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:
Начальник 1 управления
ФСТЭК России
_____
«___»_____ 2014 г.

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

ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

по направлению

090900 Информационная безопасность

«Организация и нормативно-методическое обеспечение технической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в органах государственной власти субъектов Российской Федерации, местного самоуправления, организациях и учреждениях»

Хабаровск
2014

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

Программа повышения квалификации специалистов в области информационной безопасности по теме «Организация и нормативно-методическое обеспечение технической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в органах государственной власти субъектов Российской Федерации, местного самоуправления, организациях и учреждениях» (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 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», 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, «Методический документ. Меры защиты информации в государственных информационных системах», утв. ФСТЭК России 11.02.2014, а также документы, регламентирующие вопросы обеспечения безопасности информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.

Программа составлена в соответствии с «Порядком разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности», утвержденным приказом Министерства образования и науки Российской Федерации от 5 декабря 2013 г. № 1310.

Цель обучения по программе: обеспечение заданного уровня знаний, умений и навыков у специалистов по защите информации в применении способов и средств технической защиты информации на объектах информатизации при непосредственном решении задач по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.

Поставленная цель достигается решением следующих задач:

– изучением правовых и организационных основ технической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну;
– изучением методов и процедур выявления угроз безопасности информации на объектах информатизации и оценки степени их опасности;
– практической отработкой способов и порядка проведения работ по ТЗИ;
– изучением методов оценки состояния ТЗИ в органах государственной власти

субъектов Российской Федерации, местного самоуправления, организациях и учреждениях.

Категория слушателей: 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, специалисты органов государственной власти по защите информации, осуществляющие разработку и эксплуатацию автоматизированных информационных систем, обеспечивающих обработку, хранение и передачу персональных данных, администраторы безопасности информации предприятий, учреждений и организаций различных форм собственности,

Срок обучения: 72 часа аудиторных учебных занятий в течение 2-х недель.

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

Режим занятий: 8 часов в день при пятидневной учебной неделе

Слушатели, успешно освоившие программу, будут

знать:

- нормативные правовые акты Российской Федерации в области защиты информации, нормативные и методические документы в области технической защиты информации;

– организационно-распорядительные документы, связанные с осуществлением служебной деятельности;

– физические основы возникновения, классификацию и характеристики типовых каналов утечки информации и других угроз безопасности информации;

– общие требования по технической защите информации (ТЗИ), нормы, требования и рекомендации по защите объектов информатизации от различных угроз безопасности информации, методы и методики контроля их выполнения;

– организацию, содержание, порядок и технологию проведения работ по ТЗИ, состав и содержание необходимых документов;

– требования к средствам технической защиты информации, контроля технической защиты информации;

– средства ТЗИ и контроля эффективности ТЗИ, возможности и порядок применения, перспективы развития;

– порядок организации и проведения контроля состояния ТЗИ;

– порядок проведения, содержания, правила оформления результатов специальных исследований, специальных проверок и аттестации объектов информатизации по требованиям безопасности информации;

– виды юридической ответственности за нарушение законодательства Российской Федерации в области охраны коммерческой тайны и обеспечения экономической безопасности.

уметь:

– различать между собой общедоступную информацию и информацию ограниченного доступа;

– толковать и применять в профессиональной деятельности основные нормативно – правовые акты, регулирующие порядок работы с информацией, ограниченного доступа, а также способы обеспечения экономической безопасности организации;

– использовать полученные знания для защиты информации конфиденциального характера и обеспечения экономической безопасности предприятия, учреждения и организации;

– определять возможные каналы утечки и другие угрозы безопасности информации;

– определять требования к техническим, программным программно-техническим средствам, предназначенным для хранения, обработки и передачи информации ограниченного доступа;

– осуществлять контроль состояния (организации и эффективности) ТЗИ;

– применять действующую нормативную правовую и методическую базу в области ТЗИ;

– разрабатывать проекты документов (положений, инструкций, руководств и др.) в области ТЗИ, а также оформлять результаты специальных исследований, специальных проверок и аттестации объектов информатизации по требованиям безопасности информации;

– проводить работы по категорированию, классификации защищенности информационных и автоматизированных систем от несанкционированного доступа к информации, аттестации объектов информатизации;

– организовывать и проводить практические мероприятия по обеспечению выполнения режимных требований;

– определять требования к организации технической защиты информации конфиденциального характера;

– организовывать контроль над выполнением установленных режимных мер.

владеть:

– навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем;

– криптографической терминологией;

– навыками работы с нормативными правовыми актами;

– навыками организации и обеспечения режима конфиденциальности;

– методами организации и управления деятельностью служб защиты информации на предприятии, в учреждении и организации;

– методами формирования требований по защите информации;

– методами и средствами выявления угроз безопасности информационным и автоматизированным системам;

– методами технической защиты информации;

– методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;

– профессиональной терминологией.

2. ПЕРЕЧЕНЬ ТЕМ
Наименование разделов и тем

№ п/п	Наименование темы
1	**Раздел № 1 Общие вопросы технической защиты информации**
2	**Тема №1** Правовые и организационные основы технической защиты информации ограниченного доступа, не содержащие сведений, составляющих государственную тайну
3	**Тема №2** Выявление угроз безопасности информации ограниченного доступа, не содержащие сведений, составляющих государственную тайну, на объектах информатизации. Основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа
4	**Раздел № 2 Организация обеспечения безопасности информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну**
5	**Тема №3** Основные организационные меры и технические средства защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, на объектах информатизации и в защищаемых помещениях от утечки по техническим каналам
6	**Тема №4** Нормативно-методическое обеспечение технической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, на объектах информатизации органов государственной власти, местного самоуправления, организаций и учреждений
7	**Тема №5** Оценка состояния технической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, на объектах информатизации органов государственной власти, местного самоуправления, организаций и учреждений

3. РЕФЕРАТИВНОЕ ОПИСАНИЕ ТЕМ

Тема №1. Правовые и организационные основы технической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну

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 ограниченного доступа, не содержащей сведений, составляющих государственную тайну, 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 защиты. Характеристика основных угроз несанкционированного доступа и моделей нарушителя безопасности информа-

ции, 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 (НСД) 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. Основные требования и рекомендации по защите служебной тайны. Основные рекомендации по защите информации, составляющей коммерческую тайну.

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.

Тема № 3. Основные организационные меры и технические средства защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, на объектах информатизации и в защищаемых помещениях от утечки по техническим каналам

Причины и физические явления, порождающие технические каналы утечки информации (ТКУИ) при эксплуатации объектов информатизации и защищаемых помещений. Классификация ТКУИ. Характеристики информационных сигналов, определяющие степень их опасности. Причины и физические явления, порождающие ТКУИ. Методы и средства выявления ТКУИ на типовом объекте информатизации и в защищаемых помещениях.

Основные требования и рекомендации по защите речевой информации, циркулирующей в защищаемых помещениях. Защита информации, циркулирующей в системах звукоусиления и звукового сопровождения видео-кинофильмов. Защита информации при проведении магнитной звукозаписи. Защита речевой информации при ее передаче по каналам связи.

Содержание и порядок организации и проведения специальных исследований технических средств обработки информации.

Оценка защищённости помещений от утечки речевой информации по акустическому и виброакустическому каналам и по каналу электроакустических преобразований во вспомогательных технических средствах и системах.

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. Нормативно-методическое обеспечение технической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, на объектах информатизации органов государственной власти, местного самоуправления, организаций и учреждений

Общий порядок организации ТЗИ на действующих объектах информатизации. Порядок разработки и согласования проектов тактико-технических заданий (ТТЗ) на проведение научно-исследовательских и опытно-конструкторских работ в интересах создания систем защиты информации на объектах информатизации.

Необходимое нормативное и информационное обеспечение ТЗИ на объектах информатизации. Система требований по ТЗИ на объектах информатизации и процедура обоснования указанных требований. Порядок разработки и согласования руководств и инструкций по ТЗИ. Оценка достаточности и обоснованности запланированных мероприятий по ТЗИ.

Порядок разработки и согласования проектов планов и ТТЗ по выполнению работ по строительству, реконструкции и техническому перевооружению объектов информатизации, оценка обоснованности запланированных мероприятий по ТЗИ. Порядок разработки и согласования инструкций по ТЗИ для этапа строительства, реконструкции и технического перевооружения объектов информатизации.

Тема № 5. Оценка состояния технической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, на объектах информатизации органов государственной власти, местного самоуправления, организаций и учреждений

Цели проведения оценки состояния ТЗИ на объектах информатизации органов государственной власти, местного самоуправления, организаций и учреждений субъектов Российской Федерации. Показатели и критерии оценки состояния ТЗИ. Требования к показателям и процедуре оценки состояния ТЗИ. Методические рекомендации по сбору исходной информации для проведения оценок состояния ТЗИ и обобщения этой информации. Методики определения показателей оценки состояния ТЗИ.

Цели, принципы и задачи развития системы ТЗИ в органах государственной власти, местного самоуправления, организациях и учреждениях. Определение приоритетных мероприятий по повышению эффективности ТЗИ и обеспечение деятельности системы ТЗИ.

4. УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе, аудиторных занятий, часов		Формы контроля
			лекции	практические занятия (семинары)	
1	2	3	4	5	7
1	**Раздел № 1 Общие вопросы технической защиты информации**	**28**	**18**	**8 (2)**	
2	**Тема №1** Правовые и организационные основы технической защиты информации ограниченного доступа, не содержащие сведений, составляющих	8	8		
3	**Тема №2** Выявление угроз безопасности информации ограниченного доступа, не содержащие сведений, составляющих государственную тайну, на объектах информатизации. Основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	20	10	8 (2)	Опрос на практическом занятии и семинаре
4	**Раздел № 2 Организация обеспечения безопасности информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну**	**40**	**18**	**20(2)**	
5	**Тема №3** Основные организационные меры и технические средства защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, на объектах информатизации и в защищаемых помещениях от утечки по техническим каналам	20	8	10(2)	Опрос на лекции. Опрос на практическом занятии и семинаре. Выполнение курсовой работы.

6	**Тема №4** Нормативно-методическое обеспечение технической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, на объектах информатизации органов государственной власти, местного самоуправле-	10	6	4	
7	**Тема №5** Оценка состояния технической защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, на объектах информатизации органов государственной	10	4	6	Опрос на практическом занятии
8	**Итого по видам занятий**	68	36	28(4)	
9	**Зачет с оценкой**	4			4
10	**Всего**	72	36	28(4)	4

5. 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

6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО РЕАЛИЗАЦИИ ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЫ

В процессе изучения данной программы используются действующие законодательные акты в области технической защиты информации, документы национальной системы стандартизации, организационно-распорядительные и нормативные документы уполномоченных органов государственной власти, ФСТЭК (Гостехкомиссии) России, а также учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по технической защите информации. Часть лекций излагается проблемным методом с привлечением слушателей для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций используются различные приёмы тестирования.

Наиболее сложные и важные в практической профессиональной деятельности слушателей вопросы по темам № 2 и № 3 курса - 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 отработке программно-аппаратных средств защиты информации ограниченного доступа (Тема № 2) проводится в лаборатории «Защита информации от утечки за счет несанкционированного доступа в локальных вычислительных сетях» с предварительной установкой необходимого программного обеспечения ("Secret Disk Server NG", Страж NT 2.5, SecretNet 5.0 Сетевой на 5 компьютеров + сервер, "Аккорд-NT/2000" v.3.0, SecretNet 5.0, "ФПСУ-IP Усиленный", АПКШ "Континент", Dallas Lock 8.0, TrustAceess, Security Studio Endpoint Protection, UserGate Proxy & Firewall 5.2) в компьютерной сети. Цикл практических занятий проводят два преподавателя: ведущий преподаватель (лектор) и преподаватель для обучения практическим действиям. При проведении практических занятий отрабатываются задания, учитывающие специфику функциональных обязанностей, выполняемых слушателями в соответствии с их должностным предназначением, в том числе предусматривается проведение деловых игр (эпизодов).

Практические занятия по обнаружению ТКУИ и отработке методического аппарата технического контроля эффективности защиты информации (Тема № 3) проводятся по циклам на четырех рабочих местах в лабораториях «Защита речевой информации от утечки за счет недостаточной звуко- и виброизоляции помещений» и «Защита информации от утечки по техническим каналам в локальных вычислительных сетях и помещениях».

На два рабочих места один преподаватель, развёрнуто необходимое оборудование технического контроля (система «Шепот», комплекс «Стентор», комплекс «Сигурд», комплекс «Талис»), средства имитации ТКУИ и средства защиты информации ("Шорох-3","Шорох-4-2","Хаос-4", "Сапфир-2", "Ладья", "Мозаика-3ДМ", "Со-

ната-РК1","ГШ-2500","ЛГШ-501","Соната-РС1","Соната-Р2","ФСПК-10"). Результаты, полученные в ходе практических занятий, используются в качестве исходных данных при отработке пакетов документов на практических занятиях по темам № 4 и №5.

Для проведения практических занятий используются методические разработки, позволяющие индивидуализировать задания обучаемым в зависимости от их должностных категорий. Такие задания представляют собой проблемные ситуационные варианты, различающиеся моделями объектов информатизации и, следовательно, набором конкретных действий, существенных для определённых категории обучаемых, объединённых в соответствующую подгруппу.

В качестве формы итогового контроля полученных знаний выбран зачёт (продолжительностью 4 учебных часа) с оценкой, в ходе которого используются методы тестирования с использованием компьютерных технологий.

7. СПИСОК ОСНОВНОЙ ЛИТЕРАТУРЫ

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 / Бузов Г.А, Калинин СВ., Кондратьев А.В.- М.: Горячая линия - Телеком, 2005. - 416 с.
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.
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. 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.
13. Девянин П.Н., Садердинов А.А, Трайнев В.А. и др. Учебное пособие. Информационная безопасность предприятия. - М, 2006.- 335 с.

8. СПИСОК ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ

1. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности».
2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании».
4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
5. Указ Президента Российской Федерации от 16.08.2004 №1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
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».
7. Стратегия национальной безопасности Российской Федерации до 2020 года, утверждена Указом Президента Российской Федерации от 12.05.2009 № 537.
8. Доктрина информационной безопасности Российской Федерации, утверждена Президентом Российской Федерации 09.09.2000 Пр-1895.
9. Постановление Правительства Российской Федерации от 26.01.2006 № 45 «Об организации лицензирования отдельных видов деятельности».
10. Постановление Правительства Российской Федерации от 01.02.2006 №54 «О государственном строительном надзоре в Российской Федерации».
11. Постановление Правительства Российской Федерации от 03.02.2012 №79 «О лицензировании деятельности по технической защите конфиденциальной информации».
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».
13. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Гостехкомиссия России, 1992.
14. Положение о сертификации средств защиты информации по требованиям безопасности информации, утверждено приказом Гостехкомиссии России от 27.10.1995 № 199.
15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утверждены приказом Гостехкомиссии России от 30.08.2002 № 282.
16. Сборник временных методик оценки защищённости конфиденциальной информации от утечки по техническим каналам. Гостехкомиссия России, 2002.
17. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий, утвержден приказом председателя Гостехкомиссии России от 19.06.2002 № 187.
18. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся

в государственных информационных системах».
19. Приказ ФСТЭК России от 18.02.2013 № 21. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
20. «Методический документ. Меры защиты информации в государственных информационных системах», утв. ФСТЭК России 11.02.2014.
21. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 15.02.2008.
22. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 15.02.2008.
23. 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
24. 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.
25. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации, утверждён решением председателя Гостехкомиссии России от 25.07.1997.
26. 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.
27. Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования. Утверждён решением председателя Гостехкомиссии России от 25.07.1997.
28. 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.
29. ГОСТ Р 52069.0-2003 «Защита информации. Система стандартов. Основные положения».
30. ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества».
31. ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».

32. ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний».
33. 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.
34. 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.