ИНСТИТУТ ЗАКОНОВЕДЕНИЯ И УПРАВЛЕНИЯ ВПА

КАФЕДРА ПРИКЛАДНОЙ ИНФОРМАТИКИ И
ПРОФЕССИОНАЛЬНО-ПРИКЛАДНЫХ ДИСЦИПЛИН

МЕТОДИЧЕСКИЕ И ИНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки: 38.03.02 Менеджмент
(квалификация (степень): «бакалавр»)

СОДЕРЖАНИЕ

ТЕМАТИЧЕСКИЙ ПЛАН

по дисциплине
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
для студентов
очной формы обучения

№ п/п	Наименование разделов и тем	Всего часов	Кол-во аудиторных часов			Самостоят. работа	Формируемые компетенции	**Интерактив**
			Всего	Кол-во часов по видам занятий				
				Лекции	Практ. занятия			
	Раздел 1. Основные понятия и определения, эволюция подходов к обеспечению ИБ.							
1	1.1. Информация. Информационная сфера. Информационная безопасность.	8	2	2		6	ОПК-7	
2	1.2. Национальные интересы и безопасность России.	8	2	2		6	ОПК-7	
	Раздел 2. Информационные угрозы.							
3	2.1. Информационная война. Информационное оружие.	8	2	2		6	ОПК-7	л-в
4	2.2. Угрозы безопасности России. Угрозы безопасности АСОД.	10	4	2	2	6	ОПК-7	
	Раздел 3. Защита от несанкционированного доступа, модели и основные принципы защиты информации							
5	3.1. Показатели защищенности СВТ.	10	4	2	2	6	ОПК-7	л-в
6	3.2. Защита информации в АСОД.	10	4	2	2	6	ОПК-7	л-в
7	3.3. Виды доступа. Уровни доступа. Контроль доступа.	8	2		2	6	ОПК-7	
	Раздел 4. Комп.вирусы и антивирусные программы							
8	4.1. Проблема вирусного заражения программ. Структура современных вирусных программ.	101	4	2	2	6	ОПК-7	л-в
9	4.2. Перспективные методы антивирусной защиты.	8	2		2	6	ОПК-7	
10	4.3. Основные классы антивирусных программ.	8	2		2	6	ОПК-7	лп
	Раздел 5. Защита от утечки информации							
11	5.1. Криптографические методы защиты информации.	6	4		4	2	ОПК-7	лп
12	5.2. Проблемы защиты информации в сетях ЭВМ	8	4		4	4	ОПК-7	
	Раздел 6. Организац.-правовое обеспечение ИБ							
13	6.1. Организационная защита информации. Комплексное обеспечение безопасности.	8	4		4	4	ОПК-7	
14	6.2.Правовые основы защиты информации	6	2		2	4	ОПК-7	
	Всего по дисциплине:	**144**	**42**	**14**	**28**	**102**		

для студентов заочной формы обучения

№ п/п	Наименование разделов и тем	Всего часов	Кол-во аудиторных часов			Самостоят. работа	Формируемые компетенции	**Интерактив**
			Всего	Кол-во часов по видам занятий				
				Лекции	Практ. занятия			
	Раздел 1. Основные понятия и определения, эволюция подходов к обеспечению ИБ.							
1	1.2. Информация. Информационная сфера. Информационная безопасность.	7	1	1		6	ОПК-7	
2	1.2. Национальные интересы и безопасность России.	7	1		1	6	ОПК-7	
	Раздел 2. Информационные угрозы.							
3	2.1. Информационная война. Информационное оружие.	7	1		1	6	ОПК-7	
4	2.2. Угрозы безопасности России. Угрозы безопасности АСОД.	7	1		1	6	ОПК-7	
	Раздел 3. Защита от несанкционированного доступа, модели и основные принципы защиты информации							
5	3.1. Показатели защищенности СВТ.	6				6	ОПК-7	
6	3.2. Защита информации в АСОД.	7	1	1		6	ОПК-7	л-в
7	3.3. Виды доступа. Уровни доступа. Контроль доступа.	7	1		1	6	ОПК-7	
	Раздел 4. Комп.вирусы и антивирусные программы							
8	4.1. Проблема вирусного заражения программ. Структура современных вирусных программ.	7	1		1	6	ОПК-7	лп
9	4.2. Перспективные методы антивирусной защиты.	7	1	1		6	ОПК-7	л-в
10	4.3. Основные классы антивирусных программ.	7	1		1	6	ОПК-7	лп
	Раздел 5. Защита от утечки информации							
11	5.1. Криптографические методы защиты информации.	6				6	ОПК-7	
12	5.2. Проблемы защиты информации в сетях ЭВМ	12				12	ОПК-7	
	Раздел 6. Организац.-правовое обеспечение ИБ							
13	6.1. Организационная защита информации. Комплексное обеспечение безопасности.	10				10	ОПК-7	
14	6.2.Правовые основы защиты информации	11	1	1		10	ОПК-7	л-в
	Всего по дисциплине:	**144**	**14**	**6**	**8**	**130**		

ПЛАНЫ
СЕМИНАРСКИХ И ПРАКТИЧЕСКИХ ЗАНЯТИЙ
по курсу **«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**

Раздел 1. Основные направления и способы обеспечения информационной безопасности
Тема 2. Законодательство в области информационной безопасности и защиты информации

Практическая работа 1

Цель занятия – изучить современное состояние отечественной нормативно-правовой базы по обеспечению информационной безопасности и правовых основ защиты информации.

Содержание и методика выполнения заданий:

Для выполнения задания необходимо ознакомиться с текстами нормативных актов, представленных в сборнике «Информационное право. Информационная безопасность и защита информации», а также в правовых системах «Консультант Плюс», «Кодекс» или «Гарант». Получив представление о содержании различных видов нормативно-правовых актов, студенты выполняют следующие виды заданий.

Задание 1. В виде схемы представить структуру законодательства, регулирующего правовые основы информационной безопасности и защиты информации (Конституция, кодексы, ФКЗ, ФЗ, указы Президента, постановления Правительства, ГОСТ).

Задание 2. Выявить из текстов законодательных актов основные понятия, относящиеся к сфере информационной безопасности и защите информации. Перечень понятий оформить в виде таблицы, имеющей следующие графы:

Наименование закона	Перечень понятий	Определение понятий

Задание 3. По результатам изучения основных положений законодательства в сфере информационной безопасности и защиты информации необходимо заполнить следующую таблицу в альбомной ориентации:

Название нпа, № статьи	Состав защищаемой информации	Противоправные действия (нарушения)	Ответственность	Основание

Раздел 1. Основные направления и способы обеспечения информационной безопасности
Тема 2. Законодательство в области информационной безопасности и защиты информации

Семинар 1.

Цель семинарского занятия – расширить и обобщить знания студентов по первому разделу курса «Информационная безопасность и защита информации».

Вопросы

1. Законодательство о безопасности и защите информации, его структура и содержание;
2. Понятие тайны. Виды тайн и их содержание. Конфиденциальная информация и ее сущность;
3. Промышленный и экономический шпионаж. Основные угрозы конфиденциальной информации;
4. Основные направления защиты конфиденциальной информации;
5. Опыт зарубежных стран в сфере защиты информации.

Раздел 2. Аналитическая и кадровая работа при обеспечении информационной безопасности

Тема 6. Основные направления, этапы и методы информационно-аналитической работы

Семинар 2.

Цель семинарского занятия – рассмотреть более подробно особенности информационно-аналитической работы в сфере защиты информации и выявить наиболее современные и передовые методы этой работы; изучить персонал как составную часть системы информационной безопасности предприятия.

Вопросы

1. Понятие информационно-аналитической работы, ее цели и задачи;
2. Направления и стадии информационно-аналитической работы. Порядок сбора, анализа и оценки информации;
3. Экспертные системы как метод анализа информации, его достоинства и недостатки;
4. Персонал как источник конфиденциальной информации. Особенности работы с персоналом, владеющим конфиденциальной информацией;
5. Личная безопасность персонала, работающего с конфиденциальной информацией.

Раздел 3. Организация работы с конфиденциальными документами

Тема 8. Конфиденциальное делопроизводство в системе защиты конфиденциальной информации

Практическое занятие 2

Анализ организационно-правовой документации в сфере защиты информации учреждения

Цель занятия – изучить нормативные и инструктивно-регламентирующие материалы по организации работы с документированной информацией ограниченного доступа с точки зрения оформления и содержания.

Содержание и методика выполнения заданий

Студенту выдается комплект разных видов нормативно-инструктивных документов о порядке ведения конфиденциального делопроизводства на предприятиях. На основе изучения представленных материалов студенты выполняют следующие задания.

Задание 1. Проанализировать структуру (основные разделы) этих документов и состав включаемой в них информации. Сравнительный анализ представить в виде следующей схемы:

Параметры анализа	Инструкция по информационной безопасности	Договор о конфиденциальности	Руководство пользователю локальной защищенной компьютерной сети	Методические рекомендации по организации работы
1.Реквизиты документа				
2. Структура документа				
3. Краткое содержание структурных частей				
4.Вывод об особенностях применения документа и его роли в системе информационной безопасности учреждения				

Раздел 3. Организация работы с конфиденциальными документами

Тема 8. Конфиденциальное делопроизводство в системе защиты конфиденциальной информации

Практическое занятие 3

Методика разработки Положения о работе с документированной информацией ограниченного доступа

Цель занятия – получить навыки составления инструкции (положения) по конфиденциальному делопроизводству.

В результате выполнения задания студенты должны:

1) получить представление о видах нормативно-методических изданий, регламентирующих работу с конфиденциальными документами;

2) ориентироваться в составе информации, отражаемой в инструкции по конфиденциальному делопроизводству или положении об организации работы с конфиденциальными документами;

3) овладеть методическими приемами разработки организационных документов по нормативному регулированию работы с конфиденциальными документами.

Содержание и методика выполнения заданий

Задание 1. На основании проанализированных организационных документов разработать проект инструкции или положения об организации работы с конфиденциальными документами на конкретном предприятии.

Задание 2. Подготовить проект приказа, утверждающий инструкцию или положение. Приказ оформить в соответствии с требованиями ГОСТа.

Раздел 3. Организация работы с конфиденциальными документами

Тема 10. Организация конфиденциального документооборота и его сущность

Практическое занятие 4

Цель занятия – освоить технологические процедуры и операции обработки внутренних, поступивших и отправляемых конфиденциальных документов.

Содержание и методика выполнения заданий

Студент знакомится с предлагаемыми материалами по теме и использует конспекты занятий. Получив представление о всех технологических циклах обработки конфиденциальных документов, необходимо закрепить учебный материал, выполнив следующие задания.

Задание 1. Разработать схему обработки конфиденциальных документов внутреннего и выходного потоков. Отразить материал об особенностях процедур:

а) оформления и учета носителей конфиденциальной информации;

б) обработки изданных документов.

Задание 2. Разработать схему обработки конфиденциальных документов входного потока. Отразить процедуры:

а) приема, первичной обработки, предварительного рассмотрения и распределения поступивших документов;

б) традиционного учета поступивших документов и формирования справочно-информационного банка данных по документам;

в) автоматизированного учета поступивших документов и формирования справочно-информационного банка данных по документам.

Задание 3. Сформулировать выводы об особенностях и различиях технологических операций по обработке потоков входящих, исходящих и внутренних конфиденциальных документов. Отметить преимущества и недостатки традиционных и автоматизированных технологий обработки этих документов.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Формы самостоятельной работы по курсу

*«*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*»*

1. Изучение учебного материала.
2. Чтение основной и дополнительной литературы.
3. Выполнение тестовых заданий.
4. Посещение Интернет-сайтов по данной тематике.
5. Выполнение индивидуальных заданий с целью закрепления знаний по теме.
6. Написание рефератов и выступлений по темам, предложенным ниже

ТЕМАТИКА РЕФЕРАТОВ
по дисциплине «Информационная безопасность» по направлению «Менеджмент»

Одной из наиболее эффективных форм самостоятельной работы студентов является написание студентами письменного реферата. Реферат представляет собой, обзор научной литературы по выбранной теме с комментариями и анализом. Тема реферата должна быть проблемной и профессионально ориентированной.

Студенты готовят текст реферата и делают по нему презентацию доклада, который представляют в группе. Обсуждение доклада происходит с участием всех студентов группы. Такая интерактивная технология обучения способствует развитию у студентов информационной коммуникативности, активности мышления, умению вести дискуссию, аргументировано отвечать на вопросы.

Творческая работа студентов по написанию реферата состоит из нескольких этапов:

1. Выбор темы исследования, подбор и изучение литературы по теме.
2. Составление плана и определение примерной структуры реферата.
3. Написание основного текста и формулировка выводов исследования.
4. Окончательное оформление реферата.

Реферат проверяется преподавателем, и после краткой письменной рецензии в конце реферата ставится соответствующая предварительная оценка. Окончательную оценку студент получает после сделанного на семинарском занятии доклада. Предлагаемый список тем для написания рефератов носит рекомендательный характер и может неограниченно расширяться с учетом индивидуальных интересов студентов и их профессиональной направленности. Тематика рефератов выбирается студентом самостоятельно. В течение семестра каждый студент обязан подготовить как минимум 2 реферата.

1. Информационное право и информационная безопасность.
2. Концепция информационной безопасности.
3. Основы экономической безопасности предпринимательской деятельности.
4. Анализ законодательных актов об охране информационных ресурсов открытого доступа.
5. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
6. Соотношение понятий: информационные ресурсы, информационные

системы и информационная безопасность.

7. Информационная безопасность **(**по материалам зарубежных источников и литературы).
8. Правовые основы защиты конфиденциальной информации.
9. Экономические основы защиты конфиденциальной информации.
10. Организационные основы защиты конфиденциальной информации.
11. Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.
12. Составление инструкции по обработке и хранению конфиденциальных документов.
13. Направления и методы защиты документов на бумажных носителях.
14. Направления и методы защиты машиночитаемых документов.
15. Архивное хранение конфиденциальных документов.
16. Направления и методы защиты аудио- и визуальных документов.
17. Порядок подбора персонала для работы с конфиденциальной информацией.
18. Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.
19. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.
20. Порядок проведения переговоров и совещаний по конфиденциальным вопросам.
21. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
22. Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.
23. Порядок защиты информации в рекламной и выставочной деятельности.
24. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.
25. Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).
26. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.
27. Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).
28. Назначение, виды, структура и технология функционирования системы защиты информации.
29. Поведение персонала и охрана фирмы в экстремальных ситуациях

различных типов.

30. Аналитическая работа по выявлению каналов утечки информации фирмы.
31. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.
32. Направления и методы защиты профессиональной тайны.
33. Направления и методы защиты служебной тайны.
34. Направления и методы защиты персональных данных о гражданах.
35. Методы защиты личной и семейной тайны.
36. Построение и функционирование защищенного документооборота.
37. Защита секретов в дореволюционной России.
38. Методика инструктирования и обучения персонала правилами защиты секретов фирмы.

ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

2. Определить место информационной безопасности в обеспечении системы общественной безопасности.
3. Дать определение информационной безопасности.
4. Назвать основные направления и задачи обеспечения информационной безопасности общества.
5. Назвать основные компоненты информационной безопасности автоматизированных информационных систем.
6. Охарактеризовать уровни реализации информационной безопасности.
7. Дать определение и классификацию информационных ресурсов.
8. Определить основные виды угроз информационным ресурсам.
9. Охарактеризовать особенности угроз конфиденциальной информации.
10. Проанализировать причины возникновения угроз утраты или утечки конфиденциальной информации.
11. Описать причины возникновения каналов несанкционированного доступа к информации.
12. Классифицировать виды каналов несанкционированного доступа к информации.
13. Описать характер действия организационных каналов несанкционированного доступа к информации.
14. Охарактеризовать технические каналы несанкционированного доступа к информации.
15. Охарактеризовать легальные и нелегальные методы обеспечения действия каналов утечки информации.
16. Проанализировать особенности угроз автоматизированным информационным системам.
17. Дать классификацию удаленных атак.
18. Проанализировать основные направления правовой защиты информации.
19. Раскрыть содержание нормативных актов, защищающих право граждан на своевременное получение достоверной информации.
20. Изложить законный порядок реализации права гражданина на опровержение ложной информации о нем в средствах массовой информации.
21. Показать порядок защиты прав граждан на личную тайну и неприкосновенность частной жизни законодательством Российской

Федерации о СМИ.

22. Определить объекты защиты авторских прав.

23. Назвать основные права автора в отношении его произведения.

24. Определить объекты интеллектуальной собственности, защищаемые патентным законодательством.

25. Охарактеризовать основные права патентообладателя в отношении его произведения (промышленного образца, полезной модели).

26. Дать определение государственной тайны и назвать грифы секретности.

27. Перечислить сведения, составляющие государственную тайну и сведения, которые не могут относиться к государственной тайне.

28. Изложить порядок отнесения сведений к государственной тайне и их засекречивания.

29. Раскрыть последовательность условия и формы допуска должностных лиц к государственной тайне.

30. Дать определение коммерческой тайны и перечислить сведения, которые не могут быть ее объектом.

31. Охарактеризовать порядок установления режима коммерческой тайны и основные права ее субъектов.

32. Назвать основные виды служебной тайны определенные законодательством Российской Федерации.

33. Изложить принципы и направления комплексного подхода к обеспечению информационной безопасности предприятия.

34. Назвать основные положения концепции информационной безопасности предприятия.

35. Изложить содержание регламента обеспечения информационной безопасности предприятия.

36. Определить основные методы и способы работы службы безопасности предприятия по защите конфиденциальной информации.

37. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.

38. Проанализировать содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям фирмы.

39. Обосновать критерии выделения конфиденциальных документов из общего потока поступающих документов.

40. Обосновать состав показателей учетной карточки (по выбору преподавателя) и правила их заполнения.

41. Проанализировать особенности контроля за исполнением конфиденциальных документов, его организационное и технологическое

отличие от контроля открытых документов.

42. Классифицировать состав бумажных и технических носителей информации, применяемых для составления деловой (управленческой) и технической конфиденциальной документации.

43. Проанализировать особенности текста конфиденциального документа.

44. Регламентировать в виде фрагмента инструкции порядок работы исполнителей с конфиденциальными документами.

45. Проанализировать пути использования существующих средств копирования и тиражирования документов для изготовления экземпляров и копий конфиденциальных документов.

46. Сформулировать возможности, трудности и направления использования
электронной почты для передачи конфиденциальных документов.

47. Составить фрагмент номенклатуры дел, содержащих конфиденциальные
документы.

48. Проанализировать задачи защиты информации, которые должны быть
решены при формировании и оформлении дел с конфиденциальными документами.

49. Классифицировать способы и средства физического уничтожения документов, изготовленных на носителях различных типов.

50. Проанализировать пути поиска документов и дел, не обнаруженных при
проверке их наличия, дать рекомендации, повышающие эффективность поиска и предотвращающие утрату документов и дел.

51. Составить и проанализировать технологическую схему (цепочку) приема (перевода) лиц на работу, связанную с владением конфиденциальной информацией.

52. Составить и проанализировать технологическую схему (цепочку) увольнения сотрудников, владеющих конфиденциальной информацией. .

53. Проанализировать виды угроз безопасности конфиденциальной информации фирмы при демонстрации на выставке новой продукции.

54. Составить схему каналов возможной утраты конфиденциальной информации, находящейся в компьютере, локальной сети, проанализировать степень опасности каждого канала.

55. Назвать основные элементы физической защиты территории и помещений предприятия.

56. Охарактеризовать способы и элементы программно-технической защиты информационных ресурсов.

57. Дать классификацию компьютерных вирусов.

58. Описать основные антивирусные программы.

59. Охарактеризовать основные способы криптографического преобразования данных.

Литература

Основная литература

Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ О.В. Прохорова— Электрон. текстовые данные.— Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014.— 113 с.— Режим доступа: http://www.iprbookshop.ru/43183.html.— ЭБС «IPRbooks»

Дополнительная литература

1. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ П.Н. Башлы, А.В. Бабаш, Е.К. Баранова— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677.html.— ЭБС «IPRbooks»
2. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ В.Ф. Шаньгин— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 702 с.— Режим доступа: http://www.iprbookshop.ru/63594.html.— ЭБС «IPRbooks»
3. Информационная безопасность и защита информации [Электронный ресурс]: учебно-методический комплекс/ — Электрон. текстовые данные.— Алматы: Нур-Принт, 2012.— 98 с.— Режим доступа: http://www.iprbookshop.ru/67055.html.— ЭБС «IPRbooks»
4. Информационная безопасность и защита информации на железнодорожном транспорте: Часть 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте [Электронный ресурс]: учебник/ С.Е. Ададуров [и др.].— Электрон. текстовые данные.— М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014.— 440 с.— Режим доступа: http://www.iprbookshop.ru/45259.html.— ЭБС «IPRbooks»
5. Информационная безопасность и защита информации на железнодорожном транспорте: Часть 2. Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте [Электронный ресурс]: учебник/ М.Е. Бородулин [и др.].— Электрон. текстовые данные.— М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014.— 448 с.— Режим доступа: http://www.iprbookshop.ru/45260.html.— ЭБС «IPRbooks»
6. Шубинский М.И. Информационная безопасность для работников бюджетной сферы. Защита персональных данных [Электронный ресурс]: учебное пособие/ М.И. Шубинский— Электрон. текстовые данные.— СПб.:

Университет ИТМО, 2013.— 77 с.— Режим доступа: http://www.iprbookshop.ru/68654.html.— ЭБС «IPRbooks»
7. Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ С.В. Петров, П.А. Кисляков— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 с.— Режим доступа: http://www.iprbookshop.ru/33857.html.— ЭБС «IPRbooks»
8. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ А.В. Артемов— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 с.— Режим доступа: http://www.iprbookshop.ru/33430.html.— ЭБС «IPRbooks»
9. Федин Ф.О. Информационная безопасность [Электронный ресурс]: учебное пособие/ Ф.О. Федин, В.П. Офицеров, Ф.Ф. Федин— Электрон. текстовые данные.— М.: Московский городской педагогический университет, 2011.— 260 с.— Режим доступа: http://www.iprbookshop.ru/26486.html.— ЭБС «IPRbooks»
10. Спицын В.Г. Информационная безопасность вычислительной техники [Электронный ресурс]: учебное пособие/ В.Г. Спицын— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2011.— 148 с.— Режим доступа: http://www.iprbookshop.ru/13936.html.— ЭБС «IPRbooks»