Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Тамбовский государственный университет имени Г.Р. Державина»

Институт дополнительного образования

«Утверждаю»
Ректор Тамбовского
государственного университета
имени Г.Р. Державина

_____ В.Ю. Стромов
«___» _____ 2018 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Вид профессиональной деятельности: обеспечение безопасности информации и защита информации

Наименование программы: «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»

Документ о квалификации: удостоверение о повышении квалификации установленного образца

Объем: 72 часа

Тамбов – 2018

Составитель программы: Зауголков Игорь Алексеевич, к. т. н., доцент, доцент кафедры «Математического моделирования и информационных технологий»

Эксперт: В.Н. Шамкин, д.т.н., профессор кафедры «Конструирование радиоэлектронных и микропроцессорных систем» Федерального государственного бюджетного образовательного учреждения высшего образования «Тамбовский государственный технический университет»

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Нормативные правовые основания разработки программы

Нормативную правовую основу разработки программы составляют:

1. Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»
2. Постановление Правительства Российской Федерации от 22 января 2013 г. № 23 «О Правилах разработки, утверждения и применения профессиональных стандартов»
3. Приказ Минтруда России от 12 апреля 2013 г. № 148н «Об утверждении уровней квалификаций в целях разработки проектов профессиональных стандартов»
4. Приказ Минобрнауки России от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»

Программа разработана с учетом профессионального стандарта «Безопасность информационных технологий в правоохранительной сфере».

1.2. Требования к слушателям: программа реализуется на базе высшего образования (уровень квалификации – бакалавриат, магистратура, специалитет).

1.3. Формы освоения программы: очная

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

Программа направлена на совершенствование следующих профессиональных компетенций по виду профессиональной деятельности:

Эксплуатационная деятельность:

установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов технических систем обеспечения безопасности информации;

участие в проведении специальных проверок и исследований, аттестации объектов, помещений, технических средств, систем, сертификационных испытаний программных средств на предмет соответствия требованиям защиты информации;

администрирование подсистем обеспечения информационной безопасности на объекте.

Организационно-управленческая деятельность:

разработка и контроль эффективности осуществления системы мер по формированию и использованию информационных ресурсов, систем обеспечения информационной безопасности.

Программа направлена на совершенствование следующих общепрофессиональных компетенций (ПК):

ПК-1 способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз;

ПК-3 способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации.

ПК-17 Способность организовывать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов

Виды деятельности или трудовая функция (по ПС)	Профессиональные компетенции	Практический опыт	Умения	Знания
1	2	3	4	5
	ПК-1 способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз;	Навыки формальной постановки и решения задач защиты информации	анализировать меры по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну	Основные тенденции создания комплекса мер по обеспечению безопасности информации
	ПК-3 способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации	Навыки в эксплуатации подсистем ИБ, разработки практических рекомендаций и реализацией их в системе информационной безопасности или ее элементах	администрировать подсистемы ИБ, определять рациональные меры защиты на объектах и оценивать их эффективность	Основные цели, задачи, методы по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, анализа эффективности системы защиты информации
	ПК-17 способность организовывать подготовку и представлять объект	Практический опыт участия в подготовке необходимых материалов для	выполнять подготовку к проведению сертификации средств защиты	Сетевые технологии и вопросы организации защиты автоматизированных систем и их

	информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов	получения лицензий на деятельность по защите информации	информации	компонентов от несанкционированного доступа

1.5. Трудоемкость программы: 72 часа

II. УЧЕБНЫЙ ПЛАН

№ п/п	Наименование учебных тем	Формы промежуточной аттестации	Обязательные учебные занятия		Самостоятельная работа обучающегося		Всего (час.)
			Всего (час.)	в т. ч. лабораторные и практические занятия (час.)	Всего (час.)	в т. ч. консультаций при выполнении самостоятельной работы (час.)	
1	2	3	4	5	6	7	8
1.	Правовые и организационные вопросы технической защиты информации ограниченного доступа	Отсут.	8				**8**
2.	Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	Опрос на практич. занятии и семинаре	20	10			**20**
3.	Организационные меры и технические средства защиты информации от утечки по техническим каналам на объектах информатизации.	Опрос на практич. занятии и семинаре	**16**	8	**2**		**18**
4.	Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных	Опрос на лекции	**4**	0			**4**
5.	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	Отсут.	**2**				**2**
6.	Практические реализации типовых моделей защищенных информационных систем обработки персональных данных	Опрос на практич. занятии	**14**	12	**2**		**16**
Итоговая аттестация			**4**	0	**0**	0	**4**
Всего по программе:			**68**	30	**4**		**72**

III. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Наименование учебного модуля, темы	Объем нагрузки, часов	Учебные недели											
		1				2				3			
		1 день	2 день	3 день	4 день	5 день	6 день	7 день	8 день	9 день	10 день	11 день	12 день
Правовые и организационные вопросы технической защиты информации ограниченного доступа.	**8**	2	6										
Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	**20**	4	4	4	4	4							
Организационные меры и технические средства защиты информации от утечки по техническим каналам на объектах информатизации.	**18**						4	4	4	4			

Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных.	**4**								2	2			
Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.	**2**										2		
Практические реализации типовых моделей защищенных информационных систем обработки персональных данных	**16**										4	6	6
Итоговая аттестация	**4**												4

IV. СОДЕРЖАНИЕ ПРОГРАММЫ

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся		Объем часов
1	2		3
Тема 1. Правовые и организационные вопросы технической защиты информации ограниченного доступа.	**Содержание учебного материала**	**Уровень освоения**	*8*
	1 Основные понятия в области технической защиты информации	ознакомительный	
	2 Организационная структура и компетенция ветвей государственной власти, виды обеспечения информационной безопасности	ознакомительный	
	Информационные (лекционные) занятия		*8*
	Основное содержание нормативных правовых актов и документов по защите конфиденциальной информации. Общие положения, термины и определения, организация и проведение работ по защите персональных данных при их обработке техническими средствами		
Тема 2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	**Содержание учебного материала**	**Уровень освоения**	*20*
	1 Понятие «безопасности информации», «угрозы безопасности информации», «уязвимости», «источника угрозы».	продуктивный	
	2 Классификация объектов информатизации. Методические рекомендации по классификации и категорированию объектов информатизации.	продуктивный	
	Информационные (лекционные) занятия		*10*
	Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники		
Тема 3. Организационные меры и технические средства защиты информации от утечки по техническим	**Содержание учебного материала**	**Уровень освоения**	*18*
	1 Актуальность проблемы, основные термины и определения, классификация и общая характеристика технических каналов утечки информации	продуктивный	
	2 Методы и средства выявления ТКУИ на типовом объекте информатизации.	продуктивный	
	Информационные (лекционные) занятия		*8*
	Оценка защищенности информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации		

каналам на объектах информатизации.	**Самостоятельная работа обучающихся**			*2*
Тема 4. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных.	**Содержание учебного материала**		**Уровень освоения**	*4*
	1	Особенности информационного элемента информационных систем персональных данных	продуктивный	
	2	Особенности обеспечения безопасности персональных данных, обрабатываемых на автоматизированных рабочих местах на базе автономных ПЭВМ, в локальных вычислительных сетях и при межсетевом взаимодействии	продуктивный	
	Информационные (лекционные) занятия			*4*
	Организация обеспечения безопасности персональных данных в информационных системах персональных данных			
Тема 5. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.	**Содержание учебного материала**		**Уровень освоения**	*2*
	1	Классификация информационных систем персональных данных.	продуктивный	
	2	Описание пакетов обязательных требований по обеспечению безопасности для информационных систем персональных данных.	продуктивный	
	Информационные (лекционные) занятия			*2*
	Мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных и особенности их реализации			
Тема 6. Практические реализации типовых моделей защищенных информационных систем обработки персональных данных	**Содержание учебного материала**		**Уровень освоения**	*16*
	1	Комплекс организационных и технических мероприятий (применения технических средств), в рамках подсистемы защиты персональных данных, развертываемой в в процессе ее создания или модернизации.	продуктивный	
	2	Варианты реализации мероприятий по защите персональных данных и типовые модели защищенных информационных систем персональных данных с использованием существующих сертифицированных средств защиты информации	продуктивный	
	Информационные (лекционные) занятия			*2*
	Виды, формы и способы контроля защиты персональных данных в информационных системах персональных данных.			
	Самостоятельная работа обучающихся			*2*

Всего:	*68*

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

V. ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ

5.1. Формы аттестации

Промежуточная аттестация по конкретным темам осуществляется в форме опроса. Итоговая аттестация осуществляется в форме зачета. Итоговый зачет проводится в виде собеседования со слушателем.

Состав комиссии состоит не менее чем из трех членов, включая председателя комиссии. Процедура итоговой аттестации осуществляет в присутствии только членов аттестационной комиссии и слушателя.

Оценка по результатам собеседования формируется коллегиально аттестационной комиссией. В случае удовлетворительного ответа слушателя на все поставленные вопросы выставляется оценка «зачтено». Оценка «незачтено» выставляется в случае, если слушатель не показывает достаточных знаний по темам программы.

5.2. Оценочные средства

Основные показатели оценки планируемых результатов

Результаты обучения (освоенные умения, усвоенные знания)	Основные показатели оценки результата
ПК-1 способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз;	Умение осуществить подбор комплекса мер по защите информации на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз
ПК-3 способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации	Умение корректно провести мероприятия по контролю за обеспечением защиты информации, в том числе сведений, составляющих государственную тайну, проводить анализ эффективности системы защиты информации
ПК-17 Способность организовывать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов	Умение организовывать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов

Перечень оценочных средств для проведения собеседования в рамках итоговой аттестации:

1. Организационная структура и компетенция ветвей государственной власти, виды обеспечения информационной безопасности.
2. Структура, функции и задачи структурных подразделений государственной системы защиты информации в Российской Федерации от технических разведок (ТР) и утечки по техническим каналам, задачи и функции Федеральной службы по техническому и экспортному контролю (ФСТЭК России).
3. Стратегия национальной безопасности Российской Федерации до 20202г. Доктрина информационной безопасности Российской Федерации.

4. Основное содержание нормативных правовых актов и документов по защите конфиденциальной информации.
5. Общие положения, термины и определения, организация и проведение работ по защите персональных данных при их обработке техническими средствами.
6. Особенности государственного регулирования деятельности в области технической защиты информации на предприятиях, в организациях и учреждениях различных форм собственности, правовые основы обеспечения обработки и хранения персональных данных в информационных системах, классификация персональных данных и информационных систем для их обработки.
7. Основные требования к информационным системам персональных данных. Мероприятия по обеспечению безопасности персональных данных.
8. Основные элементы информационных систем персональных данных и их связь с угрозами безопасности информации, классификация основных угроз безопасности персональных данных.
9. Угрозы утечки акустической и видовой информации, а также угрозы утечки информации по каналам побочных электромагнитных излучений, классификация средств перехвата информации.
10. Классификация угроз несанкционированного доступа к персональным данным, характеристики уязвимостей информационной системы.
11. Характеристика основных угроз и результатов несанкционированного доступа к персональным данным,
12. Типовые модели угроз для автоматизированных рабочих мест, локальных и распределенных информационных систем
13. Основные требования и рекомендации по защите информации, циркулирующей в защищаемых помещениях
14. Требования, рекомендации, порядок обеспечения защиты информации при эксплуатации АС, в ЛВС, на АРМ, при межсетевом взаимодействии, при работе с СУБД, при использовании съемных накопителей информации. Условия, порядок подключения абонентов к Сети, взаимодействие АП с Сетью, рекомендации по обеспечению безопасности информации.
15. Актуальность проблемы, основные термины и определения, классификация и общая характеристика технических каналов утечки информации, физические принципы их возникновения и способы выявления.
16. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
17. Стадии создания средств защиты персональных данных и рекомендуемые мероприятия на каждой стадии проектирования, создания и ввода в действие средств защиты персональных данных.
18. Мероприятия по защите от НСД к персональным данным при их обработке в информационных системах разных классов, а также мероприятия по защите информации от утечки по техническим каналам.
19. Классификация технических средств защиты информации, физические основы их функционирования, а также назначение, состав и основные технические характеристики.
20. Основные термины и определения. Понятие информационной системы персональных данных. Система категорирования персональных данных. Классификация информационных систем персональных данных.
21. Общие вопросы формирования мероприятий, направленных на предотвращение и парирование угроз безопасности персональных данных.
22. Порядок организации обеспечения безопасности персональных данных в информационных системах. Организация и обоснование мероприятий, направленных на обеспечение безопасности персональных данных. Организационные мероприятия по предотвращению утечки персональных данных по техническим каналам. Мероприятия по

выявлению и закрытию технических каналов утечки персональных данных. Мероприятия по защите персональных данных от НСД и неправомерных действий.

23. Классификация и общая характеристика технических каналов утечки информации,
24. Способы применения и тактико-технические характеристики средств способы и средства противодействия несанкционированной аудио-, организация защиты от утечки информации за счет ПЭМИН и технические средства для ее обеспечения.
25. Организация аттестации ОИ, методика разработки и содержание основных документов на защищаемые помещения, и объекты вычислительной техники.
26. Основные методы НСД к данным информационных систем и средствам борьбы с ними. Основные характеристики и классификация методов и средств защиты информации от НСД в информационных системах.

Предмет оценивания	Объекты оценивания	Показатели оценки	Критерии оценки
ПК-1 способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз;	Владение понятийно-терминологическим аппаратом в сфере Федерального закона "О персональных данных" N 152-ФЗ; Умение собирать документы по обеспечению безопасности информации	Полнота и правильность ответа в процессе собеседования	Корректность и полнота ответов на вопросы
ПК-3 способность организовывать и проводить мероприятия по контролю за обеспечением защиты информации, в том числе сведений,	Владение понятийно-терминологическим аппаратом в сфере Федерального закона "Об информации, информационных технологиях и защите информации№149-ФЗ; Владения навыками по контролю за обеспечением защиты	Полнота и правильность ответа в процессе собеседования	Корректность и полнота ответов на вопросы.

составляющих государственную тайну, проводить анализ эффективности системы защиты информации	информации		
ПК-17 Способность организовывать подготовку и представлять объект информатизации в ходе аттестации на соответствие требованиям государственных и ведомственных нормативных документов	Владения профессиональными навыками работы на разных стадиях аттестации на соответствие требованиям государственных и ведомственных нормативных документов	Полнота и правильность ответа в процессе собеседования	Корректность и полнота ответов на вопросы
Условия выполнения задания 1. Место выполнения задания в учебной аудитории ФГБОУ ВО «Тамбовский государственный университет им. Г. Р. Державина» 2. Максимальное время выполнения задания: 1 час. 3. В процессе итоговой аттестации слушатель имеет права пользоваться нормативно-правовыми документам, учебной литературой, а также компьютерной техникой и средствами коммуникации 4. В процессе собеседования оценивается готовность слушателя к осуществлению самостоятельной профессиональной деятельности по профилю программы.			

VI. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

6.1. **Требования к квалификации педагогических кадров, представителей предприятий и организаций, обеспечивающих реализацию образовательного процесса.**

Реализация программы повышения квалификации обеспечивается сотрудниками университета, а также лицами, привлекаемыми к реализации программы на условиях договора гражданско-правового характера. Доля научно-педагогических работников, имеющих образование, соответствующее профилю программы повышения квалификации, в общем числе научно-педагогических работников, реализующих программу, должна составлять не менее 50 процентов. Доля научно-педагогических из числа руководителей и работников организаций, деятельность которых связана с направленностью (реализуемой программы (имеющих стаж работы в данной профессиональной области не менее 3 лет) в общем числе работников, реализующих программу повышения квалификации не менее 25 процентов.

6.2. **Требования к материально-техническим условиям**

Реализация программы предполагает наличие 1 учебного кабинета.

Оборудование учебного кабинета и рабочих мест кабинета: не менее 8 учебных столов.

Технические средства обучения: в процессе обучения используется аудитория, оснащенная проектором, учебной доской, а также ноутбуком, обеспеченным доступом в Интернет.

6.3. **Требованиям к информационным и учебно-методическим условиям**

При разработке программы выполнены требования к содержанию дополнительных профессиональных программ, утвержденных приказом Минобразования РФ от 18 июня 1997 г. № 1221 "Об утверждении Требований к содержанию дополнительных профессиональных образовательных программ"

В лекциях необходимо использовать внутри – и междисциплинарные логические связи. При проведении практических занятий используется методика семинара – обсуждения существующих точек зрения на проблему и пути ее решения. В процессе обучения используются следующие учебно-методические материалы: рекомендуемая основная и дополнительная литература для организации самостоятельной работы слушателей; электронные версии федеральных законов, учебников и методических рекомендаций для подготовки к практическим занятиям.

Перечень используемых учебных изданий, Интернет-ресурсов, дополнительной литературы

1. Конституция Российской Федерации (12 .12.1993).
2. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности».
3. Федеральный закон от 21 .07. 1993 N 5485-1 «О государственной тайне» (с изм. от 18.07.2011г.).
4. Федеральный закон от 27.12.2002 N 184-ФЗ «О техническом регулировании» (с изм. от 03.12.2012г.)
5. Федеральный закон от 26.06. 2008 N 102-ФЗ «Об обеспечении единства измерений» (с изм. от 28.07.2012).
6. Федеральный закон от 27.06.2006 № 149 «Об информации, информационных технологиях и защите информации» (с изм. от 05.04.2013).
7. Федеральный закон от 4.05.2011 №99 ФЗ «О лицензировании отдельных видов деятельности» (с изм. от 04.03.2013 г.)
8. Федеральный закон от 27.06.2006 №152 ФЗ «О персональных данных» (с изм. от 05.04.2013г.)
9. Указ Президента РФ от 06.03.1997 N 188 (ред. от 23.09.2005) "Об утверждении Перечня сведений конфиденциального характера"
10. Указ Президента РФ от 16.08.2004 N 1085 (ред. от 08.02.2012) «Вопросы Федеральной службы по техническому и экспортному контролю» (от 16.08.2004 г. № 1085).
11. Указ Президента РФ от 17. 03.2008 г. N 351 (ред. от 14.01.2011 г) «О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена».
12. Указ Президента РФ от 12.05.2009 г. N 537 «О Стратегии национальной безопасности Российской Федерации до 2020 г».
13. Указ Президента РФ от 9.09.2000 г. N Пр-1895 «Доктрина информационной безопасности РФ».
14. Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) «О сертификации средств защиты информации».
15. Постановление Правительства РФ от 3 февраля 2012 г. N 79 "О лицензировании деятельности по технической защите конфиденциальной информации".
16. Постановление Правительства РФ от 3 ноября 1994 г. N 1233 (ред. 20.07.2012 г.) «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии"».
17. Постановление Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

18. Постановление Правительства РФ от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"
19. Постановление Правительства РФ от 6 июля 2008 г. N 512 (ред. 27 декабря 2012 г.) "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных".
20. Постановление Правительства РФ от 21 марта 2012 г. N 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".
21. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Решение Коллегии ГТК России № 7.2 от 2 марта 2001г. Приказ ГТК России № 282 от 30 августа 2002 г.
22. Приказ ФСТЭК России от 28.02.2013 № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
23. Положение о сертификации средств защиты информации по требованиям безопасности информации. Приказ ГТК России от 27.10.1995 №199.
24. «Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения». Решение председателя Гостехкомиссии России от 30 марта 1992 г.
25. "Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий" (введен в действие Приказом Гостехкомиссии России от 19.06.2002 N 187)
26. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 15.02.2008 год
27. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 15.02.2008 год
28. Руководящий документ Средства вычислительной техники Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации. (введен в действие Приказом Гостехкомиссии России от 30.03.1992 год).
29. «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». Решение председателя Гостехкомиссии России от 30 марта 1992 г.
30. «Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации». Решение председателя Гостехкомиссии России от 25 июля 1997 г.
31. «Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». Приказ председателя Гостехкомиссии России от 4 июня 1999 г. № 114.
32. ГОСТ Р 52069.0-2003 - Защита информации. Система стандартов. Основные положения
33. ГОСТ Р 52447-2005. Защита информации. Техника защиты информации. Номенклатура показателей качества
34. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью
35. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения
36. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
37. ГОСТ ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

38. ГОСТ Р 52863-2007. Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования
39. ГОСТ ИСО/МЭК 15408-1-2008. Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
40. ГОСТ ИСО/МЭК 15408-2-2008. Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий Часть 2. Функциональные требования безопасности.
41. ГОСТ ИСО/МЭК 15408-3-2008. Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.

Дополнительная литература

1. Белов Е.Б. Основы информационной безопасности: Учебн. пособие/ Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. – М.: Горячая линия - Телеком, 2006.
2. Торокин А. А. Инженерно-техническая защита информации. — М.: Гелиос АРВ, 2005.
3. Меньшаков Ю. К. Защита информации от технических средств разведки. — М.: РГГУ, 2002.
4. Бузов Г.А. Защита от утечки по техническим каналам: Учебн. пособие/ Бузов Г.А., Калинин С.В., Кондратьев А.В. – М.: Горячая линия – Телеком,2005.
5. Герасименко В.А. Защита информации в автоматизированных системах. – М.: Энергоатомиздат, 1994 – Книга 1 и 2.
6. Герасименко В.А. Основы защиты информации./ Герасименко В.А., Малюк А.А. – М.: МОПО РФ – МИФИ, 1997.
7. Малюк А.А.Информационная безопасность: концептуальные и методологические основы защиты информации : Учебн. пособие.- М.: Горячая линия - Телеком, 2004.
8. Специальная техника и информационная безопасность: Учебник.Т. 1 / Под ред. В. И. Кирина. — М.: Академия управления МВД России, 2000.
9. Хорев А. А. Защита информации от утечки по техническим каналам: Учебн. пособие.— М.: МО РФ, 2006.
10. Хорев А. А. Теоретические основы оценки возможностей технических средств разведки. — М.: МО РФ, 2000.
11. Ярочкин В.И. Информационная безопасность: Учебник . — М.: Академический Проект; Гаудеамус, 2004.
12. Ю.С. Сидорин Технические средства защиты информации: Учебн. пособие. – СПб.: Издательство Политехнического университета, 2005.
13. Завгородний В. И. Комплексная защита информации в компьютерных системах: Учебн. пособие. —М.: Логос, 2001.

6.4. Общие требования к организации образовательного процесса

Образовательный процесс осуществляется в соответствии с настоящей программой в соответствии локальными нормативными актами образовательной организации.

Продолжительность занятий в устанавливается локальным нормативным актом образовательной организации. Занятия начинаются не ранее 9.00 часов утра и заканчиваются не позднее 21.00 часов. Занятия могут осуществлять в субботу.