Общество с ограниченной ответственностью
«Аплана «Европа»

У Т В Е Р Ж Д А Ю
Генеральный директор

_____ И.О. Морозов

«__» _____ 20__ г.

Дополнительная профессиональная программа

повышения квалификации

СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

Москва, 2016 г.

1. Общие положения

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 учётом требований 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».

Основой для разработки Программы являются: Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные приказом ФСТЭК России от 18 февраля 2013 г. № 21 «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 11 февраля 2013 г. № 17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также документы, регламентирующие вопросы обеспечения безопасности ПДн: «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г, «Методика определения актуальных угроз безопасности ПДн при их обработке в информационных системах персональных данных», Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г, разработанная Министерством труда и социальной защиты Российской Федерации от 09 сентября 2013 г Примерная дополнительная профессиональная программа повышения квалификации специалистов в области информационной безопасности по теме: «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» для федеральных государственных гражданских служащих, ответственных за организацию защиты и обработки персональных данных.

Программа разработана с учётом требований и рекомендаций, определяемых Федеральным законом от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», Приказами Министерства образования и науки Российской Федерации от 01 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам», от 5 декабря 2013 г. № 1310 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности», и от

09 января 2014 г. № 2 «Об утверждении порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ».

2. Цель реализации дополнительной профессиональной программы

Целью реализации дополнительной профессиональной программы повышения квалификации является освоение и совершенствование специалистами актуальных изменений в вопросах профессиональной деятельности, обновление теоретических знаний и умений, получение новых компетенций и развитие навыков, необходимых для осуществления 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***:

– изучение нормативных правовых и организационных основ обеспечения безопасности персональных данных в информационных системах персональных данных;

– изучение методов и процедур выявления угроз безопасности персональных данных в информационных системах персональных данных и оценка степени их опасности;

– практическая отработка способов и порядка проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Область профессиональной деятельности слушателя, прошедшего обучение по программе повышения квалификации «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных», включает совокупность проблем, связанных с организацией обработки и обеспечением безопасности персональных данных, обрабатываемых в информационных системах персональных данных в условиях существования угроз в информационной сфере.

Объектами профессиональной деятельности являются:

– информационные системы персональных данных (ИСПДн) и другие объекты информатизации, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;

– информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере, использующие информационно-технологические ресурсы, подлежащие защите;

– технологии обеспечения информационной безопасности различных объектов информатизации, в том числе ИСПДн;

– системы и процессы управления информационной безопасностью организаций и предприятий различных форм собственности и организации.

В соответствии с видами профессиональной деятельности слушатель, успешно завершивший обучение по данной программе, должен решать следующие ***профессиональные задачи***:

организационно-управленческая деятельность:

– организационно-правовое обеспечение безопасности персональных данных, обрабатываемых в ИСПДн, и информационной безопасности различных объектов информатизации;

– организация работы малых коллективов исполнителей по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн, с учетом требований защиты информации;

– управление информационной безопасностью объекта;

– контроль эффективности реализации политики информационной безопасности объекта и функционирования системы защиты персональных данных, обрабатываемых в ИСПДн;

– участие в определении потребности в средствах защиты информации, используемых для обеспечения безопасности персональных данных;

– участие в обследовании ИСПДн и других объектов информатизации, их категорировании, классификации и определении уровней защищённости ПДн, а так же аттестации их по требованиям безопасности информации;

– мониторинг информационной безопасности объектов информатизации, в том числе ИСПДн;

– разработка проектов нормативных и методических документов, регламентирующих работу по защите информации и иных организационно-распорядительных документов, отрабатываемых в рамках организации обработки и обеспечения безопасности персональных данных.

эксплуатационная деятельность:

– установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы защиты персональных данных и обеспечения информационной безопасности с учетом установленных требований;

– администрирование системы защиты персональных данных и подсистем информационной безопасности объекта информатизации;

– выполнение установленных работ по защите информации, в том числе персональных данных, в организациях и на предприятиях различных форм организации и собственности.

3. Планируемые результаты обучения

Процесс освоения дополнительной профессиональной программы повышения квалификации направлен на качественное изменение следующих компетенций:

в части организационно-управленческой деятельности:

– способности формировать комплекс мер по защите персональных данных и информационной безопасности в целом с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-1);

– способностей организовать и поддерживать выполнение комплекса мер по защите персональных данных и информационной безопасности в целом, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации (ПК-2);

– способности проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов и иных нормативных методических документов в области защиты информации (ПК-3);

– способности использовать нормативные правовые документы в своей профессиональной деятельности (ПК-4);

– способности разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению безопасности персональных данных, информационной безопасности автоматизированных систем, государственных информационных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональ ной деятельности (ПК-5);

– способности организовать и сопровождать аттестацию объектов информатизации, в том числе информационных систем персональных данных, по требованиям безопасности информации (ПК-6).

в части эксплуатационной деятельности:

– способности принимать участие в эксплуатации системы защиты персональных данных и подсистем управления информационной безопасностью подразделений организации (предприятия) (ПК-7);

– способности администрировать систему защиты персональных данных и подсистемы информационной безопасности объекта (ПК-8);

– способности выполнять работы по установке, настройке и обслуживанию технических, программных и программно-аппаратных средств защиты информации (ПК-9);

– способности принимать участие в организации контрольных проверок работоспособности технических, программных и программно-аппаратных средств защиты информации (ПК-10).

В результате освоения дополнительной профессиональной программы повышения квалификации обучающиеся должны получить знания, умения и навыки, которые позволят качественно изменить соответствующие компетенции.

Комплекс знаний, умений и навыков, получаемых в результате освоения дополнительной профессиональной программы повышения квалификации, должен формироваться из приведенного ниже списка.

Обучающиеся 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 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.

владеть навыками:

– определения уровня защиты персональных данных;

– выявления угроз безопасности персональных данных в информационных системах персональных данных.

4. Требования к квалификации поступающего на обучение

Лица, желающие освоить дополнительную профессиональную программу повышения квалификации, должны иметь высшее профессиональное образование по техническим специальностям, связанным с информационной безопасностью, информационными технологиями и специальностями связи. Наличие указанного образования должно подтверждаться документом государственного или установленного образца.

Необходимо иметь стаж работы (не менее 1 года) в одной или нескольких следующих должностях:

- специалист подразделения по защите информации;
- специалист подразделения информационной безопасности;
- специалист подразделения информационных технологий;
- специалист подразделения, ответственного за работу с информацией конфиденциального характера;
- системный (сетевой) администратор;
- администратор безопасности (органа государственной власти, государственной или акционерной компании, ассоциации либо коммерческой структуры).

Желательно также иметь опыт работы и навыки по управлению сетевой инфраструктурой на основе ОС Microsoft Windows Server; понимание принципов работы сетей TCP/IP.

5. Содержание программы

Учебный план

№ п/п	Наименование разделов (модулей)	Всего часов	В том числе:		Формы контроля
			лекции	практ. занятия	
1	Общие вопросы технической защиты информации	22	10	12	
2	Организация обеспечения безопасности персональных данных в информационных системах персональных данных	46	10	36	
3	Итоговая аттестация	4	0	4	Экзамен в форме тестирования
	Итого:	72	20	52	

Учебно-тематический план

№ п/п	Наименование разделов, дисциплин и тем	Всего часов	В том числе:			Формы контроля
			Лекции	Выездные занятия, стажировка и др	Практические занятия, семинары и прочие виды учебных занятий и учебных работ	
1	**Общие вопросы технической защиты информации**	**22**	**10**	**0**	**12**	
1.1	Правовые и организационные основы технической защиты информации ограниченного доступа	8	6		2	
1.2	Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	14	4		10	
2	**Организация обеспечения безопасности персональных данных в информационных системах персональных данных**	**46**	**10**	**0**	**36**	
2.1	Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных	20	4		16	
2.2	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	20	4		16	

2.3	Практические реализации типовых моделей защищённых информационных систем обработки персональных данных	6	2		4	
3	**Итоговая аттестация**	**4**	**0**		**4**	**Экзамен в форме тестирования**
Итого:		**72**	**20**		**52**	

Календарный учебный график

срок обучения	недели	1					2			
	дни	1	1	1	1	1	1	1	1	1
виды занятий, предусмотренные ДПП		А	А	А	А	А	А	А	А	А/И

А – аудиторные занятия
И - итоговая аттестация

Тематическое содержание программы

Раздел 1. Общие вопросы технической защиты информации

Тема 1.1. 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.

В результате освоения темы слушатель должен обладать следующими профессиональными компетенциями: ПК-1, ПК-3, ПК-4, ПК-5, ПК-6.

Тема 1.2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа (НСД)

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. Характери-

стика 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.

В результате освоения темы слушатель должен обладать следующими профессиональными компетенциями: ПК-2, ПК-4, ПК-5, ПК-6, ПК-7.

Раздел 2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных

Тема 2.1. 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. Ос-

новные 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.

В результате освоения темы слушатель должен обладать следующими профессиональными компетенциями: ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-10.

Тема 2.2. 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.

В результате освоения темы слушатель должен обладать следующими профессиональными компетенциями: ПК-1, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10.

Тема 2.3. Практические реализации типовых моделей защищенных 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.

В результате освоения темы слушатель должен обладать следующими профессиональными компетенциями: ПК-5, ПК-6, ПК-7, ПК-8, ПК-9, ПК-10.

6. Организационно-педагогические условия реализации программы

В процессе изучения данной программы необходимо использовать действующие законодательные акты в области защиты персональных данных в информационных системах персональных данных, технической защиты информации, документы национальной системы стандартизации, организационно-распорядительные и нормативные документы ФСТЭК (Гостехкомиссии) России, а также соответствующие учебно-методические пособия и 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 проводится в компьютерном классе с предварительной установкой необходимого программного обеспечения в компьютерной сети. Для проведения цикла практических занятий выделяются два преподавателя: ведущий преподаватель (лектор) и преподаватель для привития практических навыков. 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 технических каналов утечки информации (ТКУИ) и отработке методического аппарата технического контроля 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 обучаемым индивидуализировать задания, 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, которые объединены 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 зачёт с оценкой, в процессе проведения которого применяются методы тестирования с использованием компьютерных технологий.

Учебно-методическое и информационное обеспечение программы

В процессе реализации программы повышения квалификации используются действующие правовые, нормативные и методические документы в области обеспечения информационной безопасности, документы национальной системы стандартизации, организационно-распорядительные и нормативные документы ФСТЭК России, а также соответствующие учебно-методические пособия и иллюстративный материал (презентации).

7. Формы аттестации

6.1. Итоговая аттестация обучающихся по дополнительной профессиональной программе повышения квалификации предусматривает зачёт с оценкой, в процессе проведения которого применяются методы тестирования с использованием компьютерных технологий.

Перечень тестов, используемых для проведения зачёта, целесообразно формировать на основе перечней тестов, выносимых для контроля знаний обучающихся при проведении промежуточных зачётов по учебным модулям, представленным в рабочих программах модулей.

6.2. Для проведения итоговой аттестации создается аттестационная комиссия, состав которой утверждается руководителем организации, осуществляющей образовательную деятельность.

В целях обеспечения объективного определения практической и теоретической подготовленности к выполнению профессиональных задач по результатам обучения в состав аттестационной комиссии рекомендуется включать представителей ФСТЭК России (управлений ФСТЭК России по федеральным округам).

8. Оценочные материалы

1	**«Информация» это:**	
	а	совокупность содержащихся в базах данных сведений
	б	совокупность содержащихся в базах данных сведений, зафиксированных на машинных носителях
	в	сведения (сообщения, данные) воспроизводимые различными системами
	г	сведения (сообщения, данные) независимо от формы их представления

2	**Угроза безопасности информации это:**	
	а	совокупность условий и факторов, определяющих степень важности информации
	б	совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к улучшению функционирования информационной системы
	в	совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба изделию ИТ или его владельцу.
	г	совокупность условий и факторов, определяющих условия размещения информационной системы в пределах контролируемой зоны

3	**Уязвимость информационной системы это:**	
	а	слабость информационной системы, удовлетворяющая требованиям специальных нормативных документов ФСБ
	б	слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.
	в	совокупность условий и факторов, определяющих потенциально опасные последствия реализации угроз
	г	слабость информационной системы, удовлетворяющая требованиям специальных нормативных документов ФСТЭК

4	**«Информационная система» это:**	
	а	совокупность информации, информационных технологий и технических средств
	б	совокупность информации, информационных технологий, технических средств и персонала, обслуживающего систему
	в	совокупность информационных технологий и технических средств
	г	совокупность информации, технических средств и персонала, обслуживающего информационную систему
	д	совокупность информации, технических средств и персонала, обслуживающего и эксплуатирующего информационную систему

5	**Определение уровня защищенности персональных данных производится на основе анализа следующей информации:** ***(выберите все правильные варианты ответа)***	
	а	типы актуальных угроз
	б	количество субъектов ПДн
	в	тип ИСПДн
	г	трудовые взаимоотношения субъекта и оператора
	д	наличие службы безопасности у оператора
	е	структура ИСПДн (АРМ, ЛИС, распределённая ИС)

6	«Предоставление информации» это:	
	а	действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц
	б	действия, направленные на распространение сведений в средствах массовой информации
	в	действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц
	г	действия, направленные на получение информации как определённым так и не-определённым кругом лиц или передачу информации как определенному так и неопределённому кругу лиц

7	В соответствии с требованиями 152-ФЗ «О персональных данных», оператор, являющийся юридическим лицом, назначает:	
	а	сотрудника, ответственного за персональные данные
	б	лицо, ответственное за ведение учёта персональных данных
	в	лицо, ответственное за организацию обработки персональных данных
	г	лицо, ответственное за материальные носители с персональными данными
	д	сотрудника, курирующего вопросы безопасности персональных данных

8	Реализация технического канала утечки информации может привести к нарушениям:	
	а	Конфиденциальности информации
	б	Целостности информации
	в	Доступности информации
	г	Аутентичности информации

9	По признаку отношений к природе возникновения угрозы классифицируются, как: *(выберите все правильные варианты ответа)*	
	а	Объективные
	б	Внутренние
	в	Внешние
	г	Субъективные

10	Количество категорий внутренних нарушителей, определяемых нормативными документами ФСТЭК:	
	а	4
	б	5
	в	6
	г	7
	д	8
	е	9

11	Сопротивления заземляющих проводников, а также земляных шин должны быть:	
	а	более 8 Ом
	б	не более 8 Ом
	в	более 6 Ом
	г	не более 6 Ом
	д	более 4 Ом
	е	не более 4 Ом

12	**Количеством уровней защищенности персональных данных, определяемых правовыми нормативными документами РФ, является:**	
	а	2
	б	4
	в	6
	г	8

13	**ФСТЭК**	
	а	Федеральная служба по техническому и экспертному контролю
	б	Федеральная служба по техническому и экспортному контролю
	в	Федеральная служба технического и эксплуатационного контроля
	г	Федеральная служба технологического и экспертного контроля

14	**Несанкционированный доступ к информации может быть осуществлён путём:** ***(выберите все правильные варианты ответа)***	
	а	Утечки информации за счёт ПЭМИН
	б	Просачивание информативных сигналов в линию электропитания
	в	Подключения к техническим средствам и системам объекта информатизации
	г	Хищения носителей защищаемой информации

15	**Датой принятия и номером *ФЗ* “О персональных данных” является:**	
	а	188-ФЗ от 27 июня 2007
	б	152-ФЗ от 27 июля 2006
	в	149-ФЗ от 27 июля 2006
	г	214-ФЗ от 27 августа 2008

16	**Требования к защите персональных данных при их обработке в информационных системах персональных данных определяются:**	
	а	Постановлением Правительства РФ от 01 ноября 2012 г. № 1119
	б	Постановлением Правительства РФ от 06 июля 2008 г. № 512
	в	Постановлением Правительства РФ от 17 ноября 2007 г. № 781
	г	Постановлением Правительства РФ от 15 сентября 2008 г. № 687
	д	Указом Президента РФ от 6 марта 1997 № 188
	е	Указом Президента РФ от 30 ноября 1995 № 1203

17	**К угрозам непосредственного доступа в операционную среду компьютера, реализуемым в ходе загрузки операционной системы, относятся:** ***(выберите все правильные варианты ответа)***	
	а	анализ сетевого трафика
	б	перехват управления загрузкой с изменением необходимой технологической информации для получения НСД в операционную среду
	в	реализация DDoS-атак
	г	перехват паролей

18	**“Технический канал утечки информации” это:**	
	а	совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация
	б	совокупность средств доступа к информации, нарушающих правила разграничения доступа с использованием штатных средств

	в	совокупность физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация
	г	совокупность объекта технической разведки и средств, которыми добывается защищаемая информация

19	**По характеру угрозы удалённого доступа делятся на:** *(выберите все правильные варианты ответа)*	
	а	многоточечные
	б	одноточечные
	в	активные
	г	пассивные
	д	распределённые

20	**Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, введено в действие:**	
	а	Постановлением Правительства РФ от 01 ноября 2012 г. № 1119
	б	Постановлением Правительства РФ от 06 июля 2008 г. № 512
	в	Постановлением Правительства РФ от 17 ноября 2007 г. № 781
	г	Постановлением Правительства РФ от 15 сентября 2008 г. № 687
	д	Указом Президента РФ от 6 марта 1997 № 188
	е	Указом Президента РФ от 30 ноября 1995 № 1203

21	**Требования к материальным носителям биометрических ПДн и технологиям хранения таких данных вне ИСПДн определяются:**	
	а	Постановлением Правительства РФ от 01 ноября 2012 г. № 1119
	б	Постановлением Правительства РФ от 15 сентября 2008 г. № 687
	в	Постановлением Правительства РФ от 06 июля 2008 г. № 512
	г	Постановлением Правительства РФ от 17 ноября 2007 г. № 781
	д	Указом Президента РФ от 6 марта 1997 № 188
	е	Указом Президента РФ от 30 ноября 1995 № 1203

22	**Приказ Роскомнадзора от 15 марта 2013 г. № 274 определил:**	
	а	Перечень иностранных государств, являющихся сторонами конвенции совета Европы о защите физических лиц при автоматизированной обработке ПДн не обеспечивающих адекватную защиту прав субъектов персональных данных
	б	Перечень иностранных государств не обеспечивающих адекватную защиту прав субъектов персональных данных
	в	Перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных
	г	Перечень иностранных государств, не являющихся сторонами конвенции совета Европы о защите физических лиц при автоматизированной обработке ПДн не обеспечивающих адекватную защиту прав субъектов персональных данных

23	**Приказ Роскомнадзора от 05 сентября 2013 г. № 996 определил:**	
	а	Требования и методы по обезличиванию персональных данных
	б	Требования и методы по обеспечению безопасности персональных данных
	в	Требования и методы по организации обработки персональных данных
	г	Перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных
	д	Перечень иностранных государств не обеспечивающих адекватную защиту прав субъектов персональных данных

24	**Реализация НСД может привести к нарушениям:**	
	а	Конфиденциальности информации
	б	Целостности информации
	в	Доступности информации
	г	Аутентичности информации

25	**Меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, включают:** *(выберите все правильные варианты ответа)*	
	а	наведение чистоты и порядка в помещениях где обрабатываются ПДн
	б	периодическая смена обслуживающего персонала ИСПДн
	в	назначение ответственного за организацию обработки персональных данных
	г	осуществление внутреннего контроля и (или) аудита
	д	оценка вреда, который может быть причинен субъектам персональных данных
	е	ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации

26	**Наиболее перспективными методами обезличивания ПДн являются:** *(выберите все правильные варианты ответа)*	
	а	метод подмешивания посторонней информации
	б	метод введения идентификаторов
	в	метод декомпозиции
	г	метод варьирования
	д	метод перекомпозиции
	е	метод разложения

27	**Лицо, ответственное за организацию обработки ПДн, в частности, обязано:** *(выберите все правильные варианты ответа)*	
	а	доводить до сведения работников оператора положения законодательства Российской Федерации в области налогообложения юридических лиц
	б	осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства РФ о ПДн, в том числе требований к защите персональных данных
	в	осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства РФ о ПДн, за исключением требований к защите ПДн
	г	организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов
	д	лично вести прием и обработку обращений и запросов субъектов персональных данных или их представителей

28	**Перечень 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 определяется:**	
	а	Постановлением Правительства РФ от 01 ноября 2012 г. № 1119
	б	Постановлением Правительства РФ от 06 июля 2008 г. № 512
	в	Постановлением Правительства РФ от 17 ноября 2007 г. № 781

	г	Постановлением Правительства РФ от 15 сентября 2008 г. № 687
	д	Постановлением Правительства РФ от 21 марта 2012 г. № 211

29	**Обезличивание персональных данных это:**	
	а	действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту персональных данных
	б	действия, в результате которых становится невозможным определить принадлежность ПДн конкретному субъекту персональных данных
	в	любое действие (операция) или совокупность действий (операций) с ПДн, совершаемых с использованием средств автоматизации
	г	любое действие (операция) или совокупность действий (операций) с ПДн, совершаемых без использования средств автоматизации
	д	временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)
	е	действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных

30	**Оператор вправе осуществлять без уведомления Роскомнадзора обработку персональных данных:** ***(выберите все правильные варианты ответа)***	
	а	обрабатываемых в соответствии с налоговым законодательством
	б	обрабатываемых в соответствии с трудовым законодательством
	в	обрабатываемых в соответствии с законодательством в области здравоохранения
	г	сделанных субъектом персональных данных общедоступными
	д	обрабатываемых в соответствии с законодательством о банковской деятельности

31*	**Безопасность ПДн при их обработке в ИСПДн могут обеспечивать:** ***(выберите все правильные варианты ответа)***	
	а	оператор
	б	лицо, осуществляющее обработку ПДн по поручению оператора
	в	юридические лица, имеющие лицензию на деятельность по ТЗКИ
	г	индивидуальные предприниматели, имеющие лицензию на деятельность по ТЗКИ
	д	юридические лица, имеющие любую лицензию

32*	**Идентификация и аутентификация субъектов и объектов доступа должна обеспечивать:**	
	а	проверку принадлежности субъекту доступа предъявленного им идентификатора
	б	проверку знания субъектом правил разграничения доступа
	в	проверку целостности объектов доступа
	г	проверку содержания инструкции пользователя ИС

33*	**При обезличивании персональных данных метод перемешивания предполагает:**	
	а	замену части сведений (ПДн) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным
	б	перестановку отдельных записей, а также групп записей в массиве персональных данных
	в	разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств
	г	изменение состава или семантики ПДн путем замены результатами статистической обработки, обобщения или удаления части сведений

34*	**Одним из основных условий реализации угроз непосредственного доступа в операционную среду компьютера является:**	
	а	удалённый доступ нарушителя к компьютеру
	б	физический доступ нарушителя к компьютеру
	в	наличие сетевого сканера
	г	физический доступ в помещение с компьютером

35*	**Источниками угроз НСД к информации являются:** ***(выберите все правильные варианты ответа)***	
	а	внутренние нарушители
	б	внешние нарушители
	в	технические средства негласного съёма информации
	г	аппаратные элементы компьютера
	д	аппаратные закладки

36*	**Информация в зависимости от категории доступа к ней подразделяется на:** ***(выберите все правильные варианты ответа)***	
	а	конфиденциальную
	б	общедоступную
	в	особо конфиденциальную
	г	ограниченного доступа
	д	широкого доступа

37*	**Для каких уровней защищённости ПДн, требуется реализация режима обеспечения безопасности помещений, где размещается ИСПДн?** ***(выберите все правильные варианты ответа)***	
	а	1
	б	2
	в	3
	г	4
	д	5

38*	**Подключение информационных систем, обрабатывающих персональные данные к сети Интернет:**	
	а	Не допускается
	б	Допускается
	в	Допускается только с использованием специально предназначенных для этого средств защиты информации
	г	Допускается только с использованием средств защиты информации известных производителей

39*	**Специальные категории персональных данных это:** *(выберите все правильные варианты ответа)*	
	а	национальная принадлежность
	б	территориальное размещение
	в	состояние аппетита
	г	сверхъестественные способности
	д	состояние интимной жизни
	е	политические взгляды

40*	**Для каких уровней защищённости ПДн, требуется наличие структурного подразделения, ответственного за обеспечение безопасности персональных данных?**	
	а	1
	б	2
	в	3
	г	4
	д	5
	е	6

9. Список литературы

Нормативные правовые акты

1. Конституция Российской Федерации, принята 12 декабря 1993 г.
2. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
3. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
4. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности».
5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
6. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
7. Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
8. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».
9. Федеральный закон от 27 декабря 2002 г. № 184 «О техническом регулировании».
10. Закон РФ № 195-ФЗ от 30 декабря 2001 г. «Кодекс Российской Федерации об административных правонарушениях».
11. Закон РФ № 63-ФЗ от 13 июня 1996 г. «Уголовный кодекс Российской Федерации».
12. Закон РФ № 5485-1 от 21 июля 1993 г. «О государственной тайне».
13. Стратегия национальной безопасности Российской Федерации до 2020 года. Утверждена Указом Президента Российской Федерации 12 мая 2009 г. № 537.
14. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.
15. Указ Президента Российской Федерации от 12 мая 2008 г. № 724 «Вопросы системы и структуры федеральных органов исполнительной власти».
16. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
17. Указ Президента Российской Федерации от 1 ноября 2008 г. № 1576 «О совете при Президенте Российской Федерации по развитию информационного общества в Российской Федерации».
18. Указ Президента Российской Федерации от 30 мая 2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела».
19. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей между-

народного информационного обмена».

20. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

21. Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года. Утверждена распоряжением Правительства Российской Федерации от 17 ноября 2008 г. № 1662-р.

22. Постановление Правительства Российской Федерации от 16 марта 2009 г. № 228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».

23. Постановление Правительства Российской Федерации № 1119 от 1 ноября 2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

24. Постановление Правительства Российской Федерации от 6 июля 2008 г. № 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 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

26. Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

27. Постановление Правительства Российской Федерации от 21 марта 2012 г. № 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».

28. Постановление Правительства Российской Федерации от 18 сентября 2012 г. № 940 «Об утверждении правил согласования проектов решений ассоциаций, союзов и иных объединений операторов об определении дополнительных угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с федеральной службой безопасности российской федерации и федеральной службой по техническому и экспортному контролю».

29. Постановление Правительства Российской Федерации от 21 ноября 2011 г. № 957 «Об организации лицензирования отдельных видов деятельности».

30. Постановление Правительства Российской Федерации от 16 апреля 2012 г. № 313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографиче-

ских) 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)».

31. Постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

32. Постановление Правительства Российской Федерации от 3 марта 2012 г. № 171 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

33. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».

34. Постановление Правительства Российской Федерации от 28 февраля 1996 г. № 226 «О государственном учете и регистрации баз и банков данных».

Нормативные методические документы

1. «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
2. «Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам». Гостехкомиссия России. - М., 2002.
3. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России. - М., 1995.
4. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России. - М., 2006.
5. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. - М., 2006.
6. ГОСТ Р 51583 - 2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»
7. ГОСТ Р 51624 - 2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»
8. ГОСТ 34.201 - 1989 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».
9. ГОСТ 34.601 - 1990 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии созда-

ния».

10. ГОСТ 34.602 - 1989 «Информационные технологии. Комплекс стандартов на автоматизированную систему. Техническое задание на создание автоматизированной системы».

11. ГОСТ 34.603 - 1992 «Информационная технология. Виды испытаний автоматизированных систем».

12. ГОСТ Р ИСО/МЭК 15408-1-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт России. - М., 2008.

13. ГОСТ Р ИСО/МЭК 15408-2-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России. - М., 2008.

14. ГОСТ Р ИСО/МЭК 15408-3-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России. - М., 2008.

15. ISO/IEC 27001:2005. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

16. ISO/IEC 27002:2013. Информационные технологии. Методики безопасности. Практические правила управления информационной безопасностью.

17. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 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 содержащей сведений, составляющих государственную тайну».

18. Приказ ФСБ России от 08 августа 2009 г. № 149/7/2/6-1173 «Об утверждении типового регламента проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством РФ, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

19. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации». Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/54-144.

20. «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/6/6-622.

21. Приказ ФСТЭК России от 20 марта 2012 г. № 28 «Об утверждении требований к средствам антивирусной защиты».

22. Приказ ФСТЭК России от 6 декабря 2011 г. № 638 «Об утверждении требований к системам обнаружения вторжений».

23. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

24. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

25. Методический документ. «Меры защиты информации в государственных информационных системах», Уверждён ФСТЭК России от 11 февраля 2014 г.

26. Приказ ФСТЭК России от 12 июля 2012 г. № 83 «Об утверждении административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации».

27. Приказ Роскомнадзора от 14 ноября 2011 г. № 312 «Об утверждении административного регламента проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных».

28. Приказ Роскомнадзора от 19 августа 2011 г. № 706 «Об утверждении Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных».

29. Приказ Роскомнадзора от 15 марта 2013 г. № 274 «Об утверждении перечня иностранных государств, не являющихся сторонами конвенции совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных».

30. Приказ Роскомнадзора от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

31. Методические рекомендации по применению приказа Роскомнадзора от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных». Утверждены Руководителем Роскомнадзора 13 декабря 2013 г.

32. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». - М., 1999.

33. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения». - М, 1992.

34. Руководящий документ Гостехкомиссии России «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». - М., 1992.

35. Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». -

М, 1992.

36. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». - М., 1992.

37. Руководящий документ Гостехкомиссии России «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники». - М., 1992.

38. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». - М., 1997. Федеральная служба по техническому и экспортному контролю. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.

39. Федеральная служба по техническому и экспортному контролю. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.

Основная 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. - 544 с.

2. Бузов Г.А. Защита от утечки информации по техническим каналам: Учебн. пособие / БузовГ.А, Калинин С.В., Кондратьев А.В.- М.: Горячая линия - Телеком, 2005. - 416 с.

3. 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.

4. Малюк А.А. Введение в защиту информации в автоматизированных системах: Учебн. пособие для вузов / Малюк А.А, Пазизин С.В., Погожин Н.С. - М.: Горячая линия - Телеком, 2004. - 147 с.

5. Снытников А.А. Лицензирование и сертификация в области защиты информации. - М.: Гелиос АРВ, 2003. - 192 с.

6. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. - Минск, 2005. - 304 с.

7. Хорев А.А. Защита информации от утечки по техническим каналам: Учебн. пособие. - М.: МО РФ, 2006.

8. Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных сетях. - Ростов-на-Дону: Издательство СКНЦ ВШ, 2006.

9. Язов Ю.К. Основы технологий проектирования систем защиты информации в информационно-телекоммуникационных системах: Монография /

Аграновский А.В, Мамай В.И, Назаров И.Г., Язов Ю.К. -Издательство СКНЦВШ, 2006.

10. Будников С.А, Паршин Н.В. Информационная безопасность автоматизированных систем: Учебное пособие, издание второе, дополненное - Издательство им. Е.А.Болховитинова, Воронеж, 2011.

11. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. - С.-П., 2004.- 384 с.

12. Петраков А.В. Основы практической защиты информации. Учебное пособие. - М, 2005.- 281 с.