



РЕГИОНАЛЬНЫЙ ОБРАЗОВАТЕЛЬНЫЙ ЦЕНТР

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

СОГЛАСОВАНО

Начальник 1 Управления
ФСТЭК России

А. Дротенко

« ____ » _____ 201__ г.

М.П.

УТВЕРЖДАЮ

Директор АНО «РОЦ»

_____ А. Величко

« ____ » _____ 201__ г.

М.П.

**ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
ПОВЫШЕНИЯ КВАЛИФИКАЦИИ СПЕЦИАЛИСТОВ
В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

по теме:

**«ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ
ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ
ПЕРСОНАЛЬНЫХ ДАННЫХ»**

Тюмень
2015

1. ВВЕДЕНИЕ

Дополнительная профессиональная программа повышения квалификации специалистов в области информационной безопасности по теме «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» (далее - программа) разработана с учетом требований Федерального закона от 28.12.2010 № 390-ФЗ «О безопасности», Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Основой для разработки программы являются Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных», Постановление Правительства Российской Федерации от 23.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами», Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России от 11.02.2013 № 17, «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные приказом ФСТЭК России от 18.02.2013 № 21, а также документы, регламентирующие вопросы обеспечения безопасности персональных данных:

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;

При разработке программы выполнены требования Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам, утвержденного приказом Минобрнауки России от 01.07.2013 № 499, Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности, утвержденного приказом Минобрнауки России от 05.12.2013 № 1310.

Цель обучения по программе: освоение специалистами актуальных изменений в вопросах профессиональной деятельности, обновление их теоретических знаний и умений, развитие навыков практических действий по планированию, организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах в условиях существования угроз безопасности информации.

Поставленная цель достигается решением следующих задач:

- изучением нормативных правовых и организационных основ обеспечения безопасности персональных данных в информационных системах персональных данных;
- изучением методов и процедур выявления угроз безопасности персональных данных в информационных системах персональных данных и оценки степени их опасности;
- практической отработкой способов и порядка проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Категория слушателей: специалисты по защите информации органов государственной власти, организаций и учреждений любой формы собственности, осуществляющие разработку и эксплуатацию автоматизированных информационных систем, обеспечивающих обработку, хранение и передачу персональных данных.

Срок обучения: 72 часа аудиторных учебных занятий.

Форма обучения: очная (с отрывом от государственной гражданской службы, работы).

Режим занятий: 36 часов аудиторной учебной и самостоятельной работы под руководством преподавателя в неделю.

В результате изучения курса слушатели должны:

быть ознакомлены:

- с нормативными правовыми и организационными основами защиты информации и обеспечения безопасности персональных данных в Российской Федерации;
- с порядком организации и проведения лицензирования деятельности в области защиты информации;
- с документами национальной системы стандартизации, действующими в области защиты информации;

знать:

- содержание основных нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;
- основные виды угроз безопасности персональных данных в информационных системах персональных данных;
- содержание и порядок организации работ по выявлению угроз безопасности персональных данных;
- процедуры задания и реализации требований по защите информации в информационных системах персональных данных;
- меры обеспечения безопасности персональных данных;
- требования по обеспечению безопасности персональных данных;
- порядок применения организационных мер и технических мер обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;

уметь:

- планировать мероприятия по обеспечению безопасности персональных данных;
- разрабатывать необходимые документы в интересах организации работ по обеспечению безопасности персональных данных;
- обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных;
- проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- определять состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для блокирования угроз безопасности персональных данных;

иметь навык:

определения уровня защиты персональных данных; выявления угроз безопасности персональных данных в информационных системах персональных данных.

4. УЧЕБНЫЙ ПЛАН ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЫ

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Форма контроля
			Лекции	Практические занятия (семинары)	
1	2	3	4	5	6
1	Раздел № 1. Общие вопросы технической защиты информации	22	16	4(2)	
2	Тема №1. Правовые и организационные основы технической защиты информации ограниченного доступа	8	8		
3	Тема № 2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	14	8	4(2)	Опрос на практическом занятии и семинаре
4	Раздел № 2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных	46	36	8(2)	
5	Тема № 3. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных	20	14	4(2)	Опрос на лекции Опрос на практическом занятии и семинаре
6	Тема № 4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	20	20		
7	Тема № 5. Практические реализации типовых моделей защищенных информационных систем обработки	6	2	4	Опрос на практическом занятии

	персональных данных				
8	Итого по видам занятий	68	52	12(4)	
9	Зачет с оценкой	4			4
10	Всего	72	52	12(4)	4

5. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЫ

5.1. Очное обучение

Разделы и темы	1-й день, час.	2-й день, час.	3-й день, час.	4-й день, час.	5-й день, час.	6-й день, час.	7-й день, час.
Раздел № 1. Общие вопросы технической защиты информации							
Тема № 1. Правовые и организационные основы технической защиты информации ограниченного доступа	8						
Тема № 2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	2	10	2				
Раздел № 2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных							
Тема № 3. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных			8	10	2		
Тема № 4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных					8	10	2
Тема № 5. Практические реализации типовых моделей защищенных информационных систем обработки персональных данных							6

Зачет							4
-------	--	--	--	--	--	--	---

5.2. Очно-заочное обучение

Разделы и темы	1-й день, час.	2-й день, час.	3-й день, час.	4-й день, час.	5-й день, час.
Заочная часть – 22 ч.					
Раздел № 1. Общие вопросы технической защиты информации					
Тема № 1. Правовые и организационные основы технической защиты информации ограниченного доступа	6				
Тема № 2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	4	6			
Раздел № 2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных					
Тема № 3. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных		4	10		
Тема № 4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных				10	4
Тема № 5. Практические реализации типовых моделей защищенных информационных систем обработки персональных данных					2
Зачет					4

6. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

6.1. Требования к кадровым условиям реализации дополнительной профессиональной программы:

- преподавательский состав АНО ДПО «РОЦ» должен обладать высшим, либо дополнительным профессиональным образованием в области, соответствующей темам дополнительной профессиональной программы и стажем преподавания по изучаемой тематике не менее 1 года и (или) практической работы в областях знаний, предусмотренных темами дополнительной профессиональной программы, не менее 3 (трех) лет;
- образовательной организацией наряду с традиционными лекционно-семинарскими занятиями должны применяться современные эффективные методики преподавания с применением интерактивных форм обучения, аудиовизуальных средств, информационно-телекоммуникационных ресурсов и наглядных учебных пособий.

6.2. Требования к материально-техническому и учебно-методическому обеспечению дополнительной профессиональной программы:

- АНО ДПО «РОЦ» должна располагать необходимой материально-технической базой, включая аудитории, электронную библиотеку, аудиовизуальные средства обучения, мультимедийную аппаратуру, оргтехнику. Материальная база должна соответствовать санитарным и техническим нормам и правилам и обеспечивать проведение всех видов практической и дисциплинарной подготовки слушателей, предусмотренных учебным планом реализуемой дополнительной профессиональной программы.
- в случае применения электронного обучения, дистанционных образовательных технологий каждый обучающийся в течение всего периода обучения должен быть обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде, содержащей все электронные образовательные ресурсы, необходимые для освоения дополнительной профессиональной программы.

7. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО РЕАЛИЗАЦИИ ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЫ

В процессе изучения данной программы необходимо использовать действующие законодательные акты в области защиты персональных данных в информационных системах обработки персональных данных, технической защиты информации, документы национальной системы стандартизации, организационно-распорядительные и нормативные документы ФСТЭК (Гостехкомиссии) России, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по защите персональных данных в информационных системах обработки персональных данных. Часть лекций может излагаться проблемным методом с привлечением слушателей для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

Теоретические вопросы по тематике курса, наиболее важные в профессиональной деятельности слушателей, выносятся для обсуждения на семинары. При подготовке к семинарам слушателям заранее выдаются вопросы, подготовка к которым требует самостоятельной работы с использованием рекомендованной литературы.

На практические занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл практических занятий по применению программно-аппаратных средств защиты персональных данных при их обработке в информационных системах персональных данных (тема № 2), проводится в компьютерном классе с предварительной установкой необходимого программного обеспечения в компьютерной сети. Цикл практических занятий проводится лектором самостоятельно. При проведении практических занятий необходимо отрабатывать задания, учитывающие специфику выполняемых функциональных обязанностей слушателями курсов по своему профессиональному предназначению, в том числе предусматривать задания с проведением деловых игр (эпизодов).

Практические занятия по обнаружению ТКУИ и отработке методического аппарата технического контроля (Тема № 3) проводятся по циклам на четырёх-шести рабочих местах (количество рабочих мест зависит от количества обучаемых в учебной группе). На каждом рабочем месте должен быть преподаватель, развёрнуто необходимое оборудование технического контроля и средства имитации ТКУИ.

Для проведения практических занятий должны использоваться методические разработки, позволяющие индивидуализировать задания обучаемым в зависимости от их должностных категорий. Такие задания представляют собой проблемные ситуационные варианты, различающиеся моделями информационных систем персональных данных и набором конкретных действий, существенных для определённых категорий обучаемых, объединённых в соответствующую подгруппу.

Самостоятельные занятия проводятся под руководством преподавателя. Для обеспечения занятий используются автоматизированные обучающие системы, электронные учебники, виртуальные автоматизированные системы и компьютерные сети, а также программные средства имитации несанкционированных действий.

В качестве формы итогового контроля полученных знаний выбран зачет с оценкой, в процессе проведения которого применяются методы тестирования с использованием компьютерных технологий.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Для проведения итоговой аттестации используются тестовые материалы, разрабатываемые педагогическим работником и утверждаемые руководителем образовательной организации.

Пример тестовых материалов:

1	Угрозы какого типа актуальны для ИС, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе?	
	а	1-го
	б	2-го
	в	3-го
	г	4-го

Тест состоит из 40 вопросов (10 вопросов повышенной сложности). Тест включает в себя вопросы, направленные как на контроль знаний, так и на проверку полученных навыков работы.

Оценка за каждый простой вопрос – 1 балл. Оценка за каждый вопрос повышенной сложности – 2 балла.

Общее количество набранных баллов	Уровень знаний
21 - 50 баллов	зачтено
0 – 20 баллов	не зачтено