Министерство транспорта Российской Федерации
Федеральное агентство железнодорожного транспорта
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Дальневосточный государственный университет путей сообщения»

Институт дополнительного образования

Согласовано:
Руководитель Управления ФСТЭК России по ДФО
_____ В.И. Анохин
«___»_____ 2014 г.

Утверждаю:
Ректор университета, профессор
_____ Б.Е. Дынькин
«____» _____ 2014 г.

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ
по направлению
090900 Информационная безопасность
«Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»

Хабаровск 2014

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

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 28.12.2010 № 390-ФЭ «О безопасности», Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Основой для разработки программы являются Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Постановление Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утв. приказом ФСТЭК России от 18.02.2013№21, «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утв. приказом ФСТЭК России от 11 февраля 2013 г. № 17 а также документы, регламентирующие вопросы обеспечения безопасности персональных данных: «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

При разработке программы выполнены требования к содержанию дополнительных профессиональных образовательных программ, утверждённые приказом Минобразования России от 18.06.1997 № 1221.

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

Поставленная цель достигается решением следующих задач:

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

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

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

Категория слушателей: специалисты органов государственной власти по защите информации, осуществляющие разработку и эксплуатацию автоматизированных информационных систем, обеспечивающих обработку, хранение и передачу персональных данных; руководители и специалисты подразделений по обеспечению безопасности информации в информационных и автоматизированных системах, подразделений информационных технологий, подразделений, ответственных за работу с информацией ограниченного доступа, системные и сетевые администраторы, администраторы безопасности информации предприятий, учреждений и организаций различных форм собственности.

Срок обучения: 72 часа аудиторных учебных занятий.

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

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

В результате изучения курса слушатели должны:

быть ознакомлены:

– с нормативными правовыми и организационными основами защиты информации и обеспечения безопасности персональных данных в Российской Федерации;

– с порядком организации и проведения лицензирования деятельности в области защиты информации;

– с документами национальной системы стандартизации, действующими в области защиты информации;

знать:

– содержание основных нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;

– основные виды угроз безопасности персональных данных в информационных системах персональных данных;

– содержание и порядок организации работ по выявлению угроз безопасности персональных данных;

– процедуры задания и реализации требований по защите информации в информационных системах персональных данных;

– меры обеспечения безопасности персональных данных; требования по обеспечению безопасности персональных данных; порядок применения организационных мер и технических мер обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;

уметь:

– планировать мероприятия по обеспечению безопасности персональных данных;

– разрабатывать необходимые документы в интересах организации работ по обеспечению безопасности персональных данных;

– обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных;

– проводить оценки актуальных угроз безопасности персональных данных

при их обработке в информационных системах персональных данных;

– определять состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для блокирования угроз безопасности персональных данных.

иметь навык:

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

Слушатели, завершившие освоение дополнительной профессиональной программы повышения квалификации, должны обладать следующими компетенциями:

– способностью действовать в соответствии с Конституцией Российской Федерации, федеральными конституционными законами, иными нормативными правовыми актами Российской Федерации (Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 29 июля 2004 г., Федеральный закон от 27 июля 2006 г. «О персональных данных» № 152-ФЗ, Федеральный, Федеральный закон от 28.12.2010 № 390-ФЭ «О безопасности», Постановление Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные приказом ФСТЭК России от 18.02.2013№21), и обеспечивать их исполнение;

– способностью соблюдать ограничения, выполнять обязательства и требования к служебному поведению, не нарушать запреты, которые установлены законодательством Российской Федерации в области защиты информации;

– понимать сущность и значение информации в своей профессиональной деятельности, осознанием опасности угроз, возникающих в этом процессе, умением соблюдать основные требования информационной безопасности;

– способностью применять современные информационно-коммуникационные технологии, в том числе технологию электронного документооборота;

– способностью поддерживать уровень квалификации, необходимый для надлежащего исполнения должностных обязанностей.

– способностью использовать нормативные правовые акты в своей профессиональной деятельности (ПК-6);

– способностью использовать основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий (ПК-7);

– способностью к освоению новых образцов программных, технических средств и информационных технологий (ПК-8);

– способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере своей профессиональной деятельности (ПК-9);

– способностью применять современные методы исследования с использованием компьютерных технологий (ПК-10);

– способностью разрабатывать и исследовать модели автоматизированных систем (ПК-11);

– способностью проводить анализ защищенности автоматизированных систем (ПК-12);

– способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-13);

– способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-14);

– способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем (ПК-15);

1. ПЕРЕЧЕНЬ ТЕМ

Наименование разделов и тем

№ п/п	Наименование разделов и тем
1	**Раздел № 1. Общие вопросы технической защиты информации**
2	**Тема № 1.** Правовые и организационные вопросы технической защиты информации ограниченного доступа
3	**Тема № 2.** Выявление угроз безопасности информации на объектах информатизации. основные организационные меры. технические и программные средства защиты информации от несанкционированного доступа
4	**Раздел № 2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных**
5	**Тема № 3**. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных. организационные и технические меры защиты информации в информационных системах персональных данных
6	**Тема № 4.** Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
7	**Тема № 5.** Практические реализации типовых моделей защищенных информационных систем обработки персональных данных

2. РЕФЕРАТИВНОЕ ОПИСАНИЕ ТЕМ

Раздел № 1. Общие вопросы технической защиты информации

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

Основные понятия в области технической защиты информации (ТЗИ). Стратегия национальной безопасности Российской Федерации до 2020 года. Доктрина информационной безопасности Российской Федерации. Концептуальные основы ТЗИ. Законодательные и иные правовые акты, регулирующие вопросы ТЗИ. Система документов по ТЗИ и краткая характеристика ее основных составляющих.

Структура и направления деятельности системы ТЗИ в субъектах Российской Федерации. Система органов по ТЗИ в Российской Федерации, их задачи, распределение полномочий по обеспечению ТЗИ. Задачи, полномочия и права Федеральной службы по техническому и экспортному контролю (ФСТЭК России). Задачи, полномочия и права управлений ФСТЭК России по федеральным округам.

Лицензирование деятельности в области технической защиты информации. Сертификация средств защиты информации, аттестация объектов информатизации по требованиям безопасности информации. Документы национальной системы стандартизации в области ТЗИ.

Основные документы, определяющие направления и порядок организации деятельности, организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Права субъектов персональных данных. Способы защиты прав субъектов персональных данных.

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

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

Классификация объектов информатизации. Методические рекомендации по классификации и категорированию объектов информатизации. Характеристика основных угроз несанкционированного доступа и моделей нарушителя

безопасности информации, а также способов реализации этих угроз. Характеристика основных классов атак, реализуемых в сетях общего пользования, функционирующих с использованием стека протоколов TCP/1P. Понятие программно-математического воздействия и вредоносной программы. Классификация вредоносных программ, основных деструктивных функций вредоносных программ и способов их реализации. Особенности программно-математического воздействия в сетях общего пользования. Методы и средства выявления угроз несанкционированного доступа к информации и специальных воздействий на неё. Порядок обеспечения защиты информации при эксплуатации автоматизированных систем.

Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ. Защита информации в локальных вычислительных сетях. Защита информации при межсетевом взаимодействии. Защита информации при работе с системами управления базами данных. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования.

Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники.

Содержание и порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Структура, содержание и порядок подготовки документов при аттестации объектов информатизации по требованиям безопасности информации.

Раздел № 2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных

Тема № 3. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных

Особенности информационного элемента информационной системы персональных данных.

Основные типы актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, порядок их определения. Угрозы несанкционированного доступа к информации в информационных системах персональных данных. Угрозы утечки информации по техническим каналам.

Основные принципы обеспечения безопасности персональных данных при их обработке: законности, превентивности, адекватности, непрерывности, адаптивности, самозащиты, многоуровневости, персональной ответственности и минимизации привилегий, разделения полномочий и их характеристика. Основные направления деятельности по обеспечению безопасности персональных данных при их обработке в информационных системах

персональных данных. Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных. Оценка достаточности и обоснованности запланированных мероприятий.

Особенности обеспечения безопасности персональных данных, обрабатываемых на автоматизированных рабочих местах с использованием автономных ПЭВМ, в локальных вычислительных сетях и при межсетевом взаимодействии.

Рекомендации по применению мер и средств обеспечения безопасности персональных данных от физического доступа.

Причины и физические явления, порождающие технические каналы утечки информации (ТКУИ) при эксплуатации объектов информатизации. Классификация ТКУИ.

Основные требования и рекомендации по защите речевой информации, циркулирующей в защищаемых помещениях.

Оценка защищённости информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации.

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

Определение необходимых уровней защищенности персональных данных при их обработке в информационных системах в зависимости от типа актуальных угроз для информационных систем, вида и объема обрабатываемых в них персональных данных.

Порядок проведения классификации государственных и муниципальных информационных систем.

Состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий.

Порядок выбора мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных: определение базового набора мер, адаптация базового набора, уточнение адаптированного базового набора мер, дополнение уточненного адаптированного базового набора мер.

Содержание мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных.

Требования к средствам защиты информации для обеспечения различных уровней защищенности персональных данных.

Организация обеспечения безопасности персональных данных в организациях и учреждениях. Перечень основных этапов при организации работ по обеспечению безопасности персональных данных.

Мероприятия по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных и особенности их реализации.

Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов ненормативного характера по обработке персональных данных и обеспечению безопасности персональных данных. Подготовка уведомлений об обработке персональных данных в уполномоченный орган, порядок внесения изменений в ранее представленное в уполномоченный орган уведомление.

Обязанности оператора, осуществляющего обработку персональных данных. Порядок и условия обработки персональных данных без средств автоматизации. Порядок и методы обезличивания персональных данных, их деобезличивание. Особенности обработки персональных данных в условиях государственной гражданской службы и муниципальной службы. Ответственность за нарушение требований законодательства Российской Федерации в области персональных данных.

Тема № 5. Практические реализации типовых моделей 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.

3. УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе, аудиторных занятий,		Формы контроля
			лекции	практические занятия (семинары)	
1	2	3	4	5	7
1	**Раздел № 1. Общие вопросы технической защиты информации**	**22**	**16**	**4(2)**	
2	**Тема № 1.** Правовые и организационные основы технической защиты информации ограниченного доступа	8	8		
3	**Тема № 2.** Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	14	8	4(2)	Опрос на практическом занятии и семинаре
4	**Раздел № 2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных**	**46**	**36**	**8(2)**	
5	**Тема № 3.** Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных	20	14	4(2)	Опрос на лекции. Опрос на практическом занятии и семинаре. Выполнение курсовой работы.

6	**Тема № 4.** Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	20	20		
7	**Тема № 5.** Практические реализации типовых моделей защищённых информационных систем обработки персональных данных	6	2	4	Опрос на практическом занятии
8	**Итого по видам занятий**	**68**	**52**	**12(4)**	
9	**Зачет с оценкой**	**4**			**4**
10	**Всего**	**72**	**52**	**12(4)**	**4**

4. МАТЕРИАЛЬНО-ТЕХНИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Наименование специализированных аудиторий, кабинетов, лабораторий	**Вид занятий**	**Наименование оборудования, программного обеспечения**
Аудитория	лекции	компьютер, мультимедийный проектор, экран, доска
Лаборатория «Защита ЛВС от НСД»	практические и лабораторные занятия	учебные стенды по применению технических средств защиты информации в ЛВС от НСД
Лаборатория «Защита речевой информации»	практические и лабораторные занятия	учебные стенды по применению технических средств защиты информации от утечки по акустическому, виброакустическому каналам утечки
Лаборатория «Специальных исследований»	практические и лабораторные занятия	учебные стенды по применению технических средств защиты информации представленных в виде информативных электрических сигналов и физических полей

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО РЕАЛИЗАЦИИ ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЫ

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

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

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

На практические занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл практических занятий по применению программно-аппаратных средств защиты персональных данных при их обработке в информационных системах персональных данных (тема № 2), проводится в компьютерном классе с предварительной установкой необходимого программного обеспечения в компьютерной сети. 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 ТКУИ и отработке методического аппарата технического контроля (Тема № 3) проводятся по циклам на четырёх-шести рабочих местах (количество рабочих мест зависит от количества обучаемых в учебной группе). На каждом рабочем месте должен быть преподаватель, развёрнуто необходимое оборудование технического контроля и средства имитации ТКУИ.

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

существенных для определённых категорий обучаемых, объединённых в соответствующую подгруппу.

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

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

5. СПИСОК ОСНОВНОЙ ЛИТЕРАТУРЫ

5.1 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.

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

5.3 Запечников С.В. Информационная безопасность открытых систем. Часть 1: Учебник для вузов / Запечников СВ., Милославская Н.Г Толстой А.И, Ушаков Д.В. - М.: Горячая линия - Телеком, 2006. - 686 с.

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

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

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

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

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

5.9 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.

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

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

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

5.13 Девянин П.Н., Садердинов А.А, Трайнев В.А. и др. Учебное пособие. Информационная безопасность предприятия. - М, 2006.- 335 с.

6. СПИСОК ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ

6.1 Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности».

6.2 Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

6.3 Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании».

6.4 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

6.5 Указ Президента Российской Федерации от 16.08.2004 №1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

6.6 Указ Президента Российской Федерации от 17.03.2008 №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

6.7 Стратегия национальной безопасности Российской Федерации до 2020 года, утверждена Указом Президента Российской Федерации от 12.05.2009 №537.

6.8 Доктрина информационной безопасности Российской Федерации, утверждена Президентом Российской Федерации 09.09.2000 Пр-1895.

6.9 Постановление Правительства Российской Федерации от 26.01.2006 № 45 «Об организации лицензирования отдельных видов деятельности».

6.10 Постановление Правительства Российской Федерации от 01.02.2006 №54 «О государственном строительном надзоре в Российской Федерации».

6.11 Постановление Правительства Российской Федерации от 03.02.2012 №79 «О лицензировании деятельности по технической защите конфиденциальной информации».

6.12 Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

6.13 Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Гостехкомиссия России, 1992.

6.14 Положение о сертификации средств защиты информации по требованиям безопасности информации, утверждено приказом Гостехкомиссии России от 27.10.1995 № 199.

6.15 Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утверждены приказом Гостехкомиссии России от 30.08.2002 № 282.

6.16 Сборник временных методик оценки защищённости конфиденциальной информации от утечки по техническим каналам. Гостехкомиссия России, 2002.

6.17 Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий, утвержден приказом председателя Гостехкомиссии России от 19.06.2002 № .187

6.18 Приказ ФСТЭК России от 18.02.2013 №21. Об утверждение Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах

персональных данных.
6.19 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 15.02.2008.
6.20 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 15.02.2008.
6.21 Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации, утверждён решением председателя Гостехкомиссии России от 30.03 1992
6.22 Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации, утверждён решением председателя Гостехкомиссии России от 30.03.1992.
6.23 Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. I Указатели защищенности от несанкционированного доступа к информации, утверждён решением председателя Гостехкомиссии России от 25.07.1997.
6.24 Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники, утверждён решением председателя Гостехкомиссии России от 30.03.1992.
6.25 Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования. Утверждён решением председателя Гостехкомиссии России от 25.07.1997.
6.26 Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей, утверждён приказом председателя Гостехкомиссии России от 04.06.1999 № 114.
6.27 ГОСТ Р 52069.0-2003 «Защита информации. Система стандартов. Основные положения».
6.28 ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества».
6.29 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 года № 149/6/6-622.
6.30 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 года № 149/54-144.

Директор Дальневосточного учебно-научного центра по информационной безопасности — Никитин В.Н.

Составители программы:

Директор Дальневосточного учебно-научного центра по информационной безопасности — Никитин В.Н

Специалист Дальневосточного учебно-научного центра по информационной безопасности — Гусакова Т.А.