мер ЗТС (защита технических средств). Особенности реализации данной группы мер защиты информации, содержащейся в ИС.
Тема	**Защита информационной системы, ее средств, систем связи и передачи данных. Особенности реализации** Характеристика и содержание мер ЗИС (защита информационной системы, ее средств, систем связи и передачи данных). Особенности реализации данной группы мер защиты информации, содержащейся в ИС.
	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. 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. Малюк. Теория защиты информации, 2012 г.
2.	В. Платонов. Программно-аппаратные средства защиты информации, 2013 г.
3.	Ю. Громов, В. Драчев, О. Иванова, Н. Шахов. Информационная безопасность и защита информации, 2010 г.
4.	Л. Бабенко, А. Басан, И. Журкин, О. Макаревич. Защита данных геоинформационных систем, 2010 г.
5.	В. Сердюк. Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий, 2011 г.
6.	М. Борисов, И. Заводцев, И. Чижов. Основы программно-аппаратной защиты информации, 2013 г.
7.	В.Ф. Шаньгин. Информационная безопасность и защита информации, 2014 г.
8.	А. Малюк, С. Пазизин, Н. Погожин. Введение в защиту информации в автоматизированных системах, 2011 г.
9.	А.И. Тимошкин, О.М. Лепешкин, А.П. Жук. Защита информации. Учебное пособие, 2013 г.

3.4.3. Дополнительная 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.	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»
8.	Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»
9.	Указ Президента Российской Федерации от 06 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»
10.	Доктрина информационной безопасности Российской Федерации. (утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895)
11.	Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «Об утверждении Положения о сертификации средств защиты информации»
12.	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»
13.	Постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79 «Об утверждении Положения о лицензировании деятельности по технической защите конфи-

	денциальной информации»
14.	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»
15.	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.	Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах» (утвержден директором ФСТЭК России 11 февраля 2014 г.)
4.	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.)
5.	Методика определения актуальных угроз безопасности персональных при их обработке в информационных системах персональных 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.	Административный регламент ФСТЭК по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации (утвержден Приказом ФСТЭК от 12 июля 2012 г. №83)
10.	Приказ ФСТЭК от 06 декабря 2011г. №638 «Об утверждении требований к системам обнаружения вторжений»
11.	Приказ ФСТЭК от 20 марта 2012 г. №28 «Об утверждении требований к средствам антивирусной защиты»
12.	Приказ ФСТЭК от 27 сентября 2013 г. №119 «Об утверждении требований к средствам доверенной загрузки»
13.	Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации (утверждено председателем Гостехкомиссии России 25 ноября 1994 г.)
14.	«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.
15.	«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.
16.	«Временная методика оценки защищенности речевой конфиденциальной информации от утечки по акустическому и виброакустическому каналам», Гостехкомиссия России, Москва,

	2001 г.
17.	«Временная методика оценки защищенности речевой конфиденциальной информации от утечки за счет электроакустических преобразований в вспомогательных технических средствах и системах», Гостехкомиссия России, Москва, 2001 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.
Национальные стандарты	
№ п/п	**Наименование**
1.	ГОСТ Р 51583. «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»
2.	ГОСТ Р50922-2006. «Защита информации. Основные термины и определения»
3.	ГОСТ Р 51624-2000. «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования».
4.	ГОСТ РО 0043-003 2012 «Защита информации. Аттестация объектов информатизации. Общие положения»
5.	ГОСТ РО 0043-004 2013 «Защита информации. Программа и методики аттестационных испытаний»
6.	ГОСТ Р 51275-2006. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»
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 ИСО/МЭК 15408. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
16.	ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
Научно-техническая литература	
№ п/п	**Наименование**
1.	С.С. Корт. Теоретические основы защиты информации, 2004 г.
2.	В.В. Домарев. Безопасность информационных технологий. Системный подход, 2004 г.
3.	С.Н. Семкин и др. Основы организационного обеспечения информационной безопасности объектов информатизации, 2005 г.
4.	В.В. Мельников. Безопасность информации в автоматизированных системах, 2003 г.

5.	А.Ю. Щеглов. Защита компьютерной информации от несанкционированного доступа, 2004 г.
6.	Т.Л. Партыка, Попов И.И. Информационная безопасность, 2004 г.
7.	С.В. Лебедь. Межсетевое экранирование. Теория и практика защиты внешнего периметра, 2002 г.
8.	Скотт Бармен. Разработка правил информационной безопасности, 2002 г.
9.	Вильям Столлинг. Основы защиты сетей. Приложения и стандарты, 2002 г.
10.	В. Зима, А. Молдовян. Безопасность глобальных сетевых технологий, 2003 г.
11.	П. Девянин. Анализ безопасности управления доступом и информационными потоками в компьютерных системах, 2006 г.
12.	Н.А. Гайдамакин. Разграничение доступа к информации в компьютерных системах, 2003 г.
13.	А.А. Шумский, А.А. Шелупанов. Системный анализ в защите информации, 2005 г.
14.	В.Я. Асанович, Т.Г. Маньшин. Информационная безопасность: анализ и прогноз информационного воздействия, 2006 г.
15.	Ю.К. Меньшаков. Защита объектов и информации от технических средств разведки, 2002 г.
16.	С.А. Петренко, А.А. Петренко. Аудит безопасности INTRANET, 2002 г.
17.	А.А. Малюк. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие, 2004 г.
18.	А.А. Малюк. Введение в защиту информации в автоматизированных системах, 2005 г.
19.	Е.Б. Белов, В.П. Лось. Основы информационной безопасности. Учебное пособие, 2006 г.
20.	А.А. Сидак. Общие критерии оценки безопасности информационных технологий. Учебное пособие, 2004 г.
21.	С.М. Климов. Методы и модели противодействия компьютерным атакам, 2008 г.

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