Общество с ограниченной ответственностью «Учебный центр «Конус»

УТВЕРЖДАЮ
Генеральный директор
ООО «Учебный центр «Конус»

А.С. Попов

«20» декабря 2016 г.

ДОПОЛНИТЕЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
повышения квалификации специалистов по защите информации

«Комплексное обеспечение информационной безопасности»
форма подготовки - **очная**

лекции 33 (час.)
практические занятия 39 (час.)
всего часов аудиторной нагрузки 72 (час.)

Составитель:
Генеральный директор ООО «УЦ «Конус» А.С. Попов

Улан-Удэ 2016 г.

Содержание

Учебный план программы повышения квалификации специалистов по защите информации курса «Комплексное обеспечение информационной безопасности».

Цель обучения: сформировать у слушателей знания и навыки по основам обеспечения информационной безопасности, техническим мерам и организационным мероприятиям по защите информации, а также развить в процессе обучения системное мышление, необходимое для решения задач организационно-правовой защиты информации с учетом требований системного подхода. Дать слушателям теоретические и практические навыки, необходимые при разработке организационно-распорядительной документации, регламентирующие вопросы обеспечения информационной безопасности. Повысить квалификацию руководителей и специалистов подразделений по защите информации. Дать навыки применения систем и средств защиты информации при обеспечении информационной безопасности.

Категория обучаемых: Руководители и сотрудники государственных и муниципальных органов исполнительной власти, организаций различных форм собственности, физические лица, планирующие повысить свой уровень подготовки по вопросам информационной безопасности; руководители и сотрудники департаментов (отделов, служб), ответственных за администрирование IT-инфраструктуры организации и обеспечение информационной безопасности; специалисты по защите информации.

Продолжительность обучения: 72 академических часа.

Форма обучения: очная, дневная, с отрывом от работы.

Режим занятий: по 8 академических часов в день.

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Формы контроля
			Лекции	Практические занятия	
1.	Теоретические вопросы обеспечения безопасности информации	34	34		
2.	Практические вопросы обеспечения безопасности информации	33		33	
3.	Сертификационный экзамен	5		5	**зачёт**
	Итого:	**72**	**33**	**39**	

Учебно-тематический план программы повышения квалификации специалистов по защите информации курса «Комплексное обеспечение информационной безопасности».

№ п/п	Наименование разделов, дисциплин и тем	Всего часов	В том числе:		Формы контроля
			Лекции	Практические занятия	
1.	**Теоретические вопросы обеспечения безопасности информации**	**29**	**29**		
1.1	Назначение и структура обеспечения защиты информации		2		
1.2	Законодательство РФ в области защиты информации		2		
1.3	Правовые основы защиты государственной тайны		4		
1.4	Правовые основы защиты конфиденциальной информации		4		
1.5	Обзор основных нормативных и методических документов по технической защите информации		2		
1.6	Лицензирование и сертификация в сфере защиты информации		4		
1.7	Обзор методов и способов получения несанкционированного доступа к информации.		4		
1.8	Система ответственности за нарушение норм защиты информации		4		
1.9	Расследование компьютерных правонарушений		4		
1.10	Международное законодательство в области защиты информации		2		
2.	**Практические вопросы обеспечения безопасности информации**	**34**		**34**	
2.1	Обеспечение безопасности информации с использованием организационных мер			4	
2.2.	Применение технических средств обеспечения безопасности на объекте информатизации			4	
2.3	Обеспечение безопасности			4	

№ п/п	Наименование разделов, дисциплин и тем	Всего часов	В том числе:		Формы контроля
			Лекции	Практические занятия	
	информации с использованием средств защиты информации от несанкционированного доступа				
2.4	Обеспечение безопасности информации с использованием средств межсетевого экранирования			6	
2.5	Обеспечение безопасности информации с использованием средств антивирусной защиты			4	
2.6	Обеспечение безопасности информации с использованием средств криптографической защиты информации			5	
2.7	Применение средств обнаружения вторжений и средств анализа защищенности			4	
2.8.	Проведение периодического контроля, применение специализированных программных средств контроля защищенности			2	
3	**Итоговый экзамен**	**5**			**5**
	Итого:	**72**	**34**	**33**	**5**

Учебная программа программы повышения квалификации специалистов по защите информации курса «Комплексное обеспечение информационной безопасности»

Введение.

Учебная программа повышения квалификации специалистов по защите информации курса «Комплексное обеспечение информационной безопасности» (далее - Учебная программа) разработана для повышения квалификации руководителей и сотрудников государственных и муниципальных органов исполнительной власти, организаций различных форм собственности, физических лиц, планирующих повысить свой уровень подготовки по вопросам информационной безопасности; руководителей и сотрудников департаментов (отделов, служб), ответственных за администрирование IT-инфраструктуры организации и обеспечение информационной безопасности; специалистов по защите информации

Нормативная трудоемкость Учебной программы составляет 72 часа, из них 34 часа лекционные и 33 часа практические занятия.

Слушатели, полностью выполнившие программу обучения и успешно сдавшие экзамен, получают удостоверение о краткосрочном повышении квалификации установленного образца.

Поставленная цель достигается решением следующих задач:

1. изучением правовых основ обеспечения информационной безопасности;
2. изучением нормативно-методических документов ФСБ РФ, ФСТЭК РФ;
3. изучением методов и способов обеспечения защиты информации ограниченного доступа;
4. изучением организационных основ информационной безопасности;
5. изучением порядка применения сертифицированных средств защиты информации.

В результате изучения курса слушатели должны:

1. **иметь представление**:
    a. об основах правового регулирования отношений в информационной сфере;
    b. об основах правового регулирования в области информационной безопасности;
    c. о видах компьютерных преступлений;
    d. об организационном обеспечении информационной безопасности;
2. **знать:**
    a. содержание основных понятий по правовому обеспечению информационной безопасности;
    b. правовые способы защиты государственной тайны и конфиденциальной информации;
    c. понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации;
    d. основы правового регулирования взаимоотношений администрации и персонала в области защиты информации;

e. правила лицензирования и сертификации в области защиты информации;
f. виды и признаки компьютерных преступлений, особенности основных следственных действий при расследовании указанных преступлений.

3. **уметь**:
   a. находить необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;
   b. применять действующую законодательную базу в области информационной безопасности;
   c. разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов.
4. **владеть навыками**:
   a. работы с нормативно-правовыми актами;
   b. выявления угроз информационной безопасности объекта;
   c. обеспечения информационной безопасности на объекте информатизации.

Содержание программы

Раздел 1. Теоретические вопросы правового обеспечения информационной безопасности.

Тема 1. Назначение и структура обеспечения защиты информации

Предмет, задачи и содержание курса. Терминология курса. Место курса среди других дисциплин. Структура курса. Методика аудиторной и самостоятельной работы студентов по изучению курса. Законодательные и нормативные источники. Научная и учебная литература. Периодические издания.

Тема 2. Законодательство РФ в области информационной безопасности

Понятие и структура информационной безопасности. Информационная сфера и информационная среда. Субъекты и объекты правоотношений в области информационной безопасности. Понятие и виды защищаемой информации по законодательству РФ. Отрасли законодательства, регламентирующие деятельность по защите информации. Перспективы развития законодательства в области информационной безопасности.

Тема 3. Правовые основы защиты государственной тайны

Понятие правового режима защиты государственной тайны. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Реквизиты носителей сведений, составляющих государственную тайну. Принципы, механизм и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Порядок допуска и доступа к государственной тайне. Иные меры по обеспечению сохранности сведений, составляющих государственную тайну (режим секретности как основной порядок деятельности в сфере защиты государственной тайны). Перечень и содержание организационных мер, направленных на защиту государственной тайны. Система контроля за состоянием защиты государственной тайны. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная).

Тема 4. Правовые основы защиты конфиденциальной информации

Виды конфиденциальной информации: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна. Понятие коммерческой тайны. Правовое обеспечение защиты коммерческой тайны. Сведения составляющие коммерческую тайну Правовые режимы конфиденциальной информации: содержание и особенности. Основные требования, предъявляемые к организации защиты конфиденциальной информации.. Правовые аспекты защиты информации, циркулирующей в телефонных и других линиях и системах связи. Защита КТ при хранении и обработке информации в автоматизированных системах. Правовое регулирование отношений предприятия с другими предприятиями, организациями и гражданами по защите коммерческой тайны.

Тема 5. Обзор основных нормативных и методических документов по технической защите информации

Классификация нормативных и методических документов по технической защите информации. Обзор требований НМД по обеспечению безопасности информации в различных сферах деятельности. Правовые основы организации и регулирования деятельности структурных подразделений предприятия, обеспечивающих его безопасность. Правовое регулирование использования технических средств защиты информации и противодействия угрозам информационной безопасности.

Тема 6. Лицензирование и сертификация в информационной сфере

Правовая основа системы лицензирования и сертификации в РФ. Виды деятельности в информационной сфере, подлежащие лицензированию. Лицензирование деятельности по защите информации. Объекты лицензирования в сфере защиты информации. Участники лицензионных отношений в сфере защиты информации. Органы лицензирования и их полномочия.

Понятие сертификации по российскому законодательству. Правовая регламентация сертификационной деятельности в области защиты информации. Режимы сертификации. Объекты сертификационной деятельности (сертификации). Органы сертификации и их полномочия. Лицензирование и сертификация в области международного информационного обмена.

Тема 7. Обзор методов и способов получения несанкционированного доступа к информации.

Обзор основных методов и способов получения несанкционированного доступа к информации. Технические средства негласного съема информации. Прослушивание помещений с помощью технических средств. Оптический (визуальный) канал утечки информации. Основные угрозы информации при ее передаче по каналам связи общего пользования. Реализация угроз безопасности информации при непосредственном доступе к техническим средствам обработки информации.

Тема 8. Система ответственности за нарушение норм защиты информации

Нормы ответственности за правонарушения в информационной сфере. Виды и условия применения правовых норм уголовной, гражданско-правовой, административной и дисциплинарной ответственности за разглашение защищаемой информации и невыполнение правил ее защиты. Понятие оперативно-розыскной деятельности и оперативно-розыскных мероприятий по законодательству РФ. Органы, уполномоченные на осуществление оперативно-розыскной деятельности. Система правовых актов, регулирующих проведение оперативно-розыскных мероприятий. Защита информации от неправомерных действий органов, занимающихся оперативно-розыскной деятельностью. Защита коммерческой информации от неправомерных действий контролирующих и правоохранительных органов.

Тема 9. Расследование компьютерных правонарушений

Преступления в сфере компьютерной информации. Признаки и элементы состава преступления. Криминалистическая характеристика компьютерных

преступлений. Расследование компьютерного преступления. Особенности основных следственных действий. Криминалистические аспекты проведения расследования Сбор доказательств. Экспертиза преступлений в области компьютерной информации. Проблемы судебного преследования за преступления в сфере компьютерной информации.

Тема 10. Международное законодательство в области защиты информации

Законодательство зарубежных стран в области защиты интеллектуальной собственности. Международные договоры и конвенции в области защиты информации Законодательство в области международного информационного обмена и компьютерных преступлений. Международный правовой опыт обеспечения безопасности негосударственных объектов экономики.

Раздел 2. Практические вопросы правового обеспечения информационной безопасности.

Тема 1. Обеспечение безопасности информации с использованием организационных мер.

Перечень и содержание организационных мер, направленных на защиту конфиденциальной информации и государственной тайны. Основные локальные нормативные правовые акты в организации по обеспечению режима безопасности информации. Система контроля за состоянием защиты информации в организации. Юридическая ответственность за нарушения правового режима защиты информации ограниченного доступа в организации (уголовная, административная, дисциплинарная).

Тема 2. Применение технических средств обеспечения безопасности на объекте информатизации.

Основные способы защиты информации с использованием технических средства. Технические средства защиты от негласного съема информации. Средства защиты информации от утечки по акустическому и виброакустическому каналу. Защита оптического (визуального) канала от утечки информации. Технические средства защиты телефонных каналов.

Тема 3. Обеспечение безопасности информации с использованием средств защиты информации от несанкционированного доступа.

Программные средства защиты информации от несанкционированного доступа. Аппаратные и аппаратно-программные модули доверенной загрузки. Электронные ключи и идентификаторы.

Тема 4. Обеспечение безопасности информации с использованием средств межсетевого экранирования.

Классификация средств межсетевого экранирования. Программные и программно-аппаратные средства межсетевого экранирования. Особенности применения. Типовые настройки правил фильтрации межсетевых экранов.

Тема 5. Обеспечение безопасности информации с использованием средств антивирусной защиты.

Классификация средств антивирусной защиты. Программные и программно-аппаратные средства антивирусной защиты. Настройки и применение групповых политик антивирусной защиты в локальных и распределенных сетях.

Тема 6. Обеспечение безопасности информации с использованием средств криптографической защиты информации.

Защита информации от несанкционированного доступа с использованием средств шифрования. Защита каналов связи. Особенности использования технологий VPN и SSL для защиты каналов связи.

Тема 7. Применение средств обнаружения вторжений и средств анализа защищенности

Защита от угроз безопасности информации при межсетевом взаимодействии. Средства обнаружения вторжений. Средства анализа защищенности, сетевые сканеры.

Тема 8. Проведение периодического контроля, применение специализированных программных средств контроля защищенности.

Порядок проведения периодического контроля в организации. Ведение журналов учета. Проведение инструктажа пользователей по требованиям безопасности.

Методические рекомендации по реализации образовательной программы.

Обучение слушателей по настоящей образовательной программе направлено на выработку у них навыков работы с нормативно-правовыми актами, навыков выявления и предотвращения угроз информационной безопасности объекта.

Подготовку слушателей проводить по очной форме (с отрывом от работы) в составе учебной группы. Численность группы - до 10 человек.

Общий объем учебной нагрузки в день - 8 учебных часов. Продолжительность двух учебных часов - 1 час 30 минут.

В качестве материальной базы использовать учебно-методическое обеспечение и компьютерное оборудование ООО «Учебный центр «Конус».

По окончании обучения провести итоговый экзамен в форме тестирования, являющийся заключительным этапом изучения настоящей образовательной программы и имеющий цель проверить и оценить уровень полученных знаний, навыки и умения применить полученные знания в решении практических задач.

На сдачу экзамена планировать по 5 часов на учебную группу. Вопросы для проведения экзамена утвердить руководителем ООО «Учебный центр «Конус».

В тест включить 100 (сто) вопросов.

В основу подготовки специалистов положить изучение теоретических и практических вопросов обеспечения организационно-правовых требований к обеспечению информационной безопасности, основываясь при этом на требованиях норм российского законодательства, подзаконных актах, методических и руководящих документах контролирующих органов.

При подготовке специалистов большое внимание уделить четкому уяснению их полномочий и практических действий в вопросах обеспечения организационно-правовых требований информационной безопасности, строгому следованию требованиям законодательства Российской Федерации.

Использовать следующие основные виды учебных занятий: лекцию, практическое (лабораторное) занятие, самостоятельную подготовку.

На лекциях давать основы знаний по изучаемым вопросам, детально изучать теоретические вопросы применения норм Российского законодательства к обеспечению информационной безопасности объекта. В ходе занятий раскрывать наиболее сложные вопросы учебного материала, уделяя особое внимание их творческому осмыслению. К чтению лекций приказом руководителя ООО «Учебный центр «Конус» допускать преподавателей, имеющих соответствующую квалификацию. Лекции проводить методом рассказа, рассказа-показа.

На практических (лабораторных) занятиях давать слушателям практические навыки разработки документов, регламентирующих вопросы обеспечения информационной безопасности объекта. Для повышения эффективности практических занятий преподавателю необходимо заранее выдавать слушателям задания на практические занятия. На данных занятиях требуется создавать учебную обстановку для решения практических задач слушателями в определенной должности. В целях интенсификации обучения на заключительном этапе занятия учебную группу можно делить на подгруппы. Некоторые занятия проводить в

форме тренировок, главным содержанием которых является практическая работа каждого слушателя.

При изучении отдельных вопросов допускать обсуждение, обмен мнениями по существу рассматриваемого вопроса. Всемерно поощрять и развивать активность слушателей, учить их самостоятельно анализировать и объективно оценивать сущность вопроса, проблемы.

Методические и практические навыки слушателям прививать и совершенствовать на протяжении всего периода обучения, на всех теоретических и практических занятиях и в часы самостоятельной подготовки. В процессе практического обучения особое внимание уделять формированию и развитию у слушателей практических умений и навыков.

На практических (лабораторных) занятиях отводить время для проверки знаний и навыков слушателей по пройденному материалу и усвоению изучаемой темы.

Текущий контроль должен охватывать как можно большее число слушателей с обязательной оценкой их знаний, умений и навыков. Он должен стимулировать учебную работу слушателей и проводиться в форме, избранной преподавателем или предусмотренной рабочей программой.

Для достижения высокой методической подготовки специалистов предъявлять высокую требовательность к организации каждого занятия, использовать образцовую методику проведения занятий и самостоятельное проведение слушателями практических занятий по изучаемым темам.

В целях повышения эффективности учебного процесса широко использовать схемы, макеты, реальные аппаратные и программные средства и другие наглядные пособия.

Самостоятельную подготовку использовать для закрепления и углубления знаний, полученных слушателями на всех видах учебных занятий. Индивидуальные и групповые консультации проводить преподавателями в целях оказания помощи слушателям при их подготовке к практическим занятиям, экзамену.

Для предупреждения в ходе занятий несчастных случаев при работе на действующей аппаратуре в начале занятий со слушателями изучать правила техники безопасности и принимать зачет. Преподавателю в ходе занятий строго контролировать соблюдение слушателями установленных правил техники безопасности. Неподготовленных слушателей к занятиям не допускать. В ходе занятий преподавателю нести личную ответственность за правильное использование оборудования, приборов и соблюдение мер техники безопасности слушателями.

Руководство обучением должно быть конкретным и обеспечивать полное и качественное выполнение настоящей образовательной программы.

Форма итогового контроля: Экзамен в форме теста.

Условия реализации образовательной программы.

В целях реализации настоящей образовательной программы составляется рабочая программа, на базе которой и с учетом располагаемой и используемой учебно-материальной базы будет осуществляться обучение специалистов.

При составлении рабочей программы разрешается:

1. изменять объем часов, отводимых на освоение учебного материала в соответствии с Учебной программой в пределах не более чем на 15% для отдельных тем при условии сохранения содержания, предусмотренного Учебной программой;
2. устанавливать количественный состав обучаемых при проведении практических занятий;
3. определять необходимую глубину преподавания отдельных тем в соответствии имеющимся профессиональным уровнем подготовки обучаемых;
4. распределять часы внеаудиторной (самостоятельной) работы путем составления план-графика проведения внеаудиторной работы.

Список литературы.

Правовые и нормативно-методические документы

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
3. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»;
4. Федеральный закон Российской Федерации от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;
5. Федеральный закон Российской Федерации от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи»;
6. Постановление Правительства Российской Федерации от 08 сентября 2010 года № 697 «О единой системе межведомственного электронного взаимодействия»;
7. Постановление Правительства Российской Федерации от 02 октября 2009 года № 1403-р «Технические требования к организации взаимодействия системы межведомственного электронного документооборота с системами электронного документооборота федеральных органов исполнительной власти»;
8. Постановление Правительства Российской Федерации от 22 сентября 2009 года № 754 «Об утверждении положения о системе межведомственного электронного документооборота»;
9. Постановление Правительства Российской Федерации от 07 июля 2011 года № 552 «О порядке предоставления федеральным органам исполнительной власти и государственными внебюджетными фондами доступа к своим информационным системам в части информации, необходимой для выпуска, выдачи и обслуживания универсальных электронных карт»;
10. Постановление правительства Российской Федерации от 09 февраля 2012 года № 111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи»;
11. Постановление правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
12. Постановление Правительства Российской Федерации от 3 ноября 1994 года № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного доступа в федеральных органах исполнительной власти»;

13. Постановление Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
14. Постановление Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
15. Постановление Правительства Российской Федерации от 18 мая 2009 года № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным системам»;
16. Указ Президента Российской Федерации от 17 марта 2008 года № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
17. Указ Президента Российской Федерации от 15января 2013 года № 31с «О создании Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;
18. Указ Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении сведений конфиденциального характера»;
19. Приказ Министерства связи и массовых коммуникаций Российской Федерации от 27 декабря 2009 года № 190 «Об утверждении Технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия»;
20. Приказ Федеральной службы охраны Российской Федерации от 07 августа 2009 года № 487 «Об утверждении положения о сегменте информационно-телекоммуникационной сети интернет для федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации»;
21. Приказ Министерства связи и массовых коммуникаций Российской Федерации от 25 августа 2009 года № 104 «Об утверждении требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования»;
22. Совместный приказ от 31 августа 2010 года ФСБ России № 416 и ФСТЭК России № 489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»;
23. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
24. Приказ ФСТЭК России от 12 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

25. Приказ Гостехкомиссии России от 30 августа 2002 г. № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»;
26. Приказ ФАПСИ России от 13 июня 2001 года № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
27. Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и использовании шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
28. Приказ 8 центра ФСБ России от 21 февраля 2008 года № 149/54-144 «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации»;
29. Приказ 8 центра ФСБ России от 21 февраля 2008 года № 149/6/6-622 «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»
30. Руководящий документ ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
31. Руководящий документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
32. Руководящий документ ФСТЭК России от 18 мая 2007 года «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры»;
33. Руководящий документ ФСТЭК России от 18 мая 2007 года «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры»;
34. Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»;
35. Информационное сообщение ФСТЭК России от 20 ноября 2012 года № 240/24/4669 «Об особенностях защиты персональных данных при их обработке в информационных системах персональных данных и сертификации средств защиты информации, предназначенных для защиты персональных данных»;
36. «Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам»;

Основная литература.

1. «Безопасность сетей. Полное руководство» Издательство: Эком 2006 г;
2. «Защита информации в компьютерных системах и сетях» Издательство: ДМК Пресс 2012 г;
3. «Защита компьютерной информации» Издательство: Книга по Требованию 2010 г;
4. «Защита от взлома: сокеты, эксплойты, shell-код: выявление уязвимостей операционных систем и прикладных программ к атакам хакеров» Издательство: Книга по Требованию 2006 г;
5. «Информационная безопасность» Издательство: Академия 2012 г;
6. «Информационная безопасность и защита информации» Издательство: ТНТ 2010 г;
7. «Информационная безопасность. Защита и нападение» Издательство: ДМК Пресс 2012 г;
8. «Как защитить компьютер на 100%» Издательство: Питер 2014 г;
9. «Комплексная защита информации на предприятии» Издательство: Городец 2008 г;
10. «Комплексная система защиты информации на предприятии» Издательство: Академия 2009 г;
11. «Мониторинг и анализ сетей. Методы выявления неисправностей» Издательство: Лори 2012 г;
12. «Обеспечение защиты персональных данных» Издательство: 1С-Паблишинг 2010г;
13. «Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий» Издательство: Высшая Школа Экономики (Государственный Университет) 2011г;
14. «Основы программно-аппаратной защиты информации» Издательство: Либроком 2013г;
15. «Особенности защиты персональных данных в трудовых отношениях» Издательство: Либроком 2012г;
16. «Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 640-816» Издательство: Вильямс 2013г;
17. «Правовая защита информации в коммерческих организациях» Издательство: Академия 2009г;
18. «Практическое руководство по выявлению специальных технических средств несанкционированного получения информации» Издательство: Горячая Линия – Телеком 2010г;
19. «Проектирование и внедрение компьютерных сетей» Издательство: БХВ-Петербург 2004г;
20. «Расследование компьютерных преступлений» Издательство: Лори 2012г;
21. «Теория защиты информации» Издательство: Телеком 2012г;
22. «Управление рисками и безопасностью» Издательство: Ленанд 2010г;
23. «Управление рисками и безопасностью» Издательство: Ленанд 2009г;
24. «Управление рисками информационной безопасности» Издательство Горячая Линия – Телеком 2014г.

Дополнительная литература

1. «Безопасность сетей. Полное руководство» Издательство: Эком 2006 г;
2. «Защита информации в компьютерных системах и сетях» Издательство: ДМК Пресс 2012 г;
3. «Комплексная защита информации на предприятии» Издательство: Городец 2008 г;
4. «Комплексная система защиты информации на предприятии» Издательство: Академия 2009 г;
5. «Мониторинг и анализ сетей. Методы выявления неисправностей» Издательство: Лори 2012 г;
6. «Основы программно-аппаратной защиты информации» Издательство: Либроком 2013г;
7. «Практическое руководство по выявлению специальных технических средств несанкционированного получения информации» Издательство: Горячая Линия – Телеком 2010г;
8. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей» Издательство: Академия 2006г;
9. «Проектирование и внедрение компьютерных сетей» Издательство: БХВ-Петербург 2004г.