ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ ТЮМЕНСКОЙ ОБЛАСТИ
Государственное автономное образовательное учреждение
среднего профессионального образования Тюменской области
«ЗАПАДНО-СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ КОЛЛЕДЖ»

УТВЕРЖДАЮ
Директор ГАОУ СПО ТО
«Западно-Сибирский
государственный колледж»

_____ Г. Шатохин
«____» _____ 2018 г.

М.П.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
повышения квалификации специалистов
в области информационной безопасности
по теме:

«Безопасность информационных технологий и комплексная защита персональных данных»

Тюмень – 2018

1. ВВЕДЕНИЕ

Дополнительная профессиональная программа повышения квалификации специалистов в области информационной безопасности по теме «Безопасность информационных технологий и комплексная защита персональных данных» (далее - программа) разработана с учетом требований Федерального закона от 28.12.2010 № 390-ФЗ «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», утвержденные приказом ФСТЭК России от 18.02.2013 № 21, а также документы, регламентирующие вопросы обеспечения безопасности персональных данных:

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;

При разработке программы выполнены требования Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам, утвержденного приказом Минобрнауки России от 01.07.2013 №499 и Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности, утвержденного приказом Минобрнауки России от 05.12.2013 № 1310.

Цель реализации образовательной программы: приобретение слушателями знаний и возможностей различных видов программных и программно-аппаратных средств защиты информации, практических навыков выбора рациональных вариантов и решений по их эффективному применению для противодействия угрозам безопасности автоматизированных систем, навыков обеспечения правомерности и конфиденциальности обработки персональных данных с использованием правовых, организационных и технических мер, способов снижения рисков утечки персональных данных и наложения штрафных санкций со стороны государственных надзорных органов.

Задачи образовательной программы: научить слушателей: • разрабатывать основные положения концепции построения и эффективного применения комплексных систем защиты информации в автоматизированных системах; • планировать защиту и рационально распределять соответствующие функции между подразделениями и сотрудниками предприятия, организовывать их взаимодействие на различных этапах жизненного цикла автоматизированных систем; • организовывать деятельность служб технической защиты информации в действующих и проектируемых системах защиты информации; • ориентироваться в проблемах информационной безопасности в сетях Интернет/Интранет, уязвимостях сетевых протоколов и служб, атаках в IP-сетях; • ориентироваться в средствах защиты информации от несанкционированного доступа, межсетевых экранах, средствах контроля контента, средствах анализа защищенности и средствах обнаружения атак для обеспечения информационной безопасности в IP-сетях; • организовывать поиск и использование оперативной информации о новых уязвимостях в системном и прикладном программном обеспечении, а также других актуальных для

обеспечения информационной безопасности данных; • организовать обработку персональных данных в соответствии с требованиями российского законодательства.

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

Срок обучения: 72 часа аудиторных учебных занятий.

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

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.

Дополнительная профессиональная программа рассмотрена и обсуждена на заседании педагогического совета колледжа (учебно-методического совета). Протокол (решение) № 2 от «13» февраля 2014 г.

2. ПЕРЕЧЕНЬ ТЕМ

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

3. 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/IP. Понятие программно-математического воздействия и вредоносной программы. Классификация вредоносных программ, основных деструктивных функций вредоносных программ и способов их реализации. Особенности программно-математического воздействия в сетях общего пользования. Методы и средства выявления угроз несанкционированного доступа к информации и специальных воздействий на неё. Порядок обеспечения защиты информации при эксплуатации автоматизированных систем.

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

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

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

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

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

Особенности информационного элемента информационной системы персональных данных.

Раскрытие понятия актуальных угроз безопасности персональных данных. Основные типы актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, порядок их определения. Методы и процедуры выявления угроз безопасности персональных данных в информационных системах персональных данных. Перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Классификация угроз безопасности и уязвимостей информационной системы персональных данных, а также их характеристики. Описание типовых моделей угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных, в зависимости от целей и содержания персональных данных. 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 защищенности информации, обрабатываемой основными техническими средствами и системами, от утечки за счет побочных электромагнитных излучений и наводок на вспомогательные технические средства и системы и их коммуникации.

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

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

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

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

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

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

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

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

Понятие государственной информационной системы, обрабатывающей персональные данные. Особенности защиты информации, содержащейся в государственной информационной системе персональных данных. Определение класса защищенности государственной информационной системы и необходимых мер по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

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.

4. УЧЕБНЫЙ ПЛАН ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЫ

/п	Наименование разделов и дисциплин	и	В том числе		Форма контроля
			Лекции	Практические занятия (семина	
	2		4	5	6
	Раздел № 1. Общие вопросы технической защиты информации	2	16	4(2)	
	Тема №1. Правовые и организационные основы технической защиты информации ограниченного доступа		8		
	Тема № 2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа	4	8	4(2)	Опрос на практическом занятии и семинаре

	Раздел № 2. Организация обеспечения безопасности персональных данных в информационных системах персональных данных	6	36	8(2)	
	Тема № 3.Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных	0	14	4(2)	Опрос на лекции Опрос на практическом занятии и семинаре
	Тема № 4. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	0	20		
	Тема № 5. Практические реализации типовых моделей защищенных информационных систем обработки		2	4	Опрос на практическом занятии
	персональных данных				
	Итого по видам занятий	8	52	12(4)	
	Зачет с оценкой				4
0	**Всего**	2	52	12(4)	4

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, проводится в компьютерном классе с предварительной установкой необходимого программного обеспечения в компьютерной сети. При проведении практических занятий необходимо отрабатывать задания, учитывающие специфику выполняемых функциональных обязанностей слушателями курсов по своему

профессиональному предназначению, в т.ч. предусматривать задания с проведением деловых игр (эпизодов).

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 зачет с оценкой, в процессе проведения которого применяются методы тестирования с использованием компьютерных технологий.

6. СПИСОК ОСНОВНОЙ ЛИТЕРАТУРЫ

6.1. 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.

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

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

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

6.5. 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.

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

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

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

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

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

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

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

6.13. 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 СКНЦ ВШ, 2006.

7. СПИСОК ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ

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

7.2. Федеральный закон от 27.07.2006

№ 149-ФЗ «Об информации, информационных технологиях и о защите информации».

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

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

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

7.6. 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».

7.7. Стратегия национальной безопасности Российской Федерации до 2020 года. Утверждена Указом Президента Российской Федерации от 12.05.2009 № 537.

7.8. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 09.09.2000 № Пр-1895.

7.9. Постановление Правительства Российской Федерации от 21.11.2011 № 957 «Об организации лицензирования отдельных видов деятельности».

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

7.11. Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

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

7.13. Постановление Правительства Российской Федерации от 21.03.2012 № 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 и муниципальными органами».

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

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

7.16. Положение о сертификации средств защиты информации по требованиям безопасности информации. Утверждено приказом Гостехкомиссии России от 27.10.1995 № 199.

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

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

7.19. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Утвержден приказом председателя Гостехкомиссии России от 19.06.2002 № 187.

7.20. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

7.21. 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».

7.22. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15.02.2008.

7.23. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15.02.2008.

7.24. 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.

7.25. 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.

7.26. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированногодоступа к информации. Утверждён решениемпредседателя Гостехкомиссии России от 25.07.1997.

7.27. 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.

7.28. Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования. Утверждён решением председателя Гостехкомиссии России от 25.07.1997.

7.29. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных воможностей. Утверждён приказом председателя Гостехкомиссии России от 04.06.1999 № 114.

7.30. ГОСТ Р 52069.0-2003 «Защита информации. Система стандартов. Основные положения».

7.31. ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества».

7.32. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».

7.33. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» (взамен ГОСТ Р 51275-96).

7.34. ГОСТ Р 52863-2007 «Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к намеренным силовым электромагнитным воздействиям. Общие требования».

7.35. ГОСТ Р ИСО/МЭК 15408-1-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». Часть 1. Введение и общая модель.

7.36. ГОСТ Р ИСО/МЭК 15408-2-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных

технологий». Часть 2. Функциональные требования безопасности.

7.37. ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». Часть 3. Требования доверия к безопасности.

7.38. ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».

7.39. ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методика аттестационных испытаний».

7.40. Методический документ. «Меры защиты информации в государственных информационных системах». Утвержден ФСТЭК России 11.02.2014.