Министерство образования и науки Российской Федерации

ГОУВПО «Сыктывкарский государственный университет»

«УТВЕРЖДАЮ»

Ректор ГОУВПО «Сыктывкарский государственный университет»

_____ В.Н.Задорожный

«09» декабря 2010 г.

УЧЕБНАЯ ПРОГРАММА

«Организационно-правовое обеспечение защиты персональных данных»

г. Сыктывкар

2010

1. ВВЕДЕНИЕ

Образовательная программа «Организационно-правовое обеспечение защиты персональных данных» разработана в соответствии с правовыми и нормативными документами в области информационной безопасности, введенными в действие указами Президента Российской Федерации и Постановлениями Правительства Российской Федерации. Основой для разработки программы являются документы, регламентирующие вопросы защиты 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», утвержденные 15.02.2008 ФСТЭК России, Приказ ФСТЭК России от 5 февраля 2010 г. N 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных».

При разработке программы выполнены требования к содержанию дополнительных профессиональных программ, утвержденные приказом Министерства образования России от 18.06.1997 № 1221.

Программа рассмотрена и одобрена на заседании учебно-методической комиссии факультета информационных систем и технологий с участием кафедры защиты информации 08.12.2010 (Протокол № УМК-04-10/11).

Цель обучения по программе: обеспечить слушателей теоретическими и практическими знаниями организации и проведения работ по обеспечению безопасности персональных данных.

Поставленная цель обучения достигается решением следующих задач:

- изучением правовых и организационных основ обеспечения безопасности ПДн в ИСПДн;
- определение актуальности угроз безопасности ПДн в ИСПДн;
- практической отработкой порядка проведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн.

Категория слушателей: специалисты, осуществляющие работу с персональными данными, юристы, работники кадровых служб, делопроизводители, бухгалтера.

Срок обучения: 72 часа

Форма обучения: с отрывом от производства (очная).

Режим занятий: 32 часа самостоятельной работы и 5 дней по 8 часов аудиторной учебной работы под руководством преподавателя.

Виды занятий: самостоятельная подготовка – 32 ауд.ч.

лекции – 26 ауд.ч.

практические занятия – 8 ауд.ч.

семинарские занятия – 2 ауд.ч

зачётное занятие – 4 ауд.ч.

В результате изучения курса слушатели должны:

быть ознакомленными:

- с концептуальными основами защиты информации в стране;
- с лицензированием деятельности в области защиты информации;
- с документами национальной системы стандартизации, действующими в области защиты информации.

знать:

- основные виды угроз безопасности ПДн;
- содержание и порядок организации работ по выявлению угроз безопасности ПДн;
- содержание основных нормативных актов, регламентирующих порядок организации работ по обеспечению безопасности ПДн;
- порядок организации мероприятий по созданию системы защиты персональных данных;
- организацию контроля и оценки степени безопасности ПДн при их обработке в ИСПДн.

уметь:

- планировать организацию мероприятий по обеспечению защиты ПДн;
- разрабатывать необходимые документы в интересах организации работ по защите ПДн;
- производить категорирование ПДн и обосновывать требования по защите информации в ИСПДн.

иметь навык:

- применения организационных мер и программно-аппаратных средств обеспечения безопасности ПДн при их обработке в ИСПДн от несанкционированного доступа (далее - НСД).

2. Перечень тем

№	Наименование тем
1.	**Правовые основы обеспечения защиты персональных данных (ПДн)**
1.1	Законодательство РФ в области защиты ПДн
1.2	Основные понятия, используемые в Законе РФ «О персональных данных» и Трудовом кодексе РФ. Ответственность за нарушение законодательства в области защиты ПДн
1.3	Правовой статус Уполномоченного органа по защите прав субъектов ПДн
2.	**Организация мероприятий по обеспечение защиты персональных данных**
2.1	Порядок отнесения сведений к персональным данным
2.2	Классификация информационных систем персональных данных
2.3	Разрешительная система доступа к ПДн
2.4	Система физической защиты объектов. Организация охраны, пропускного и внутриобъектового режима
2.5	Разработка (проектирование) системы защиты персональных данных (далее – СЗПДн). Организация контроля за обеспечением уровня защищенности персональных данных.
2.6	Разработка внутренних нормативных документов по обеспечению защиты ПДн
2.7	Организация делопроизводства с документами ограниченного доступа
3.	**Техническая защита персональных данных**
3.1	Модель угроз безопасности ПДн при их обработке в ИСПДн
3.2	Методы и способы защиты информации в ИСПДн
3.3	Нормативные документы предприятия по обеспечению безопасности ПДн при их обработке в автоматизированных системах

3. РЕФЕРАТИВНОЕ ОПИСАНИЕ ТЕМ

Раздел 1. Правовые основы обеспечения защиты персональных данных (ПДн).

Тема 1. Законодательство РФ в области защиты ПДн.

Концептуальные основы информационной безопасности в РФ. Роль и место ПДн в общей системе национальной безопасности РФ. Защита ПДн как реализация конституционных прав граждан на неприкосновенность частной жизни. Законодательные и иные правовые акты, регламентирующие защиту ПДн в РФ.

Структура, задачи и функции государственной системы защиты ПДн. Лицензирование деятельности по ТЗИ.

Тема 2. Основные понятия, используемые в Законе РФ «О персональных данных» и Трудовом кодексе РФ. Ответственность за нарушение законодательства в области защиты ПДн.

Основные понятия. Содержание категории «персональные данные». Информационные системы персональных данных (далее – ИСПДн). Область применения закона. Ограничения.

Обработка персональных данных. Принципы обработки ПДн.

Условия обработки ПДн. Согласие субъекта. Права субъектов ПДн и их соблюдение при обработке. Обязанности оператора ПДн в ходе сбора и обработки ПДн, ответы на запросы субъектов. Прекращение обработки. Обработка биометрических данных.

Обработка ПДн третьим лицом в интересах оператора. Трансграничная передача ПДн. Особенности обработки ПДн в государственных или муниципальных ИСПДн.

Требования Трудового кодекса РФ по защите ПДн.

Ответственность за нарушение законодательства в области защиты ПДн.

Тема 3. Правовой статус Уполномоченного органа по защите прав субъектов ПДн.

Нормативные документы Роскомнадзора. Реестр операторов. Проведение контрольно-надзорных мероприятий.

Раздел 2. Организация мероприятий по обеспечение защиты персональных данных.

Тема 1. Порядок отнесения сведений к персональным данным.

Составление перечня персональных данных, как составной части перечня конфиденциальных сведений. Сведения, которые не могут быть отнесены к конфиденциальной информации.

Права собственников информации в связи с ограничением её распространения. Распоряжение конфиденциальными сведениями. Передача персональных данных другим организациям. Трансграничная передача ПДн.

Тема 2. Классификация информационных систем персональных данных.

Классификация информационных систем персональных данных.

Нормативная база классификации ИСПДн. Критерии классификации ИСПДн. Классы ИСПДн. Порядок проведения классификации ИСПДн и её документального оформления. Подклассы ИСПДн.

Тема 3. Разрешительная система доступа к ПДн.

Порядок разграничения прав доступа к ПДн. Порядок оформления разрешения на доступ к ПДн и его снятие. Ограничение прав лиц, допущенных к закрытой информации.

Организация доступа к ПДн.

Тема 4. Система физической защиты объектов. Организация охраны, пропускного и внутриобъектового режима.

Система физической защиты объектов. Организация охраны, пропускного и внутриобъектового режима. Разработка нормативных документов по организации пропускного и внутриобъектового режима, на случай ЧС.

Тема 5. Разработка (проектирование) системы защиты персональных данных (далее – СЗПДн). Организация контроля за обеспечением уровня защищенности персональных данных.

Создание подразделения по защите информации или приказ о назначении ответственных за реализацию и контроль системы защиты на предприятии. Требования Федерального закона от 27.07.2006 № 152-ФЗ и Постановления Правительства РФ от 17.11.2007 № 781 к обеспечению безопасности ПДн. Обязательные механизмы защиты. Основные принципы построения СЗПДн.

Меры защиты и основные принципы обеспечения безопасности информации. Достоинства и недостатки различных видов мер защиты.

Определение структуры, состава и основных функций СЗПДн.

Общий порядок организации обеспечения безопасности ПДн в ИСПДн.

Оптимизация состава ПДн, и процессов их обработки.

Оценка достаточности и обоснованности запланированных мероприятий.

Виды, формы и способы контроля защиты ПДн в ИСПДн. Планирование работ по контролю состояния защиты ПДн в ИСПДн. Основные вопросы, подлежащие проверке (анализу) при контроле состояния организации защиты ПДн.

Тема 6. Разработка внутренних нормативных документов по обеспечению защиты ПДн.

Разработка организационно-распорядительной документации, регламентирующей вопросы организации обеспечения безопасности ПДн.

Тема 7. Организация делопроизводства с документами ограниченного доступа.

Назначение, задачи и организация конфиденциального делопроизводства. Требования государственных стандартов по оформлению документов. Размножение, учет и уничтожение документов, содержащих персональные данные.

Раздел 3. Техническая защита персональных данных.

Тема 1. Модель угроз безопасности ПДн при их обработке в ИСПДн

Нормативная база. Понятие «безопасности информации», «угрозы безопасности информации», «уязвимости», «источника угрозы». Целостность, конфиденциальность и доступность информации. Классификационная схема угроз безопасности информации и их общая характеристика.

Характеристика основных угроз НСД и моделей нарушителя безопасности информации, а также способов реализации этих угроз.

Понятие модели угроз ПДн и модели нарушителей.

Тема 2. Методы и способы защиты информации в ИСПДн.

Основные методы и способы защиты информации (средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных и т.д.). Порядок обеспечения защиты информации при эксплуатации автоматизированных систем.

Тема 3. Нормативные документы предприятия по обеспечению безопасности ПДн при их обработке в автоматизированных системах.

Инструкции пользователей АС, система учета МНИ, порядок уничтожения информации с МНИ и т.д.

4. НАИМЕНОВАНИЕ ВИДОВ ЗАНЯТИЙ ПО ТЕМАМ

Тема №	Наименование разделов и дисциплины	Всего часов	В том числе			
			Лекции	ПЗ	СЗ	Самоподготовка
1.	**Правовые основы обеспечения защиты персональных данных (ПДн).**	**22**	**2**			**20**
1.1	Законодательство РФ в области защиты ПДн.	**6**				6
1.2	Основные понятия, используемые в Законе РФ «О персональных данных» и Трудовом кодексе РФ. Ответственность за нарушение законодательства в области защиты ПДн.	**10**				10
1.3	Правовой статус Уполномоченного органа по защите прав субъектов ПДн.	**6**	2			4
2.	**Организация мероприятий по обеспечение защиты персональных данных**	**32**	**16**	**6**	**2**	**8**
2.1	Порядок отнесения сведений к персональным данным.	**4**	2			2
2.2	Классификация информационных систем персональных данных.	**4**	2			2
2.3	Разрешительная система доступа к ПДн.	**4**	2	2		
2.4	Система физической защиты объектов. Организация охраны, пропускного и внутриобъектового режима.	**2**	2			
2.5	Разработка (проектирование) системы защиты персональных данных (далее – СЗПДн). Организация контроля за обеспечением уровня защищенности персональных данных.	**6**	2		2	2
2.6	Разработка внутренних нормативных документов по обеспечению защиты ПДн.	**6**	2	2		2
2.7	Организация делопроизводства с документами ограниченного доступа.	**6**	4	2		
3.	**Техническая защита персональных данных**	**14**	**4**	**4**	**2**	**4**
3.1	Модель угроз безопасности ПДн при их обработке в ИСПДн.	**6**	2	2		2
3.2	Методы и способы защиты информации в ИСПДн.	**6**	2		2	2
3.3	Нормативные документы предприятия по обеспечению безопасности ПДн при их обработке в автоматизированных системах.	**2**		2		
	Итого занятий	**68**	**22**	**10**	**4**	**32**
	Итоговая аттестация(входной и выходной контроль)	**4**				
	ИТОГО	**72**				

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО РЕАЛИЗАЦИИ **УЧЕБНОЙ ПРОГРАММЫ**

Слушателям курсов до начала обучения направляются учебно-методические рекомендации по самостоятельному изучению первой, второй и третьей темы раздела 1 программы и некоторой части тем второго раздела программы.

Перед началом обучения проводится входной контроль слушателей в форме тестирования на проверку знаний, полученных в результате самоподготовки. Слушатели, получившие зачет, допускаются для дальнейшего изучения программы курсов повышения квалификации. Слушатели, не получившие зачет, отчисляются.

В процессе изучения данной программы необходимо использовать действующие законодательные акты в области защиты ПДн в ИСПДн, 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 ПДн в ИСПДн. Часть лекций может излагаться проблемным методом с привлечением слушателей для решения сформулированной преподавателем проблемы.

На практические занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений.

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 ИСПДн и набором конкретных действий, существенных для определенных категорий обучаемых, объединенных в соответствующую подгруппу.

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.

Примерные темы семинарских занятий:

- Проектирование системы защиты персональных данных;

- Порядок обеспечения защиты информации при эксплуатации автоматизированных систем;

- Организационные мероприятия по обеспечению безопасности ПДн при их обработке в ИСПДн.

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

6. СПИСОК ОСНОВНОЙ ЛИТЕРАТУРЫ

6.1. Закон Российской Федерации от 05.03.1992 № 2446-1 «О безопасности».

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

6.3. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании» (в ред. Федерального закона от 09.05.2005 № 45-ФЗ)

6.4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (в ред. Федеральных законов от 25.11.2009 № 266-ФЗ, от 27.12.2009 № 363-ФЗ)

6.5. Указ Президента Российской Федерации от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» (в ред. Указов Президента РФ от 22.03.2005 № 330, от 20.07.2005 № 846, от 30.11.2006 № 1321; от 23.10.2008 № 1517, от 17.11.2008 № 1625).

6.6. Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» (в ред. Указа Президента РФ от 21.10.2008 № 1510).

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

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

6.9. Постановление Правительства Российской Федерации от 26.01.2006 № 45 «Об организации лицензирования отдельных видов деятельности» (в ред. Постановлений Правительства РФ от 05.05.2007 № 269, от 03.09.2007 № 556, от 02.10.2007 № 634, от 07.04.2008 № 241, от 12.06.2008 № 452, от 27.06.2008 № 478, от 12.08.2008 № 599, от 07.11.2008 № 821, от 27.01.2009 № 50)

6.10. Постановление Правительства Российской Федерации от 01.02.2006 № 54 «Об утверждении Положения об осуществлении государственного строительного надзора в Российской Федерации».

6.11. Постановление Правительства Российской Федерации от 15.08.2006 № 504 «О лицензировании деятельности по технической защите конфиденциальной информации».

6.12. Постановление Правительства Российской Федерации от 31.08.2006 № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

6.13. Постановление Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

6.14. Постановление Правительства Российской Федерации от 06.07.2006 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

6.15. Постановление Правительства Российской Федерации от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

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

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

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

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

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

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

6.22. Приказ ФСТЭК России, ФСБ России и Минпромсвязи России от 13.02.2008 № 55/86/20 «Порядок проведения классификации информационных систем персональных данных».

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

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

6.25. Приказ ФСТЭК России от 5 февраля 2010 г. N 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных». Зарегистрирован в Минюсте РФ 19 февраля 2010 г. N 16456.

6.26. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссия России от 30.03.1992.

6.27. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автомати-

зированных систем и требования по защите информации. Утвержден решением председателя Гостехкомиссии России от 30.03.1992.

6.28. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссии России от 25.07.1997.

6.29. 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. Утвержден решением председателя Гостехкомиссии России от 30.03.1992.

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

6.31. Руководящий документ. Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден приказом председателя Гостехкомиссии России от 04.06.1999 №114.

6.32. ГОСТ Р52069.0-2003 Защита информации. Система стандартов. Основные положения.

6.33. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества.

6.34. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

6.35. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы воздействующие на информацию. Общие положения.

6.36. ГОСТ Р 52863-2007. Защита информации. Автоматизированные системы в защищённом исполнении. Испытания на устойчивость к намеренным силовым электромагнитным воздействиям. Общие требования.

6.37. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель (на основе прямого применения международного стандарта ИСО/МЭК 15408:99).

6.38. ГОСТ Р ИСО/МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий Часть 2. Функциональные требования безопасности (на основе прямого применения международного стандарта ИСО/МЭК 15408:99).

6.39. ГОСТ Р ИСО/МЭК 15408-3-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности (на основе прямого применения международного стандарта ИСО/МЭК 15408:99).

7. СПИСОК ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ

7.1. Белов Е.Б., Основы информационной безопасности: Учебное пособие./ Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. - М.: Горячая линия - Телеком, 2005.

7.2. Бузов Г.А. Защита от утечки информации по техническим каналам: Учебное пособие./ Бузов Г.А., Калинин С.В., Кондратьев А.В.- М.: Горячая линия – Телеком, 2005.

7.3. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994. - Книга 1 и 2.

7.4. Герасименко В.А., Основы защиты информации. -/Герасименко В.А., Малюк А.А., М.: МОПО РФ-МИФИ, 1997.

7.5. 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, 2004.

7.6. Малюк А.А. Введение в защиту информации в автоматизированных системах: Учебное пособие для вузов / Малюк А.А., Пазизин С.В., Погожин Н.С.- М.: Горячая линия – Телеком, 2004.

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

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

7.9. Хорев А.А. Защита информации от утечки по техническим каналам: Учеб. Пособие. М.: МО РФ, 2006.

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

7.11. 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.

7.12. Будников С.А., Паршин Н.В. Информационная безопасность автоматизированных систем: Учебное пособие – Воронеж, ЦПКС ТЗИ, 2009.

7.13. Мельников В.В. Защита информации в компьютерных системах. - М.,1997.

7.14. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа.- С.-П.,2004.

7.15. Петраков А.В. Основы практической защиты информации. Учебное пособие.- М.,2005.

7.16. Девянин П.Н., Садернинов А.А., Трайнев В.А. и др. Учебное пособие. Информационная безопасность предприятия. - М.,2006.