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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

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

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

Дополнительная профессиональная программа
повышения квалификации специалистов
в области информационной безопасности

«Организация и проведение работ по оценке (подтверждению) соответствия требованиям по безопасности информации продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну»
(СЗИ НСД)

г. Королев
2016 г.

Перечень сокращений

АРМ	-автоматизированное рабочее место
ЗБ	-задание по безопасности
ИТ	- информационная технология
МЭ	- межсетевой экран
НСД	- несанкционированный доступ
ОО	- объект оценки
ОУД	- оценочный уровень доверия
ПЗ	- профиль защиты
ПО	- программное обеспечение
РД	- руководящий документ
СЗИ	- средства защиты информации
СВТ	- средства вычислительной техники
ТДБ	- требование доверия безопасности
ФСТЭК	- Федеральная служба по техническому и экспортному контролю
ФТБ	-функциональное требование безопасности

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 программы является повышение у слушателей уровня профессиональных компетенций, необходимых для выполнения работпо сертификации средств защиты информации и экспертизы материалов сертификационных испытаний в Системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01.БИ00.

1.3. Категории обучающихся:

- руководители и специалисты испытательных лабораторий;
- эксперты органов по сертификации средств защиты информации и экспертизы материалов сертификационных испытаний.

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 оценкой (подтверждением) соответствия средств защиты информации требованиям по безопасности информации (обязательной сертификации средств защиты информации по требованиям безопасности информации).

1.4.2. Объекты профессиональной деятельности

Объектом профессиональной деятельности являются средства защиты информации, включающие:

- средства защиты информации от несанкционированного доступа, включая средства, в которых они реализованы, а также средства контроля эффективности защиты информации от несанкционированного доступа;
- средства обеспечения безопасности информационных технологий, включая защищенные средства обработки информации.

1.4.3. Вид и задачи профессиональной деятельности

Вид профессиональной деятельности:

организация и проведение работ по оценке (подтверждению) соответствия требованиям по безопасности информации продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну.

Задачи профессиональной деятельности:

– организация работ по проведению сертификационных испытанийсредств защиты информации по требованиям безопасности информации;

– разработка программ и методик сертификационных испытаний средств защиты информации по требованиям безопасности информации;

– проведение сертификационных испытаний средств защиты информации в соответствии с утвержденными программами и методиками;

– разработка программ и методик предварительной проверки производствасредств защиты информации;

– проведение предварительной проверки производствасредств защиты информации;

– разработка отчетных материалов по результатам сертификационных испытаний и предварительной проверки производства;

– экспертиза материалов сертификационных испытанийи предварительной проверки производства.

1.5.Планируемые результаты обучения

Процесс освоения обучающимися дополнительной профессиональной программы повышения квалификациинаправлен на качественное изменение компетенций в области оценки соответствия требованиям по безопасности информации продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну.

В результате освоения дополнительной профессиональной программы повышениякваликациинобучающиеся должны получить знания, умения и навыки, которые позволят качественно изменить их компетенции в области оценки (подтверждения) соответствия средств защиты информации требованиям по безопасности информации.

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

– способность организовать работы по сертификации средств защиты информации;

– способность разрабатывать программы и методики сертификационных испытаний средств защиты информации;

– способность разрабатывать программы и методики предварительной проверки производства сертифицируемых средств защиты информации;

– способность проводить сертификационные испытания средств защиты информации;

– способность разрабатывать отчетную документацию по результатам сертификационных испытаний;

– способность проводить экспертизу материалов сертификационных испытаний и предварительной проверки производства средств защиты информации.

Обучающийся, освоивший программу повышения квалификации, должен

знать:

– законодательные и нормативные акты Российской федерации в области оценки соответствия требованиям по безопасности информации продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну;

– структуру системы сертификации средств защиты информации в Российской Федерации и принципы её деятельности;

– нормативные правовые акты ФСТЭК России, касающиеся организации и порядка проведения работ в Системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01.БИ00;

– нормативные правовые акты ФСТЭК России, определяющие требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа;

– государственные и международные стандарты, определяющие требования к средствам защиты информации, организацию и методы проведения оценки их соответствия требованиям по безопасности информации;

– методические документы ФСТЭК России, определяющие методы (методики) в области оценки (подтверждения) соответствия средств защиты информации требованиям по безопасности информации.

уметь:

– организовывать работы по проведению сертификационных испытаний средств защиты информации по требованиям безопасности информации;

– разрабатывать программы и методики сертификационных испытанийсредств защиты информации по требованиям безопасности информации;

– организовывать и проводить испытания средств защиты информации по требованиям безопасности информации;

– выполнять работы с использованием измерительныхприборов, испытательного оборудования, программных(программно-аппаратных) средств, в том числе средств контроля защищённости информации, средств контроля (анализа) исходных текстов программного обеспечения (с учетом области деятельности испытателя (эксперта);

– разрабатывать программы и методики предварительной проверки производствасредств защиты информации;

– организовывать и проводить предварительную проверку производствасредств защиты информации;

– проводить экспертизу материалов сертификационных испытанийи предварительной проверки производства.

владеть:

– профессиональной терминологией;
– методами технической защиты информации;
– методами организации и управления деятельностью;
– методами проведения сертификационных испытаний.

1.6. Трудоемкость программы

Общая трудоемкостьосвоения данной программы повышения квалификации составляет 72(семьдесят два) часа.

1.7. Форма и сроки обучения

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

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

1.8. Режим занятий

Учебные занятия проводятся в соответствии с расписанием, утверждаемым директором.

Продолжительность одного занятия – 45 минут.

Перерыв между занятиями 10 минут.

Перерыв на обед – 1 час.

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

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный план

Наименование разделов (тем)	Всего часов	В том числе, час				
		Л	СЗ	ПЗ	Зач	К, СР
Раздел 1. Вводная часть.	**2**	**2**				
Тема1. Законодательные, нормативные правовые акты, стандарты и методические документы, регламентирующие проведение работ по оценке соответствия требованиям по безопасности информации продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну.	2	2				
Раздел 2. Организационная структура и задачи Системы сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01.БИ00.	**2**	**2**				
Тема 2. Перечень продукции, подлежащей оценке соответствия в Системе сертификации средств защиты информации по требованиям безопасности информации. Основные требования к продукции и схемы ее сертификации.	1	1				
Тема 3. Организационная структура Системы сертификации средств защиты информации по требованиям безопасности информации, основные задачи и предъявляемые требования к ее элементам.	1	1				
Раздел 3. Порядок организации и проведения сертификационных испытаний	**13**	**8**	**5**			
Тема 4. Процедура сертификации средств защиты информации и инспекционного контроля сертифицированной продукции.	1	1				
Тема 5. Порядок оформления и подачи заявки на проведение сертификации продукции в Системе сертификации средств защиты информации по требованиям безопасности.	1	1				
Тема 6. Требования к содержанию программы и методики сертификационных испытаний.	1	1				
Тема 7. Разработка и согласование Программы и методики сертификационных испытаний.	2		2			
Тема 8. Требования к производству сертифицированных средств защиты информации.	2	2				
Тема 9. Программа предварительной проверки производства.	1	1				
Тема 10. Порядок проведения предварительной проверки производства.	1	1				
Тема 11. Содержание и порядок разработки отчетных материалов испытательной лаборатории по результатам сертификационных испытаний СЗИ.	2		2			
Тема 12. Особенности проведения экспертизы материалов сертификационных испытаний средств защиты информации.	2	1	1			
Раздел 4. Основные положения ГОСТ ИСО/МЭК 15408.	**16**	**7**	**4**	**1**		**4**

Наименование разделов (тем)	Всего часов	В том числе, час				
		Л	СЗ	ПЗ	Зач	К, СР
Тема 13. Основные понятия и принципы оценки безопасности ИТ, общая модель оценки.	2	1				1
Тема 14. Формирование требований безопасности к изделиям ИТ.	4	1	2	1		
Тема 15. Концепция профиля защиты и задания по безопасности.	3	1	1			1
Тема 16. Функциональные компоненты безопасности, зависимости функциональных компонентов безопасности, операции над функциональными компонентами безопасности.	3	2				1
Тема 17. Компоненты доверия к безопасности, оценочные уровни доверия к безопасности.	4	2	1			1
Раздел 5. Принципы построения и особенности применения нормативных документов ФСТЭК России, определяющих требования к средствам защиты информации.	**7**	**1**	**6**			
Тема 18. Структура и принципы построения нормативных правовых и методических документов ФСТЭК России.	1	1				
Тема 19. Особенности применения правовых и методических документов для отдельных видов изделий ИТ.	6		6			
Раздел 6. Основные требования к подготовке документации на изделие, представляемое на сертификационные испытания.	**8**	**5**		**3**		
Тема 20. Требования к разработке профилей защиты и заданий по безопасности.	4	2		2		
Тема 21. Требования к разработке проектной и эксплуатационной документации на сертифицируемое изделие.	2	2				
Тема 22. Рекомендации по подготовке материалов свидетельств для оценки.	2	1		1		
Раздел 7. Методология оценки безопасности информационных технологий.	**20**	**6**	**3**	**7**		**4**
Тема 23. Общие положения методологии оценки безопасности информационных технологий.	2	2				
Тема 24. Содержание работ по оценке профилей защиты и заданий по безопасности.	4		2			2
Тема 25. Методы проведения и формирования заключений по результатам оценки безопасности изделий ИТ.	3	1	1	1		
Тема 26. Особенности проведения сертификационных испытаний изделий на соответствие требованиям Руководящего документа по контролю отсутствия недекларированных возможностей.	4	2		2		
Тема 27. Методы проведения анализа отсутствия уязвимостей сертифицируемого изделий и среды его функционирования.	2	1		1		
Тема 28. Использование программных средств анализа и контроля при проведении сертификационных испытаний	5			3		2
Итоговая аттестация (зачет)	**4**				**4**	
	72	**31**	**18**	**11**	**4**	**8**

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 сертификации средств защиты информации.

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. Вводная часть.	2	2							
Раздел 2. Организационная структура и задачи Системы сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01.БИ00.	2	2							
Раздел 3. Порядок организации и проведения сертификационных испытаний	13	5	8						
Раздел 4. Основные положения ГОСТ ИСО/МЭК 15408.	16		1	9	6				
Раздел 5. Принципы построения и особенности применения нормативных документов ФСТЭК России, определяющих требования к средствам защиты информации.	7				3	4			
Раздел 6. Основные требования к подготовке документации на изделие, представляемое на сертификационные испытания.	8					5	3		
Раздел 7. Методология оценки безопасности информационных технологий.	20						6	9	5
Итоговая аттестация	4								4

СОДЕРЖАНИЕ РАЗДЕЛОВ И ТЕМ

Раздел 1. Вводная часть.

Тема1. Законодательные, нормативные правовые акты, стандарты и методические документы, регламентирующие проведение работ по оценке соответствия требованиям по безопасности информации продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну.

Законодательство Российской Федерации о подтверждении соответствия продукции требованиям технических регламентов, положениям стандартов, сводов правил и особенностях технического регулирования продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну (далее средств защиты информации). Особенности оценки соответствия средств защиты информации, определяемые постановлениями Правительства Российской Федерации, нормативными правовыми актами ФСТЭК России.

Раздел 2. Организационная структура и задачи Системы сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01.БИ00.

Тема 2. Перечень продукции, подлежащей оценке соответствия в Системе сертификации средств защиты информации по требованиям безопасности информации. Основные требования к продукции и схемы ее сертификации.

Перечень средств защиты информации, подлежащихобязательной сертификации в системе сертификации ФСТЭК России и их общая характеристика.Основные требования к представлению на сертификацию технических средств защиты от утечки информации по техническим каналам, технических, программных и программно-технических средств защиты информации от НСД. Возможные схемы сертификации средств защиты информации и их характеристика.

Тема 3. Организационная структура Системы сертификации средств защиты информации по требованиям безопасности информации, основные задачи и предъявляемые требования к ее элементам.

Структура Системы сертификации средств защиты информации по требованиям безопасности информации ФСТЭК России. Функции Федерального органа по сертификации, органов по сертификации, испытательных лабораторий и заявителей. Порядок аккредитации органов по сертификации и испытательных лабораторий. Задачи, права и ответственность органов по сертификации и испытательных лабораторий. Система качества органов по сертификации и испытательных лабораторий.

Раздел 3. Порядок организации и проведения сертификационных испытаний

Тема 4. Процедура сертификации средств защиты информации и инспекционного контроля сертифицированной продукции.

Основные принципы проведения сертификационных испытаний. Общие требования к порядку проведения сертификационных испытаний и аттестации производства средств защиты информации. Особенности проведения отдельных видов работ в ходе сертификационных испытаний средств защиты информации на материально-технической базе их разработчика (производителя), не являющегося Заявителем.Требования к экспертизе материалов сертификационных испытаний. Порядок, периодичность и объем проведения государственного контроля и надзора и инспекционного контроля за сертифицированными средствами защиты информации. Информирование о результатах сертификации средств защиты информации, рассмотрение апелляций.

Тема 5. Порядок оформления и подачи заявки на проведение сертификации продукции в Системе сертификации средств защиты информации по требованиям безопасности.

Требования к заявителю, подающему заявку на сертификацию средств защиты информации. Содержание заявки на проведение сертификации. Определение нормативных документов, на соответствие которым предполагается проводить сертификацию средств защиты информации. Требования к документам, представляемым заявителем при подаче заявки на сертификацию. Содержание решения на сертификацию.

Тема 6. Требования к содержанию программы и методики сертификационных испытаний.

Структура программы и методики сертификационных испытаний. Описание объекта испытаний, цель испытаний, условия, объем, методы и порядок проведения испытаний. Требования к описанию испытательного стенда. Особенности описания методик проведения испытаний для конкретных средств защиты информации.

Тема 7. Разработка и согласование Программы и методики сертификационных испытаний.

Требования нормативных и методических документов, определяющих порядок разработки и согласования Программы и методики сертификационных испытаний.Практическая разработка Программы и методики сертификационных испытаний на конкретные образцы средств защиты информации.

Тема 8. Требования к производству сертифицированных средств защиты информации.

Требования основных нормативных документов и государственных стандартов по организации производства продукции. Управление качеством продукции. Особенности производства технических и программных средств защиты информации.

Тема 9. Программа предварительной проверки производства.

Структура программы предварительной проверки производства продукции на соответствие требованиям по обеспечению качестваи неизменности сертифицируемых параметров. Описание объекта проверки, цели проверки, объема проверок, условий и порядка проведения проверки, отчетности.

Тема 10. Порядок проведения предварительной проверки производства.

Проверка организации производства. Проверка системы качества производства. Контроль управления документацией и данными, организации контроля за закупками комплектующих. Контроль идентификации и прослеживаемости продукции. Контроль проведения испытаний продукции. Проверка материально-технического обеспечения производства продукции и ее испытаний.

Тема 11. Содержание и порядок разработки отчетных материалов испытательной лаборатории по результатам сертификационных испытаний СЗИ.

Структура технического отчета при оценке ПЗ и при оценке ОО. Структура протокола сертификационных испытаний. Описание архитектуры ОО. Сведения о методах оценки, технологии, инструментальных средствах и применяемых стандартах. Структура и содержание технического заключения.

Тема 12. Особенности проведения экспертизы материалов сертификационных испытаний средств защиты информации.

Порядок проведения экспертизы материалов сертификационных материалов. Основные принципы и правила проведения экспертизы. Обязанности эксперта. Оформление результатов экспертизы.

Раздел 4. Основные положения ГОСТ ИСО/МЭК 15408.

Тема 13. Основные понятия и принципы оценки безопасности ИТ, общая модель оценки.

Определение объекта оценки, различные представления и конфигурации объектов оценки. Понятия, используемые при оценке и их взаимосвязь. Корректность объекта оценки и среды функционирования. Этапы и результаты оценки.

Тема 14. Формирование требований безопасности к изделиям ИТ.

Использование функциональных компонент и компонент доверия из ИСО/МЭК 15408. Разрешённые операции для конкретизации требований. Условия выполнения операций «итерация», «назначение», «выбор», «уточнение». Зависимости между компонентами.

Тема 15. Концепция профиля защиты и задания по безопасности.

Структура и содержание ПЗ и ЗБ. Взаимосвязь между содержанием ПЗ, ЗБ и объектом оценки (ОО). Порядок применения профилей защиты. Многократное использование профилей защиты. Результаты оценки ПЗ, ЗБ и ОО.Использование результатов оценки ЗБ и ОО.

Тема 16. Функциональные компоненты безопасности, зависимости функциональных компонентов безопасности, операции над функциональными компонентами безопасности.

Парадигма функциональных требований. Форма представления функциональных требований.Структура класса, семейства и компонента функциональных требований. Описание классов функциональных компонент безопасности. Таблицы перекрестных ссылок зависимостей функциональных компонент.

Тема 17. Компоненты доверия к безопасности, оценочные уровни доверия к безопасности.

Парадигма доверия, причины и значимость уязвимостей. Структура классов, семейств и компонентов доверия к безопасности. Описание оценочных уровней доверия, составных пакетов доверия, классов доверия. Зависимость между компонентами доверия.

Раздел 5. Принципы построения и особенности применения нормативных документов ФСТЭК России, определяющих требования к средствам защиты информации.

Тема 18. Структура и принципы построения нормативных правовых и методических документов ФСТЭК России.

Обзор действующих нормативных правовых и методических документов ФСТЭК России, их взаимосвязь и особенности применения при проведении сертификации средств защиты информации.

Тема 19. Особенности применения правовых и методических документов для отдельных видов изделий ИТ.

Особенности применения при сертификации нормативных и методических документов, определяющих требования к конкретным видам средств защиты информации (средствам антивирусной защиты, системам обнаружения вторжений, доверенной загрузки, контроля съемных носителей информации и др.). Особенности сертификации на соответствие требованиям РД СВТ, РД МЭ, технических условий.

Раздел 6. Основные требования к подготовке документации на изделие, представляемое на сертификационные испытания.

Тема 20. Требования к разработке профилей защиты и заданий по безопасности.

Общая информация по разработке иисполь зованию профилей защиты и заданий по безопасности. Уточнение требований профилей защитыи заданий по безопасности. Дополнение требований профилей защитыи заданий по безопасности.

Тема 21. Требования к разработке проектной и эксплуатационной документации на сертифицируемое изделие.

Требования нормативных документов и государственных стандартов к структуре и содержанию технических условий, формуляра,проектных документов, руководств по эксплуатации и других документов на средство защиты информации, предусмотренных нормативными методическими документами ФСТЭК России.

Тема 22. Рекомендации по подготовке материалов свидетельств для оценки.

Состав свидетельств. Требования к содержанию свидетельств. Рекомендации по их разработке.

Раздел 7. Методология оценки безопасности информационных технологий.

Тема 23. Общие положения методологии оценки безопасности информационных технологий.

Общая модель методологии оценки. Получение исходных данных для оценки. Выполнение подвидов деятельности по оценке. Оформление результатов оценки. Содержание технического отчета по оценке. Демонстрация компетентности органу по оценке.

Тема 24. Содержание работ по оценке профилей защиты и заданий по безопасности.

Требования и методология оценки ПЗ и ЗБ.Идентификация ПЗ, оценка проблем и целей безопасности, оценка определения расширенных компонентов, оценка четкости, недвусмысленности, полноты и внутренней непротиворечивости требований безопасности.Идентификация ЗБ и ОО, оценка утверждения о соответствии, оценка четкости определения проблемы и целей безопасности, оценка определения расширенных компонентов,оценка четкости, недвусмысленности, полноты и внутренней непротиворечивости описания функциональных требований безопасности (ФТБ) и требований доверия безопасности (ТДБ).

Тема 25. Методы проведения и формирования заключений по результатам оценки безопасности изделий ИТ.

Оценка проектной документации, руководств для пользователей, процедур, применяемых для разработки и сопровождения объекта оценки, анализ свидетельств разработчика, независимое тестирование. Оценка уязвимостей в объекте оценке и среде функционирования, исследование и тестирование взаимодействия между компонентами объекта оценки.

Тема 26. Особенности проведения сертификационных испытаний изделий на соответствие требованиям Руководящего документа по контролю отсутствия недекларированных возможностей.

Структура и содержание руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». Методика проведения испытаний программного обеспечения СЗИ для различных уровней контроля отсутствия недекларированных возможностей.

Тема 27. Методы проведения анализа отсутствия уязвимостей сертифицируемого изделий и среды его функционирования.

Обзор методов проведения анализа отсутствия уязвимостей сертифицируемого изделий и среды его функционирования и применяемых для этих целей программ анализа кода.

Тема 28. Использование программных средств анализа и контроля при проведении сертификационных испытаний

Обзор программных средств анализа и контроля и возможность их применения при проведении сертификационных испытанийсредств защиты от несанкционированного доступа к 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 аудиториии специализированные классы.Учебные аудитории оборудованы учебными досками, компьютерами, экранами и мультимедийными проекторами. Специализированные классы оборудованы стендами и компьютерами с установленнымлицензионным программным обеспечением,средствами защиты информации, инструментальными средствами контроля эффективностизащиты информации, а также инструментальными средствами, позволяющими отрабатывать практические навыки проведения сертификационных испытаний.

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

3.4. Требования к информационному и учебно-методическому обеспечению программы

3.4.1. Основная литература

№ п/п	Наименование
1.	В.В. Липаев. Сертификация программных средств, СИНТЕГ, Москва, 2010 г.
2.	В.В. Липаев. Методы обеспечения качества крупномасштабных программных средств, СИНТЕГ, Москва, 2003 г.
3.	Д.П. Зегжда, А.М. Ивашко. Как построить защищённую информационную систему, 1997 г.
4.	А.П. Трубачев. Концептуальные вопросы оценки безопасности информационных технологий, JetInfo, 1998 г.
5.	Трубачев А.П., Долинин М.Ю., Кобзарь М.Т.,Сидак А.А., Сороковиков В.И., под общей редакцией В.А. Галатенко. Оценка безопасности информационных технологий. Москва, 2001 г.
6.	А.А.Сидак. Общие критерии оценки безопасности информационных технологий.Учебное пособие, 2004г.
7.	Сидак А.А. Формирование требований безопасности современных сетевых ин технологий, Москва, 2001 г.
8.	В. Платонов. Программно-аппаратные средства защиты информации, 2013 г.
9.	А. Малюк. Теория защиты информации, 2012 г.
10.	А.И. Тимошкин, О.М.Лепешкин, А.П.Жук. Защита информации. Учебное пособие, 2013 г.

3.4.2. Дополнительная литература

№ п/п	Наименование
	Законодательно-правовые акты
1.	Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»
2.	Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»
3.	Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельно-

	сти».
4.	Федеральный закон от 28 декабря 2013 г. N 412-ФЗ «Об аккредитации в национальной системе аккредитации»
5.	Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895)
6.	Указ Президента Российской Федерации от 12 мая 2009 г. № 537 «О стратегии национальной безопасности Российской Федерации до 2020г.»
7.	Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»
8.	Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «Об утверждении Положения о сертификации средств защиты информации»
9.	Постановление Госстандарта РФ от 17 марта 1998 г. N 11 «Об утверждении Положения о Системе сертификации ГОСТ Р»
10.	Постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79 «Об утверждении Положения о лицензировании деятельности по технической защите конфиденциальной информации»
11.	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»
12.	Постановление Правительства Российской Федерации от 21.04.2010г. № 266 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг), и о внесении изменения в положение о сертификации средств защиты информации
13.	Постановление Правительства Российской Федерации от 3 ноября 2014 г. N 1149 г. «Об аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по оценке (подтверждению) соответствия в отношении оборонной продукции (работ, услуг), поставляемой по государственному оборонному заказу, продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерациииной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, а также о внесении изменений в некоторые акты Правительства Российской Федерации в части оценки соответствия указанной продукции (работ, услуг)».
Нормативно-методические документы	
1.	Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации (утверждено приказом председателя Гостехкомиссии России 25 ноября 1994 г.)
2.	Типовое положение об испытательной лаборатории (утверждено приказом председателя Гостехкомиссии России 25 ноября 1994г.)
3.	Положение о сертификации средств защиты информации по требованиям безопасности информации (утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199)
4.	Типовое положение об органе по сертификации средств защиты информации по требованиям безопасности информации (утверждено приказом председателя Гостехкомиссии России 05 января 1996 г., № 3)
5.	Приказ ФСТЭК России от 28 января 2015 г. № 5 «Об утверждении формы аттестата аккредитации»
6.	Приказ ФСТЭК России от 10 апреля 2015г. № 33 «Об утверждении правил выполнения отдельных работ по аккредитации органов по сертификации и испытательных лабораторий, выполняющих работы по оценке (подтверждению) соответствия в отношении продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государ-

	ственную тайну, в установленной ФСТЭК России сфере деятельности»
7.	Приказ ФСТЭК России от 06 декабря 2011г. №638 «Об утверждении требований к системам обнаружения вторжений»
8.	Приказ ФСТЭК России от 20 марта 2012 г. №28 «Об утверждении требований к средствам антивирусной защиты»
9.	Приказ ФСТЭК России от 27 сентября 2013 г. №119 «Об утверждении требований к средствам доверенной загрузки»
10.	Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
11.	Приказ ФСТЭК России от 18 февраля 2013 г.№ 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
12.	Приказ ФСТЭК России от 14 марта 2014 г.№ 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»
13.	РД. Гостехкомиссия России, 2002г. «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий».
14.	РД. Гостехкомиссия России, 1992г. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».
15.	РД. Гостехкомиссия России, 1992г. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».
16.	РД. Гостехкомиссия России, 1992г. «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники».
17.	РД. Гостехкомиссия России, 1997г. «Средства вычислительной техники. Межсетевые экраны.Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».
18.	РД. Гостехкомиссия России, 1999г. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей».
19.	Методические документы. ФСТЭК России, 2014г. «Профили защиты средств контроля съемных машинных носителей информации».
20.	Методические документы. ФСТЭК России, 2014г. «Профили защиты средств доверенной загрузки».
21.	Нормативный документ. ФСТЭК России, 2011г. «Требования к системам обнаружения вторжений»
22.	Нормативный документ. ФСТЭК России,2012г. «Требования к средствам антивирусной защиты».
23.	Методические документы. ФСТЭК России, 2012г. «Профили защиты средств обнаружения вторжений».
24.	Информационное письмо ФСТЭК России, 2012г. «Об утверждении требований к системам обнаружения вторжений».
Национальные стандарты	
1.	ГОСТ Р 51583-2014. «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. Об-

	щие 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 19.301-79 «Программа и методика испытаний. Требования к содержанию и оформлению»
15.	ГОСТ Р ИСО\МЭК 9126-90 «Информационная технология. Оценка программной продукции. Характеристика качества и руководства по их применению»
16.	ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»
17.	ГОСТ Р ИСО/МЭК 27001-2006«Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
18.	ГОСТ Р ИСО/МЭК 18045-2008 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»
19.	ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей»
20.	ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем»
Научно-техническая литература	
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, 2002г.
8.	Скотт Бармен. Разработка правил информационной безопасности, 2002г.
9.	Вильям Столлинг. Основы защиты сетей. Приложения и стандарты, 2002г.
10.	В. Зима, А. Молдовян. Безопасность глобальных сетевых технологий, 2003г.
11.	П. Девянин. Анализ безопасности управления доступом и информационными потоками в компьютерных системах, 2006г.
12.	Н.А. Гайдамакин. Разграничение доступа к информации в компьютерных системах, 2003г.
13.	А.А. Шумский, А.А. Шелупанов. Системный анализ в защите информации, 2005г.
14.	В.Я. Асанович, Т.Г. Маньшин. Информационная безопасность: анализ и прогноз информационного воздействия, 2006г.
15.	Ю.К. Меньшаков. Защита объектов и информации от технических средств разведки, 2002г.
16.	С.А. Петренко, А.А. Петренко. Аудит безопасности INTRANET, 2002г.
17.	А.А. Малюк. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие, 2004г.
18.	А.А. Малюк. Введение в защиту информации в автоматизированных системах, 2005г.
19.	Е.Б. Белов, В.П. Лось. Основы информационной безопасности. Учебное пособие, 2006г.
20.	С.М. Климов. Методы и модели противодействия компьютерным атакам, 2008г.

3.4.3. Программное обеспечение

Пакетпрограмм фирмы Microsoft.

Программные средства защиты информации: SecretNet, DallasLock, Аккорд, Страж и др.

Программа фиксации и контроля исходного состояния «ФИКС 2.0.2».

Программа поиска и гарантированного уничтожения информации на дисках «TERRIER» версия 3.0.

Анализатор исходных текстов программ «АИСТ–С».

Программы моделирования системы разграничения доступа «Ревизор-1 XP», «Ревизор -2 XP»

Программа анализа программного и аппаратного обеспечения TCP/IP сетей (сетевой сканер) «Ревизор Сети» версия 2.0.

Программа сбора информации о программном и аппаратном обеспечении «Агент инвентаризации»

3.4.4. Пакет слушателя

Пакет слушателя (раздаточный материал)включает:

– конспект лекций (презентаций) для слушателя курса по дополнительной профессиональной программе повышения квалификации специалистов в области информационной безопасности: «Организация и проведение работ по оценке (подтверждению) соответствиятребованиям по безопасности информации продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну»;

– приложение к конспекту лекций (презентаций), содержащее справочные и дополнительные материалы по изучаемым темам.

3.5. Порядок передачи программы повышения квалификации другой организации

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

4. ФОРМЫ АТТЕСТАЦИИ

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

Для проведения итоговой аттестации создается аттестационнаякомиссия, 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.

Начальник учебно-методической группы В.И. Крук