ИНСТИТУТ ЗАКОНОВЕДЕНИЯ И УПРАВЛЕНИЯ ВПА

КАФЕДРА ПРИКЛАДНОЙ ИНФОРМАТИКИ И
ПРОФЕССИОНАЛЬНО-ПРИКЛАДНЫХ ДИСЦИПЛИН

МЕТОДИЧЕСКИЕ И ИНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ «ЗАЩИТА ИНФОРМАЦИИ»

Направление подготовки: Юриспруденция
(квалификация (степень): «бакалавр»)

СОДЕРЖАНИЕ

ТЕМАТИЧЕСКИЙ ПЛАН

по дисциплине
«ЗАЩИТА ИНФОРМАЦИИ»
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.	2	1	1		1	ОК-3	
2	1.2. Национальные интересы и безопасность России.	2	1	1		1	ОК-3	
	Раздел 2. Информационные угрозы.							
3	2.1. Информационная война. Информационное оружие.	2	2	2			ОК-3 ОК-4	л-в
4	2.2. Угрозы безопасности России. Угрозы безопасности АСОД.	2	2	2			ОК-3 ОК-4	
5	**Раздел 3. Защита от несанкционированного доступа, модели и основные принципы защиты информации**							
6	3.1. Показатели защищенности СВТ.	3	3	1	2		ОК-4 ПК-3	лп
7	3.2. Защита информации в АСОД.	3	3	1	2		ОК-3 ОК-4	лп
8	3.3. Виды доступа. Уровни доступа. Контроль доступа.	2	2		2		ПК-3	
	Раздел 4. Комп.вирусы и антивирусные программы							
9	4.1. Проблема вирусного заражения программ. Структура современных вирусных программ.	3	3	1	2		ПК-3	л-в
10	4.2. Перспективные методы антивирусной защиты.	3	3	1	2		ПК-3	
11	4.3. Основные классы антивирусных программ.	4	4	2	2		ПК-3	лп
	Раздел 5. Защита от утечки информации							
12	5.1. Криптографические методы защиты информации.	2	2		2		ПК-3	лп
13	5.2. Проблемы защиты информации в сетях ЭВМ	2	2		2		ПК-3	
	Раздел 6. Организац.-правовое обеспечение ИБ							
14	6.1. Организационная защита информации. Комплексное обеспечение безопасности.	3	2	2		1	ОК-3 ОК-4	
15	6.2.Правовые основы защиты информации	3	2	2		1	ОК-3 ОК-4	л-в
	Всего по дисциплине:	**36**	**32**	**16**	**16**	**4**		

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	1.1 Информация. Информационная сфера. Информационная безопасность.	3	1	1		2	ОК-3	
2	1.2. Национальные интересы и безопасность России.	3	1	1		2	ОК-3	
	Раздел 2. Информационные угрозы.							
3	2.1. Информационная война. Информационное оружие.	3	1		1	2	ОК-3 ОК-4	
4	2.2. Угрозы безопасности России. Угрозы безопасности АСОД.	3	1		1	2	ОК-3 ОК-4	
5	**Раздел 3. Защита от несанкционированного доступа, модели и основные принципы защиты информации**							
6	3.1. Показатели защищенности СВТ.	3	1	1		2	ОК-4 ПК-3	
7	3.2. Защита информации в АСОД.	3	1	1		2	ОК-3 ОК-4	
8	3.3. Виды доступа. Уровни доступа. Контроль доступа.	3	1		1	2	ПК-3	
	Раздел 4. Комп.вирусы и антивирусные программы							
9	4.1. Проблема вирусного заражения программ. Структура современных вирусных программ.	3	1		1	2	ПК-3	лп
10	4.2. Перспективные методы антивирусной защиты.	3	1	1		2	ПК-3	л-в
11	4.3. Основные классы антивирусных программ.	1	1		1		ПК-3	лп
	Раздел 5. Защита от утечки информации							
12	5.1. Криптографические методы защиты информации.	3	1		1	2	ПК-3	
13	5.2. Проблемы защиты информации в сетях ЭВМ						ПК-3	
	Раздел 6. Организац.-правовое обеспечение ИБ							
14	6.1. Организационная защита информации. Комплексное обеспечение безопасности.	2				2	ОК-3 ОК-4	
15	6.2.Правовые основы защиты информации	3	1	1		2	ОК-3 ОК-4	л-в
	Всего по дисциплине:	**36**	**12**	**6**	**6**	**24**		

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Основные понятия и определения, эволюция подходов к обеспечению ИБ.

Тема 1.1. Информация. Информационная сфера. Информационная безопасность

Студенты должны

иметь представление:

составляющие информационной сферы.

знать:

— понятия «Информация»

— различие понятия информационного воздействия и информационного взаимодействия

— свойства информации в форме сведений и в форме сообщений

— виды информации как объекта исследования

уметь:

— определять свойства информации в форме сведений

— определять свойства информации в форме сообщения

Содержание понятия «Информация». Формы информации. Свойства информации в форме сведений и в форме сообщений. Информация как объект исследования. Понятия информационного воздействия и информационного взаимодействия. Составляющие информационной сферы.

Тема 1.2. Национальные интересы и безопасность России. (ОПК-7)

Студенты должны

иметь представление:

— принципы соблюдения информационной безопасности

— основные составляющие национальных интересов в информационной сфере.

знать:

— классификации национальных интересов

— общие методы обеспечения информационной безопасности

— понятие информационных ресурсов

— пять классов информационных ресурсов

уметь:

— классифицировать национальные интересы

— относить информационные ресурсы к различным классам

Принципы соблюдения информационной безопасности. Две классификации национальных интересов. Основные составляющие национальных интересов в информационной сфере. Общие методы обеспечения информационной безопасности. Понятие информационных ресурсов. Основные классы информационных ресурсов

Раздел 2. Информационные, программно-математические, физические и организационные угрозы

Тема 2.1. Информационная война. Информационное оружие.

Студенты должны

иметь представление:

— концепцию национальной безопасности Российской Федерации
— национальные интересы России
— на какие объекты воздействуют в информационной войне
— термины начала и окончания войны.

знать:

— составляющие национальной безопасности
— цели информационной войны в мирное и военное время

уметь:

— классифицировать информационное оружие
— определять цели информационной войны

Интересы и угрозы в области информационной безопасности. Составляющие национальной безопасности. Проблемы информационной войны. Классификация информационного оружия. Основные объекты воздействия в информационной войне. Цели информационной войны. Понятия начала и окончания войны.

Тема 2.2. Угрозы безопасности России. Угрозы безопасности АСОД.

Студенты должны

иметь представление:

— понятие «Интегральная информационная безопасность».

знать:

— Угрозы безопасности России
— Угрозы безопасности в АСОД.
— Мировые стандарты в области информационной безопасности.

уметь:

— классифицировать угрозы безопасности России
— составлять схему основных элементов и объектов защиты в АСОД
— составлять общую схему анализа безопасности.

Виды угроз безопасности России. Классификация угроз. Понятие «Интегральная информационная безопасность». Схема основных элементов и объектов защиты в АСОД. Угрозы безопасности в АСОД. Мировые стандарты в области информационной безопасности. Основные компоненты критериев безопасности ITSEC. Процесс управления рисками. Общая схема анализа безопасности.

Раздел 3. Защита от несанкционированного доступа, модели и основные принципы защиты

Тема 3.1. Показатели защищенности СВТ.

Студенты должны

иметь представление:

— функции и задачи защиты информации

знать:

— группы факторов, влияющие на информационную безопасность технической системы
— показатели защищенности СВТ (АС).

уметь:

— классифицировать показатели защищенности СВТ (АС)

Функции и задачи защиты информации. Функции непосредственной защиты. Механизмы защиты. Управление механизмами защиты. Основные группы факторов, влияющие на информационную безопасность технической системы. Класс и показатели защищенности СВТ (АС).

Тема 3.2. Защита информации в АСОД

Студенты должны

иметь представление:

— понятие защиты информации

— понятие защиты информации в АСОД

знать:

— методы защиты информации в вычислительных сетях

— методы, применяемые для установления подлинности различных объектов.

уметь:

— применять методы защиты информации в вычислительных сетях

— применять методы для установления подлинности различных объектов

Понятие защиты информации. Понятие защиты информации в АСОД. Основные методы защиты информации в вычислительных сетях. Методы, применяемые для установления подлинности различных объектов.

Тема 3.3. Виды доступа. Уровни доступа. Контроль доступа

Студенты должны

иметь представление:

— термины ограничение доступа, разграничение доступа, разделение доступа(привилегий)

знать:

— виды информации с ограниченным доступом

— методы защиты информации от несанкционированного доступа

уметь:

— реализовывать различные алгоритмы для идентификации и аутентификации пользователя

Виды доступа к информации. Обязательное доведение. Свободный доступ. Ограничения и запреты. Виды информации с ограниченным доступом. Методы защиты информации от преднамеренного доступа (при применении простых средств хранения и обработки информации). Идентификация и аутентификация пользователя.

Лабораторная работа №1

Идентификация и аутентификация пользователя

Практическая работа №1.

Основные методы и приемы защиты от несанкционированного доступа

Раздел 4. Компьютерные вирусы и антивирусные программы

Тема 4.1. Проблема вирусного заражения программ. Структура современных вирусных программ.

Студенты должны

иметь представление:

— последствия от вирусных вторжений и катастроф

знать:

— пути проникновения компьютерных вирусов;

— классификацию закладок и их общие характеристики;

уметь:

— распознавать воздействие вируса на программный продукт или данные

— противодействовать вирусной атаке

Компьютерный вирус(закладка): понятие, пути распространения, проявление действия вируса. проникновения Структура современных вирусов: модели поведения вирусов; деструктивные действия вируса; разрушение программ защиты, схем контроля или

изменение состояния программной среды. Воздействия на программно-аппаратные средства защиты информации. Последствия от вирусных вторжений и катастроф.

Тема 4.2. Перспективные методы антивирусной защиты.

Студенты должны

иметь представление:

— новейшие технологии антиспамовых и антивирусных решений

знать:

— спам

— принципы защиты от спама и вирусов

уметь:

— проводить антивирусные проверки на ПК

— применять различные принципы защиты от спама и вирусов

Перспективные методы антивирусной защиты. Антивирусные проверки на ПК, на файловых серверах и серверах приложений, на прокси-серверах, на межсетевых экранах. Борьба со спамом. Базовые однолинейные методы. Спамоборона. Многоплатформенные антивирусные и антиспамовые решения компании Sophos.

Тема 4.3. Основные классы антивирусных программ.

Студенты должны

иметь представление:

— технологии компании Sybari.для безопасности почтовых серверов

— иерархию программ семейства Dr.Web®

знать:

— состав ядра Dr.Web®

уметь:

— применять антивирусные программы Dr.Web®

Программы-детекторы, программы-доктора, программы - ревизоры, программы-фильтры. Интегрированные антиспамовые и антивирусные решения от компании Sybari. Антивирусные программы семейства Dr.Web® для рабочих станций. Структура Dr.Web®. Ядро Dr.Web®. Программы – антивирусы: Aidstest, Adinf, Norton Antivirus, AVP. Профилактика заражения вирусом.

Практическая работа №2.

Особенности закладок и защита от воздействия закладок. Пакеты антивирусных программ

Раздел 5. Защита от утечки информации по техническим каналам

Тема 5.1. Криптографические методы защиты информации.

Студенты должны

иметь представление:

— принципы закрытия информации методами стеганографии

— метод закрытия информации электронно-цифровой подписью

знать:

— два направления в криптологии

— цели криптографии и криптоанализа

уметь:

— закрывать информацию (шифровать) различными методами

— работать с криптоцентром MS OutLook

Периоды развития криптологии. Первые шифры. Два направления в криптологии. Цели криптографии и криптоанализа. Разделы криптографии. Стеганография. Закрывать информацию методами

зимены,(моно-алфавитной и поли-алфавитной подстановки), перестановки, с помощью аналитических преобразований, методом гаммирования. Система с открытым ключем. Электронно-цифровая подпись. Приемы хеширования. Работа с криптоцениром MS OutLook.

Лабораторная работа №2. Моноалфавитная подстановка.

Лабораторная работа №3. Полиалфавитная подстановка.

Лабораторная работа №4. Шифрование методом перестановки.

Лабораторная работа №5. Электронно-цифровая подпись и приемы хеширования.

Тема 5.2. Проблемы защиты информации в сетях ЭВМ

Студенты должны

иметь представление:

— цели, функции и задачи защиты информации в сетях ЭВМ

— архитектуру механизмов защиты в сетях

знать:

— назначение сервисов безопасности, межсетевых экранов, прокси серверов

— международные стандарты

уметь:

— защитить информацию в ПК

— применять межсетевых экранов

Защита информации в ПК. Сервисы безопасности. Архитектура механизмов защиты в сетях. Международные стандарты. Межсетевые экраны. Прокси серверы..

Практическая работа №3.

Перехват вывода на экран, перехват ввода с клавиатуры. Перехват и обработка файловых операций

Практическая работа №4.

Защита информации от копирования. Защита программ от дисассемблирования.

Практическая работа №5.

Защита программ в оперативной памяти. Приемы работы с защищенными программами.

Раздел 6. Организационно-правовое обеспечение ИБ

6.1. Организационная защита информации. Комплексное обеспечение безопасности.

Студенты должны

иметь представление:

— сущность ОЗИ и ее место в комплексной системе защиты информации

знать:

— виды ОЗИ;

— назначение должностных инструкций;

— методы контроля за исполнением должностных инструкций;

уметь:

— разработать мероприятия по организация физической охраны предприятия.

Сущность ОЗИ и ее место в комплексной системе защиты информации. Виды ОЗИ. Лицензирование деятельности предприятия по проведению работ, связанных с использование сведений составляющих гостайну. Организация физической охраны предприятия. Источники. Состав и назначение должностных инструкций. Порядок создания, утверждения и исполнения должностных инструкций.

Тема 6.2.Правовые основы защиты информации

Студенты должны

знать:

— основные международные правовые акты по защите информации

— основные положения и принципы международных соглашений

— соответствие российских и международных правовых отношений

— российские общегосударственные правовые документы по защите информации

— российские отраслевые нормативные документы по защите информации

уметь:

— применять законы о защите информации

Опыт законодательного регулирования информатизации в России и за рубежом. Концепция правового обеспечения информационной безопасности РФ. Стандарты и нормативно-методические документы в области обеспечения информационной безопасности. Государственная система обеспечения информационной безопасности. Международные правовые акты по защите информации.

Планы практических и семинарских занятий

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

«ЗАЩИТА ИНФОРМАЦИИ»

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 преподавателем

ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Определить место информационной безопасности в обеспечении системы общественной безопасности.
2. Дать определение информационной безопасности.
3. Назвать основные направления и задачи обеспечения информационной безопасности общества.
4. Назвать основные компоненты информационной безопасности автоматизированных информационных систем.
5. Охарактеризовать уровни реализации информационной безопасности.
6. Дать определение и классификацию информационных ресурсов.
7. Определить основные виды угроз информационным ресурсам.
8. Охарактеризовать особенности угроз конфиденциальной информации.
9. Проанализировать причины возникновения угроз утраты или утечки конфиденциальной информации.
10. Описать причины возникновения каналов несанкционированного доступа к информации.
11. Классифицировать виды каналов несанкционированного доступа к информации.
12. Описать характер действия организационных каналов несанкционированного доступа к информации.
13. Охарактеризовать технические каналы несанкционированного доступа к информации.
14. Охарактеризовать легальные и нелегальные методы обеспечения действия каналов утечки информации.
15. Проанализировать особенности угроз автоматизированным информационным системам.
16. Дать классификацию удаленных атак.
17. Проанализировать основные направления правовой защиты информации.
18. Раскрыть содержание нормативных актов, защищающих право граждан на своевременное получение достоверной информации.
19. Изложить законный порядок реализации права гражданина на опровержение ложной информации о нем в средствах массовой информации.
20. Показать порядок защиты прав граждан на личную тайну и неприкосновенность частной жизни законодательством Российской Федерации о СМИ.
21. Определить объекты защиты авторских прав.
22. Назвать основные права автора в отношении его произведения.
23. Определить объекты интеллектуальной собственности, защищаемые патентным законодательством.
24. Охарактеризовать основные права патентообладателя в отношении его произведения (промышленного образца, полезной модели).
25. Дать определение государственной тайны и назвать грифы секретности.
26. Перечислить сведения, составляющие государственную тайну и сведения, которые не могут относиться к государственной тайне.
27. Изложить порядок отнесения сведений к государственной тайне и их засек-

речивания.

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

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

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

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

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

33. Назвать основные положения концепции информационной безопасности предприятия.

34. Изложить содержание регламента обеспечения информационной безопасности предприятия.

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

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

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

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

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

40. Проанализировать особенности контроля за исполнением конфиденциальных документов, его организационное и технологическое отличие от контроля открытых документов.

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

42. Проанализировать особенности текста конфиденциального документа.

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

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

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

46. Составить фрагмент номенклатуры дел, содержащих конфиденциальные документы.

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

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

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

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

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

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

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

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

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

56. Дать классификацию компьютерных вирусов.

57. Описать основные антивирусные программы.

58. Охарактеризовать основные способы криптографического преобразования данных.