Вх. 9465

Автономная некоммерческая организация
дополнительного профессионального образования
«Учебный центр «Информзащита»

СОГЛАСОВАНО

Начальник 1 управления
ФСТЭК России

_____ / Мартинец Н.М. /
(подпись)

«25» сентября 2018 г.

М.П.

УТВЕРЖДАЮ

Директор
АНО ДПО «Учебный центр
«Информзащита»

_____ / Степаненко А.А. /
(подпись)

«23» 09 2018 г.

М.П.

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

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

Код: ПК123

Москва, 2018

1. Общие положения

Настоящая программа повышения квалификации «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Программа повышения квалификации, Программа) разработана с учетом требований: Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», Федерального закона от 28 декабря 2010 г. № 390-ФЗ «О безопасности», Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», приказа Министерства образования и науки Российской Федерации от 5 декабря 2013 г. № 1310 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну», «Методических рекомендаций по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации», утвержденных ФСТЭК России 4 апреля 2015 г. и примерной программы повышения квалификации, разработанной Минтруда России (письмо Минтруда России № 18-3/10/1-4091 от 9 сентября 2013 г.).

Основой для разработки программы являются: Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», «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 февраля 2013 г. № 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».

Программа повышения квалификации реализуется в АНО ДПО «Учебный центр «Информзащита».

Программа разработана в инициативном порядке на основании Приказа Директора АНО ДПО «Учебный центр «Информзащита» от 05 февраля 2018 г. №02/02/18.

Разработчики Программы:

- Ершов Дмитрий Вячеславович, к.т.н., заместитель директора по учебно-методической работе;

- Журавлев Владимир Владимирович, заведующий кафедрой юридических проблем защиты конфиденциальной информации.

Программа обсуждена и одобрена на заседании Методического совета АНО ДПО «Учебный центр «Информзащита» и утверждена Директором Учебного центра 23 марта 2018 г.

2. Цель реализации Программы повышения квалификации

Целью обучения по Программе является 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 персональных данных 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.

3. Требования к квалификации поступающего на обучение

К освоению программы допускаются:

лица, имеющие высшее образование по направлению подготовки (специальности) в области информационной безопасности, или прошедшие профессиональную переподготовку для выполнения нового вида профессиональной деятельности в области информационной безопасности, или имеющие иное высшее образование, подтвержденное документом об образовании, и стаж работы в области защиты информации не менее одного года.

4. Планируемые результаты обучения

Процесс освоения слушателями Программы повышения квалификации направлен на совершенствование и (или) получение следующих компетенций:

- способность организовывать и проводить работы по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

- способность проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- способность определять уровни защиты персональных данных;
- способность обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных;
- способность определять состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для блокировки угроз безопасности персональных данных.

В результате изучения курса слушатели должны:
быть ознакомлены:

- с нормативными правовыми и организационными основами 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 блокировки угроз безопасности персональных данных.

владеть навыками:

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

5. Условия реализации Программы

Теоретическое и практическое обучение слушателей рекомендуется осуществлять в аудиториях, компьютерных классах, оборудованных автоматизированными рабочими местами для занятий по учебным дисциплинам из расчета одно рабочее место на одного обучающегося.

Компьютерные классы оснащены комплектом лицензионного программного обеспечения и средств защиты информации.

Формирование профессиональных компетенций обеспечивается широким использованием в учебном процессе активных и интерактивных форм проведения занятий (деловых и ролевых игр, разбора конкретных ситуаций) с целью формирования и развития профессиональных навыков обучающихся.

В рамках Программы повышения квалификации проведение практических занятий осуществляется специалистами высшего уровня квалификации в области защиты персональных данных, имеющими практический опыт работы в российских компаниях и государственных организациях.

Каждому обучающемуся обеспечивается доступ к библиотечному фонду, укомплектованному печатными и электронными изданиями основной учебной литературы, из расчета не менее одного экземпляра на одного обучающегося.

Для обучающихся обеспечен доступ к современным профессиональным базам данных, информационным справочным и поисковым системам по тематике информационной безопасности.

Программа повышения квалификации реализуется в АНО ДПО «Учебный центр «Информзащита». Передача Программы другим образовательным организациям не предусматривается.

Изменения и дополнения вносятся в Программу по мере необходимости в целях ее актуализации в случае изменений законодательной базы и осуществляются по распоряжению директора АНО ДПО «Учебный центр

«Информзащита».

6. Формы аттестации и оценочные материалы

Форма обязательной итоговой аттестации обучающихся, освоивших Программу повышения квалификации, определяется в зависимости от категории обучающихся:

- итоговый зачёт в форме тестирования.

Перечень тестов, используемых для проведения экзамена, формируется на основе перечней тестов, выносимых для контроля знаний обучающихся при проведении промежуточных аттестаций по учебным модулям, представленным в рабочей программе курса повышения квалификации.

Для проведения итоговой аттестации создается аттестационная комиссия, состав которой утверждается директором АНО ДПО «Учебный центр «Информзащита».

Обучающимся, успешно освоившим Программу повышения квалификации и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации установленного образца.

7. УЧЕБНЫЙ ПЛАН ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

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

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

7.3. Продолжительность обучения: 72 часа.

7.4. Режим занятий: 8 часов учебных занятий в день.

7.5. План учебного процесса

№ п/п	Наименование учебных модулей, разделов (тем)	Всего учебных часов	В том числе		Формы аттестации и контроля знаний
			Лекции	Практические занятия (семинары)	
1	2	3	4	5	6
1.	**Раздел № 1. Общие вопросы технической защиты информации**	**22**	**16**	**4(2)**	–
1.1.	**Тема** № 1. Правовые и организационные основы технической защиты информации ограниченного доступа	8	8	–	Опрос на лекции.
1.2.	**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.
2.	**Раздел № 2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных**	**46**	36	**8(2)**	–
2.1.	**Тема** № 3. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных,	20	14	4(2)	Опрос на лекции. Опрос на практическом занятии и семинаре

1	2	3	4	5	6
	организационные и технические меры защиты информации в информационных системах персональных данных				
2.2.	**Тема № 4.** Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	20	20		Опрос на лекции.
2.3.	**Тема № 5.** Практические реализации типовых моделей защищенных информационных систем обработки персональных данных	6	2	4	Опрос на практическом занятии
	Итоговая аттестация	**4**	**–**	**–**	**Зачет**
	Всего	**72**	**52**	**12(4)**	**4**

7.6. Сводные данные по бюджету времени

Общий объем времени, отводимого на освоение программы (календарных дней/часов)			Распределение учебного времени (количество часов)					
Всего	Из них		Всего часов учебных занятий	В том числе		Время на самостоя-тельную работу	Итоговая аттестация	Резерв учебного времени
	Выходные, праздничные дни	Учебное время		Учебные занятия по расписанию	Практики			
11	2	72	72	68	–	–	4	

8. Календарный учебный график

Срок обучения по программе повышения квалификации (недели)	1					2			
Срок обучения по программе повышения квалификации (дни)	1	2	3	4	5	6	7	8	9
Виды занятий, предусмотренные программой повышения квалификации	А	А	А	А	А	А	А	А	А,И

А— аудиторские занятия
И— итоговая аттестация

9. Рабочая программа учебного курса

9.1. Содержание учебных модулей, разделов (тем)

Раздел № 1. Общие вопросы технической защиты информации

Тема № 1. Правовые и организационные основы технической защиты информации ограниченного доступа

- Основные понятия в области технической защиты информации (ТЗИ). Стратегия национальной безопасности Российской Федерации до 2020 года. Доктрина информационной безопасности Российской Федерации. Концептуальные основы ТЗИ. Законодательные и иные правовые акты, регулирующие вопросы ТЗИ. Система документов по ТЗИ и краткая характеристика ее основных составляющих.
- Структура и направления деятельности системы ТЗИ в субъектах Российской Федерации. Система органов по ТЗИ в Российской Федерации, их задачи, распределение полномочий по обеспечению ТЗИ. Задачи, полномочия и права Федеральной службы по техническому и экспортному контролю (ФСТЭК России). Задачи, полномочия и права управлений ФСТЭК России по федеральным округам.
- Лицензирование деятельности в области технической защиты информации. Сертификация средств защиты информации, аттестация объектов информатизации по требованиям безопасности информации. Документы национальной системы стандартизации в области ТЗИ.
- Основные документы, определяющие направления и порядок организации деятельности, организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.
- Права субъектов персональных данных. Способы защиты прав субъектов персональных данных.

Тема № 2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа

- Понятия «безопасности информации», «угрозы безопасности информации», «уязвимости», «источника угрозы». Целостность, конфиденциальность и доступность информации. Классификационная схема угроз безопасности информации и их общая характеристика. Особенности проведения комплексного исследования объектов информатизации на наличие угроз безопасности информации. Методы оценки опасности угроз.
- Классификация объектов информатизации. Методические рекомендации по классификации и категорированию объектов информатизации.

Характеристика основных угроз несанкционированного доступа и моделей нарушителя безопасности информации, а также способов реализации этих угроз. Характеристика основных классов атак, реализуемых в сетях общего пользования, функционирующих с использованием стека протоколов TCP/IP. Понятие программно-математического воздействия и вредоносной программы. Классификация вредоносных программ, основных деструктивных функций вредоносных программ и способов их реализации. Особенности программно-математического воздействия в сетях общего пользования. Методы и средства выявления угроз несанкционированного доступа к информации и специальных воздействий на неё. Порядок обеспечения защиты информации при эксплуатации автоматизированных систем.

- Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ. Защита информации в локальных вычислительных сетях. Защита информации при межсетевом взаимодействии. Защита информации при работе с системами управления базами данных. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.
- Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники.
- Содержание и порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Структура, содержание и порядок подготовки документов при аттестации объектов информатизации по требованиям безопасности информации.

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

- Особенности информационного элемента информационной системы персональных данных.
- Основные типы актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, порядок их определения. Угрозы несанкционированного доступа к информации в информационных системах персональных данных. Угрозы утечки информации по техническим каналам.
- Основные принципы обеспечения безопасности персональных данных при их обработке: законности, превентивности, адекватности, непрерывности, адаптивности, самозащиты, многоуровневости, персональной ответственности и минимизации привилегий, разделения полномочий и их

характеристика. Основные направления деятельности по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных. Оценка достаточности и обоснованности запланированных мероприятий.

- Особенности обеспечения безопасности персональных данных, обрабатываемых на автоматизированных рабочих местах с использованием автономных ПЭВМ, в локальных вычислительных сетях и при межсетевом взаимодействии.
- Рекомендации по применению мер и средств обеспечения безопасности персональных данных от физического доступа.
- Причины и физические явления, порождающие технические каналы утечки информации (ТКУИ) при эксплуатации объектов информатизации. Классификация ТКУИ.
- Основные требования и рекомендации по защите речевой информации, циркулирующей в защищаемых помещениях.
- Оценка защищённости информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации.

Тема № 4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

- Определение необходимых уровней защищенности персональных данных при их обработке в информационных системах в зависимости от типа актуальных угроз для информационных систем, вида и объема обрабатываемых в них персональных данных.
- Состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий.
- Порядок выбора мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных: определение базового набора мер, адаптация базового набора, уточнение адаптированного базового набора мер, дополнение уточненного адаптированного базового набора мер.
- Содержание мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных.

- Требования к средствам защиты информации для обеспечения различных уровней защищенности персональных данных.
- Организация обеспечения безопасности персональных данных в организациях и учреждениях. Перечень основных этапов при организации работ по обеспечению безопасности персональных данных.
- Мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных и особенности их реализации.
- Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов ненормативного характера по обработке персональных данных и обеспечению безопасности персональных данных. Подготовка уведомлений об обработке персональных данных в уполномоченный орган, порядок внесения изменений в ранее представленное в уполномоченный орган уведомление.
- Обязанности оператора, осуществляющего обработку персональных данных. Порядок и условия обработки персональных данных без средств автоматизации. Порядок и методы обезличивания персональных данных, их деобезличивание. Особенности обработки персональных данных в условиях государственной гражданской службы и муниципальной службы. Ответственность за нарушение требований законодательства Российской Федерации в области персональных данных.

Тема № 5. Практические реализации типовых моделей защищённых информационных систем обработки персональных данных

- Комплекс организационных и технических мероприятий (применения технических средств), в рамках подсистемы защиты персональных данных, развертываемой в информационной системе персональных данных в процессе ее создания или модернизации. Основное содержание этапов организации обеспечения безопасности персональных данных.
- Варианты реализации мероприятий по защите персональных данных и типовые модели защищенных информационных систем персональных данных с использованием существующих сертифицированных средств защиты информации.
- Виды, формы и способы контроля защиты персональных данных в информационных системах персональных данных. Планирование работ по контролю состояния защиты персональных данных в информационных системах персональных данных. Основные вопросы, подлежащие проверке (анализу) при контроле состояния организации защиты персональных данных.

9.2. Лабораторный практикум

В процессе изучения рабочей программы учебного курса лабораторный практикум не предусмотрен.

9.3. Практические занятия (семинары)

9.3.1. Семинары

№ п/п	Номер (наименование) учебного модуля, темы	Тематика семинаров	Количество времени, отводимого на проведение семинара (час.)
1.	Раздел № 1, Тема № 2	• Характеристика основных угроз несанкционированного доступа и моделей нарушителя безопасности информации, а также способов реализации этих угроз.	2
2.	Раздел № 2, 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.	2

9.3.2. Практические занятия

№ п/п	Номер (наименование) учебного модуля, темы	Тематика практических занятий	Количество времени, отводимого на проведение практических занятий (час.)
1.	Раздел № 1, Тема № 2	• Выявление угроз безопасности информации на объектах информатизации • Классификация объектов информатизации	4
2.	Раздел № 2, Тема № 3	• Разработка плана по организации обеспечения безопасности персональных данных в информационных системах персональных данных. • Оценка достаточности и обоснованности запланированных мероприятий.	4
3.	Раздел № 2, Тема № 5	• Практические реализации типовых моделей защищённых информационных систем обработки персональных данных. • Варианты реализации мероприятий по защите персональных данных и типовые модели защищенных информационных систем персональных данных с использованием существующих сертифицированных средств защиты информации. • Планирование работ по контролю состояния защиты персональных данных в информационных системах персональных данных.	4

9.4. Учебно-методическое и информационное обеспечение учебного курса

а) основная литература:

1. Аверченков В.И., Организационная защита информации: 3 издание: учебн. пособие/ В.И. Аверченков, М.Ю. Рытов.- Москва: Издательство «Флита», 2011.-184с.
2. Технические средства и методы защиты информации; Учебное пособие для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков; под ред. А.П. Зайцева и А.А. Шелупанова. - 7-е изд. испр. - М.: Горячая линия - Телеком, 2012.
3. Безопасность информационных технологий. Руководство слушателя курса БТ01. – М.: УЦ Информзащита, 2018. – 349 с.
4. Безопасность компьютерных сетей. Руководство слушателя курса БТ03.- М.: УЦ Информзащита, 2018. – 436 с.
5. Основы TCP/IP. Руководство слушателя курса БТ05. – М.: УЦ Информзащита, 2013. – 130 с.
6. Безопасность ОС Windows 7/8.1/10/2012 R2. Руководство слушателя курса БТ30. – М.: УЦ Информзащита, 2016. – 752 с.
7. Порядок применения системы защиты Secret Net 7.0 (автономный вариант). Руководство слушателя курса К005.- М.: Код Безопаснсоти, 2017.–138 с.
8. Контроль защищенности информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок. Аттестационные испытания по требованиям безопасности информации: Учебное пособие / А.А. Голяков, В.С. Горбатов, А.П. Дураковский, А.Е. Панин, М.С. Чистяков; под общ. ред. ЮЛ. Лаврухина - М: НИЯУ МИФИ, 2014.
9. Запечников С.В. Информационная безопасность открытых систем. Часть 1: Учебник для вузов / Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. – М.: Горячая линия – Телеком, 2006, - 686 с.
10. Реализация режима коммерческой тайны на предприятии. Руководство слушателя курса КП30. – М.: УЦ Информзащита, 2015. – 82 с.
11. Организация конфиденциального делопроизводства. Руководство слушателя курса КП31. – М.: УЦ Информзащита, 2014. – 226 с.

б) Законодательство

1. «Конституция Российской Федерации», принята всенародным голосованием 12 декабря 1993г.
2. «О Декларации прав и свобод человека и гражданина», Постановление Верховного Совета РСФСР от 22.11.1991 № 1920-1.
3. «Доктрина информационной безопасности Российской Федерации»,

утверждена Президентом РФ 5 декабря 2016г. №646.

4. Регламент ЕС 2016/679 от 27 апреля 2016 г. или GDPR — General Data Protection Regulation http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC

Кодексы:

5. «Уголовный кодекс Российской Федерации», принят Федеральным законом от 13 июня 1996г. № 63-ФЗ.
6. «Кодекс Российской Федерации об административных правонарушениях», принят Федеральным законом от 30 декабря 2001г. №195-ФЗ.
7. «Трудовой кодекс Российской Федерации», принят Федеральным законом от 30 декабря 2001 г. № 197-ФЗ.

Федеральные законы:

8. Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
9. Федеральный Закон от 19 декабря 2005г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
10. Федеральный Закон от 27 июля 2006г. № 152-ФЗ «О персональных данных».
11. Федеральный Закон от 29 июля 2004г. № 98-ФЗ «О коммерческой тайне».
12. Федеральный закон от 4 мая 2011г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
13. Федеральный закон от 6 апреля 2011г. № 63-ФЗ «Об электронной подписи».
14. Федеральный закон от 27 декабря 2002г. № 184-ФЗ «О техническом регулировании».
15. Федеральный закон от 28 декабря 2010г. № 390-ФЗ «О безопасности».
16. Федеральный закон от 3 апреля 1995г. № 40-ФЗ «О Федеральной службе безопасности».

Указы Президента Российской Федерации:

17. Указ Президента Российской Федерации от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года».
18. Указ Президента Российской Федерации от 6 марта 1997г. № 188 «Об утверждении перечня сведений конфиденциального характера».
19. Указ Президента Российской Федерации от 30 мая 2005г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного

дела».

20. Указ Президента Российской Федерации от 17 марта 2008г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

Постановления Правительства Российской Федерации:

21. Постановление Правительства Российской Федерации от 16 марта 2009г. №228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».
22. Постановление Правительства Российской Федерации от 15 сентября 2008г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
23. Постановление Правительства Российской Федерации от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
24. Постановление Правительства Российской Федерации от 6 июля 2008г. №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
25. Постановление Правительства Российской Федерации от 4 марта 2010г. №125 «О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию».
26. Постановление Правительства Российской Федерации от 16 апреля 2012г. №313 «Об утверждении Положения о лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или

индивидуального предпринимателя)».

27. Постановление Правительства Российской Федерации от 3 марта 2012г. №171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации».
28. Постановление Правительства Российской Федерации от 3 февраля 2012г. №79 «О лицензировании деятельности по технической защите конфиденциальной информации».
29. Постановление Совета Министров – Правительства Российской Федерации от 15 сентября 1993г. №912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» (Извлечения).
30. Постановление Правительства Российской Федерации от 21 марта 2012г. №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 или муниципальными органами».

Нормативные документы ФСТЭК России:

31. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 14 февраля 2008г.
32. «Меры защиты информации в государственных информационных системах», методический документ, утвержден ФСТЭК России 11 февраля 2013г.
33. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)», утверждена Заместителем директора ФСТЭК России 15 февраля 2008г.
34. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказ ФСТЭК России от 18 февраля 2013г. № 21.
35. «Методические рекомендации по технической защите информации, составляющей коммерческую тайну», утверждены Заместителем директора ФСТЭК России 25 декабря 2006г.
36. «Положение о сертификации средств защиты информации по требованиям безопасности информации», утверждено приказом председателя Государственной технической комиссии при Президенте Российской

Федерации от 27 октября 1995г. № 199.

37. «Положение по аттестации объектов информатизации по требованиям безопасности информации», утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.
38. «Методические рекомендации управлениям ФСТЭК России по федеральным округам об организации работ по аттестации объектов информатизации по требованиям безопасности информации», утверждены заместителем директора ФСТЭК России 25 апреля 2006г.
39. «Сборник временных методик оценки защищённости конфиденциальной информации, обрабатываемой техническими средствами и системами», утверждены приказом председателя Государственной технической комиссии при Президенте Российской Федерации, 2001г.
40. «Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения», утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.
41. «Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.
42. «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.
43. «Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.
44. «Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники», утвержден решением председателя Гостехкомиссии России от 30 марта 1992г.
45. «Руководящий документ. Требования к межсетевым экранам. Приказ ФСТЭК России от 9 февраля 2016 г. № 9 (зарегистрирован Минюстом России 25 марта 2016 г., регистрационный № 41564).
46. «Руководство по разработке профилей защиты и заданий по безопасности», Гостехкомиссия России, 2003г.

47. «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры», утверждены заместителем директора ФСТЭК России 19 ноября 2007г.

Нормативные документы ФСБ России:

48. Приказ ФСБ от 10 июля 2014 г. №378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
49. «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные руководством 8 Центра ФСБ России (№ 149/7/2/6-432 от 31.03.2015).
50. Приказ ФСБ России от 9 февраля 2005г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».
51. Приказ ФАПСИ России от 13 июня 2001г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащих сведений, составляющих государственную тайну», зарегистрирован в Министерстве юстиции Российской Федерации 6 августа 2001 г. № 2848.

Стандарты:

52. ГОСТ Р 51275-06. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения», принят и введен в действие Постановлением Госстандарта Российской Федерации от 1 февраля 2008г.
53. ГОСТ Р 50739-95. «Средства вычислительной техники. Защита от НСД к информации. Общие технические требования»
54. ГОСТ Р ИСО/МЭК 15408-1-2002. «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель». Госстандарт России.
55. ГОСТ Р ИСО/МЭК 15408-2-2002. «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности». Госстандарт России.

56. ГОСТ Р ИСО/МЭК 15408-3-2002. «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности». Госстандарт России.
57. ГОСТ Р 50922-06. «Защита информации. Основные термины и определения».
58. ГОСТ Р ИСО/МЭК 27002. «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».
59. ГОСТ Р ИСО/МЭК 27002 2012 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»
60. ГОСТ Р ИСО/МЭК 27003 2012 «Информационные технологии. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности».

в) базы данных, информационно-справочные и поисковые системы:

1. https://bdu.fstec.ru/threat База данных угроз безопасности информации на сайте ФСТЭК России;
2. Официальный портал персональных данных (Роскомнадзор) http://rkn.gov.ru/personal-data/portal
3. Список уязвимостей https://www.cvedetails.com/vulnerabilities-by-types.php

9.5. Материально-техническое обеспечение учебного курса

Наименование специализированных аудиторий, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
Специализированный учебный класс	Лекции	Автоматизированное рабочее место преподавателя в составе: ПЭВМ. Принтер. Проектор LCD. Экран. Операционная система Windows 7 Корпоративная. Офисные программы Microsoft Office 2007, Adobe Acrobat Reader. Антивирусные программы KasperskyInternet Security 10
Специализированный компьютерный класс	Семинары и практические занятия	Автоматизированное рабочее место преподавателя в составе: ПЭВМ. Принтер. Проектор LCD. Экран. Автоматизированное рабочее место обучающегося (в расчете - одно рабочее место на одного обучающегося) в составе: ПЭВМ.

Наименование специализированных аудиторий, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
		Операционная система. Офисные программы. Программное обеспечение для проведения компьютерных тестов. Средства защиты информации: • Средство защиты информации от НСД «Secret Net» версии 7.6 (ООО «Код Безопасности»); • Программно-аппаратный комплекс доверенной нагрузки ПАК «Соболь» версии 3.0 (ООО «Код Безопасности»); • Антивирусный пакет «Kaspersky Endpoint Security для бизнеса - Расширенный», «Антивирус Касперского для Всех устройств» (ООО «Лаборатория Касперского»); • Межсетевой экран типа В «Secret Net Studio» версии 8.1 (ООО «Код Безопасности»); • Межсетевой экран типа А,Б АПКШ «Континент» версии 3.7 (ООО «Код Безопасности»); • Средство защиты информации в среде виртуализации «vGate» версии 7.6 (ООО «Код Безопасности»).

9.6. Методические рекомендации по организации учебногокурса

В процессе изучения 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 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.

Для проведения практических занятий необходимо использовать 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, объединенных в соответствующую подгруппу.

С целью текущего контроля знаний в ходе практических занятий должны проводиться выборочные опросы и (или) использоваться различные приёмы тестирования.

9.7. Примерные вопросы контроля знаний

1. Основные документы, определяющие направления и порядок организации деятельности, организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.
2. Права субъектов персональных данных.
3. Способы защиты прав субъектов персональных данных.
4. Понятия «угрозы безопасности информации», «уязвимости», «источника угрозы».
5. Методы оценки опасности угроз.
6. Методы и средства выявления угроз несанкционированного доступа к информации и специальных воздействий на неё.
7. Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ.
8. Защита информации в локальных вычислительных сетях.
9. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.
10. Защита информации при работе с системами управления базами данных.
11. Меры и средства обеспечения безопасности персональных данных от физического доступа.
12. Определение необходимых уровней защищенности персональных данных при их обработке в информационных системах.
13. Порядок выбора мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных: определение базового набора мер, адаптация базового набора, уточнение адаптированного базового набора мер, дополнение уточненного адаптированного базового набора мер.
14. Требования к средствам защиты информации для обеспечения различных уровней защищенности персональных данных.
15. Перечень основных этапов при организации работ по обеспечению безопасности персональных данных.
16. Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов ненормативного характера по обработке персональных данных и обеспечению безопасности персональных данных.
17. Подготовка уведомлений об обработке персональных данных в уполномоченный орган, порядок внесения изменений в ранее представленное в уполномоченный орган уведомление.
18. Порядок и условия обработки персональных данных без средств автоматизации.
19. Ответственность за нарушение требований законодательства Российской Федерации в области персональных данных.