Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Горно-Алтайский государственный университет»

РАБОЧАЯ ПРОГРАММА

дисциплины: **Информационная безопасность**
Уровень основной образовательной программы: **бакалавриат**
Рекомендуется для направления подготовки 09.03.03 Прикладная информатика
профиль подготовки «Прикладная информатика в экономике»

Программа составлена в соответствии с требованиями ФГОС ВО
по направлению подготовки 09.03.03 Прикладная информатика
(утверждён приказом Минобрнауки от 12.03. 2015 года № _207) и учебного плана по направлению подготовки 09.03.03 Прикладная информатика (профиль «Прикладная информатика в экономике»), утвержденного Ученым советом ГАГУ
(от 24.12.2015 протокол №12)

Рабочая программа утверждена на заседании кафедры экономики предприятия и прикладной информатики 26.01.16 г., протокол №5

1 Цели и задачи дисциплины

Цель дисциплины:

Овладение знаниями по основным уровням информационной безопасности, происхождению угроз, развитие умений применения современных методов и технологий защиты информации на ПК и в сетях, антивирусного программное обеспечение, методов шифрования информации; развитие творческих навыков при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности личности, общества и государства.

Задачи дисциплины:

- развить и дополнить знания студентов, полученных в результате изучения других предметов, по основам защиты информации;
- рассмотреть понятие внешних и внутренних угроз, направленных на компьютерную систему;
- рассмотреть уровни безопасности компьютерных систем и дать представление об современных методах защиты информации на соответствующих уровнях;
- рассмотреть понятие вируса и его функциональные возможности;
- изучить антивирусное программное обеспечение и получить навыки работы с ним;
- рассмотреть современные технологии шифрования информации.
- рассмотреть вопросы обеспечения информационной безопасности личности, общества и государства;

2 Место дисциплины в структуре ООП

Дисциплина «Информационная безопасность» относится к специальным дисциплинам профессионального цикла (Б1.Б.12).

Для освоения дисциплины «Информационная безопасность» обучающиеся используют знания, умения, навыки и установки, сформированные в ходе изучения дисциплин «Информатика и программирование», «Вычислительные системы, сети и телекоммуникации», «Операционные системы», «Информационные системы и технологии».

Освоение дисциплины «Информационная безопасность» не является необходимой основой для последующего изучения каких-либо дисциплин.

Междисциплинарные связи разделов и (или) тем дисциплины с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	Наименование разделов (темы) данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин				
		Информационные угрозы и уровни обеспечения информационной безопасности.	Информационные угрозы и уровни обеспечения информационной безопасности.	Информационные угрозы и уровни обеспечения информационной безопасности.	Информационные угрозы и уровни обеспечения информационной безопасности.	Информационные угрозы и уровни обеспечения информационной безопасности.

1	Информатика и программирование		+			+
2	Вычислительные системы, сети и телекоммуникации		+	+	+	+
3	Операционные системы		+		+	+
4	Информационные системы и технологии	+	+	+	+	+

3 Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:
ОПК-4 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

В результате изучения дисциплины студент должен:

Знать: основные угрозы безопасности компьютерным системам; законодательство в информационной сфере; основные средства и приемы борьбы с угрозами возникающие в компьютерных системах, основные методы криптографической защиты информации;

цели, задачи, принципы и основные направления обеспечения информационной безопасности личности, общества, государства; основные термины по проблематике информационной безопасности; правовые аспекты обеспечения информационной безопасности; методологию создания систем защиты информации; перспективные направления развития систем и методов защиты информации; современные подходы к построению систем защиты информации; компьютерную систему, как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;

Уметь: выявлять и классифицировать угрозы информационной безопасности; разрабатывать модели злоумышленников, схемы решения проблем безопасности в компьютерных системах; создавать препятствия проникновению в компьютер и сеть нежелательной информации; находить и использовать новые средства защиты информации в условиях появления новых угроз; разрабатывать политики информационной безопасности организации, обосновывать организационно-технические мероприятия по защите информации в ИС; реализовывать защиту информационных систем от компьютерных вирусов и других вредоносных программ; применять методы и средства защиты конфиденциальной информации, включая криптографические средства; оформлять необходимую документацию.

Владеть: навыками установки и эксплуатации антивирусного программного обеспечения; работы с криптографическим программным обеспечением; установки электронных средств компьютерной защиты; навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем; правилами и приемами защиты сведений, составляющих государственную тайну,

коммерческую тайну, а также персональных данных; работы с инструментальными средствами защиты информации.

4 Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3 зачетных единиц

Вид учебной работы	Всего часов / зачетных единиц	Семестр
		7
Аудиторные занятия всего В том числе:	44/1,44	44
Лекции	14/0,61	14
Лабораторные работы (ЛР)	20/0,55	20
Практические (П)	10/0,28	10
Самостоятельная работа всего В том числе:	64/1,56	64
Реферат	24	24
Курсовая работа	-	-
Другие виды самостоятельной работы	40/1,51	40
Вид аттестации (зачет, экзамен)	зачет с оценкой	
Общая трудоемкость, часы,	108	108
зачетные единицы	3	3

Матрица соответствия компетенций и разделов дисциплины

№	Наименование раздела дисциплины	Всего часов	Компетенция	
			ОПК-4	Итого:
Модуль 1				
1	Информационные угрозы и их классификация. Компоненты ИБ. Уровни обеспечения ИБ.	12	+	1
2	Законодательно-правовой аспект. Информационное законодательство.	18	+	1
3	Административно-организационный аспект. Политика ИБ.	20	+	1
Модуль 2				
4	Программно-технический аспект. Вирусы и антивирусы.	34	+	1
5	Технологии (механизмы) обеспечения ИБ. Криптография и шифрование.	24	+	1
	ИТОГО	108		

Работа студентов и уровень освоения содержания курса «Информационная безопасность» оценивается по 100 бальной шкале в соответствии с модульно-рейтинговой системой. (Возможно превышение набора баллов более 100 только в случае выполнения работ по НИРС, в соответствии с Положением о МРС). Оценивается посещаемость и активность студента на лекциях и лабораторных семинарских занятиях, качество выполняемой самостоятельной работы, полнота и точность ответов. Зачет с оценкой выводится в следующем порядке:

Критерии оценки преподавателя по МРС

Вид контроля	**Форма контроля**	**Условие допуска к контролю**	**Порядок оценки**	**Итоговый бал (рейтинг)**
I рейтинг (первый промежуточный)	Решение самостоятельных заданий	Посещение лекционных и лабораторных занятий	Первое лабораторное занятие	3
			Второе лабораторное занятие	3
			Третье лабораторное занятие	3
			Четвертое лабораторное занятие	3
			Пятое лабораторное занятие	3
			Каждый правильный ответ 0,5 балла, максимальное количество баллов 14	14

II рейтинг (первый промежуточный)	НИРС	Посещение лекционных и лабораторных занятий	НИРС	40 и более
	Решение самостоятельных заданий		Шестое лабораторное занятие	3
			Седьмое лабораторное занятие	3
			Восьмое лабораторное занятие	3
			Девятое лабораторное занятие	3
			Десятое лабораторное занятие	3
			Каждый правильный ответ 0,5 балла, максимальное количество баллов 14	14
Зачет с оценкой	Устный опрос по билетам, состоящим из двух основных вопросов и одного дополнительного	По каждой составляющей промежуточного контроля получен итоговый бал (рейтинг)	Первый вопрос	10
			Второй вопрос	10
			Задача	20
Сумма баллов по всем видам контроля			≥91 От 76 до 90 От 61 до 75 < 61	Отлично Хорошо Удовлетворительно Неудовлетворительно

5 Содержание дисциплины
5.1 Содержание разделов дисциплины

№ п/п	Наименование раздела	Содержание раздела
1	Информационные угрозы и их классификация. Компоненты ИБ. Уровни обеспечения ИБ.	Внешние и внутренние угрозы; природного и человеческого характера; умышленные и неумышленные; угрозы на программном, аппаратном и механическом уровне. Компоненты ИБ: доступность, целостность, конфиденциальность. Уровни (аспекты) обеспечения ИБ: законодательно-правовой; административно-организационный; программно-технический. Формирование режима ИБ.
2	Законодательно-правовой аспект. Информационное законодательство.	Понятие информационного общества и информационного законодательства. Основные положения закона РФ о защите информации: понятие информации, владельцы информации, уровни информационного взаимодействия. Нарушения в информационной сфере. Понятие Государственной тайны.
3	Административно-организационный аспект. Политика ИБ.	Цели, задачи и содержание административного уровня обеспечения ИБ предприятия. Разработка политики ИБ предприятия. Подготовка кадров. Проведение анализа угроз. Расчет и страхование рисков.
4	Программно-технический аспект. Вирусы и антивирусы.	Программно-технический аспект ИБ. Понятие вируса как вредоносной программы. Структура, функционал вируса, предметы и цели, примеры реальных вирусных атак. Понятие антивирусной программы, как автоматизированного средства борьбы с вирусами. Поиск, уничтожение вирусов. Классификация антивирусного ПО.
5	Технологии (механизмы) обеспечения ИБ. Криптография и шифрование.	Идентификация и аутентификация пользователей. Методы разграничения доступа. Регистрация и аудит ИС. Межсетевое экранирование. Понятие шифров и кодов. Эволюция методов шифрования и кодирования информации. Механические, аппаратные и программные криптографические средства. Электронная цифровая подпись.

5.2 Распределение объема часов разделов (тем) дисциплины «Информационная безопасность» по видам занятий (технологическая карта)

№ п/п	Наименование раздела	Всего часов	Аудиторные занятия			Самостоят. работа
			лекции	практич. занятия	лабор. работы	
Модуль 1						
1.	Информационные угрозы и уровни обеспечения информационной безопасности.	12	2	2	0	8
2.	Законодательно-правовой аспект. Информационное законодательство.	18	4	2	4	8
3.	Административно-организационный аспект. Политика ИБ предприятия.	20	2	2	4	12
Модуль 2						
4.	Программно-технический аспект ИБ. Вирусы и антивирусы.	34	8	2	8	14
5.	Технологии обеспечения ИБ. Криптография и шифрование.	24	6	2	4	14
	Итого:	108	14	10	20	44
Форма итогового контроля:		Зачет с оценкой				

5.3. Лабораторный практикум (20 часов)

Лабораторная работа №1 (4 ч.)

Dr. Web для Windows

Программа представляет собой классический полифаг и предназначена для использования в 32-битных операционных системах семействах Windows. Программа производит сканирование файлов и системных областей дисков компьютера на наличие в них компьютерных вирусов и при нахождении последних их лечит.

Dr. Web реализует эвристический метод поиска вирусов, который заключается в обнаружении фрагментов программ, типичных для компьютерных вирусов. Эвристический анализатор используется полисами для обнаружения вирусов, не входящих в базу данных полифага. Эффективность эвристического анализатора определяется двумя параметрами: процентом обнаруженных вирусов и процентом ложных срабатываний (подозрений на вирусы в файлах, в которых их нет).

Антивирусная проверка с помощью Dr.Web

Запустите программу Dr. Web., нажав кн «Антивирусная проверка с помощью Dr.Web»

Задание №1. С помощью антивирусной программы Dr.Web произвести проверку файлов с расширением .doc локального диска [C:], присвоив программе Dr.Web самый высокий приоритет. Проверить также память и загрузочные секторы диска.

Методика выполнения работы:

1. Запустите программу Dr. Web *(Пуск — Программы — Dr.Web).*
2. Нажав кнопку *Дерево дисков,* выберите диск [C:].

3. Нажмите кнопку *Установка* и во вкладке *Проверка* установите флажки: *Проверять память, Проверять загрузочные секторы,* во вкладке *Типы* укажите файлы с расширением *.doc.

4. Во вкладке *Общие* установите самый высокий приоритет *программы* Dr. Web.

5. Нажав кнопку *Статистика,* просмотрите результаты работы программы.

6. Отчет оформите в виде фотографии экрана, содержащей изображение окна *Статистика.*

Задание №2. С помощью антивирусной программы Dr. Web. произвести проверку всех файлов диска [C:] в режиме обнаружения неизвестных вирусов, при этом проверять архивные файлы.

Методика выполнения работы:

1. Нажав кнопку Дерево дисков, выберите диск [C:].
2. Нажав кнопку Установка во вкладке Проверка, установите флажок: эвристический анализ.
3. Нажав кнопку Установка во вкладке Типы, установите флажки: Все файлы. Файлы в архивах.
4. Нажав кнопку Список отчета, просмотрите результаты работы программы.

Отчет о работе оформите в виде фотографии экрана, содержащей изображение окна *Список отчета.*

Лабораторная работа №2 (4 ч.)

AntiViral Tookit Pro

AVP — новый шаг в борьбе с компьютерными вирусами. Она представляет собой 32-разрядное приложение, оптимизированное для работы в среде Microsoft Windows и использующее все ее возможности. AVP предоставляет пользователю максимум сервиса — возможность обновления антивирусных баз через Internet (в том числе и автоматический), возможность задания параметров автоматического сканирования и лечения зараженных файлов.

Обновления на сайте AVP появляются практически еженедельно, а база данных включает описания более 40 тысяч вирусов.

AVP состоит из нескольких важных модулей:

1) **AVP Сканер** проверяет и «лечит» оперативную память (DOS, XMS, EMS); файлы, включая архивные, упакованные и документы, созданные в формате Microsoft Office; системные сектора, содержащие Master Boot Record, загрузочный сектор (Boot-сектор) и таблицу разбиения диска (Partition Table).

2) **AVP Monitor** — резидентный модуль, постоянно находящийся в памяти компьютера и отслеживающий все файловые операции в системе. Позволяет обнаружить и удалить вирус до момента реального заражения системы в целом.

3) **AVP Inspector** позволяет отлавливать неизвестные вирусы. Этот модуль использует в работе метод контроля изменений размеров файлов, Внедряясь в файл, вирус неизбежно увеличивает его «объем» и вызывает изменение его размера — и тем выдает себя.

Основное меню содержит команды по установлению и сохранению настроек пользователя, по обновлению антивирусной базы и прекрасно организованную систему справочной информации.

Антивирусная проверка программой AVP

Задание №1. С помощью антивирусной программы AVP Сканер произвести проверку локального диска [C:], включая сканирование системной памяти, системных секторов и

файлов в режиме обнаружения неизвестных вирусов и предупреждения о поврежденных файлах или подозрительных последовательностей машинных инструкций в памяти компьютера.

Методика выполнения работы:

1. Запустите программу AVP *(Пуск — Программы — Anti Viral Tookit Pro — AVP Сканер).*
2. В главном окне установите флажок *Локальные диски.* Если имеется несколько локальных дисков, снимите выделение со всех, за исключением диска [C:].
3. Во вкладке *Объекты* установите флажки: *Лечить, Только отчет, Сканировать Секторы, Файлы.*
4. Во вкладке *Параметры* установите флажки: *Создавать файл отчета, Установить процесс сканирования <Высокий>* (через справку (F1) узнайте назначение).
5. Во вкладке *Настройка* установить: *Выводить предупреждение.*
6. Нажмите кнопку *Пуск* (начать сканирование).
7. Во вкладке *Статистика* просмотрите результаты работы программы.
8. Оформите отчет в виде фотографии экрана, содержащей изображение окна *Статистика.*

Обслуживание магнитных дисков

При работе на компьютере требуется сохранять в целостности информацию, защищать ее от возможных разрушений, вызванных сбоями системы при работе, образованием дефектных участков на поверхности магнитных дисков, воздействием программных вирусов или ошибками пользователей.

Поэтому необходимо периодически проводить работу по обслуживанию жесткого диска. Сервисные программы можно условно подразделить на три группы: программы обслуживания магнитных дисков; программы-архиваторы; антивирусные программы.

1. Программы обслуживания магнитных дисков

Программы, предназначенные для улучшения работы компьютера, называют утилитами. Утилиты могут распространяться как поодиночке, так и в составе больших и мощных пакетов. Один из лучших Intemet-сайтов, посвященных утилитам — www.download.com — включает в себя информацию о тысячах программ. И каждый день на свет появляются новые.

На российском рынке наиболее популярными пакетами утилит по обслуживанию компьютера являются: пакет служебных программ Norton Utilities от фирмы Symantec (http:/www.symantec.com/region/ru/ prodact/nubrochure), пакет Nuts & Bolts фирмы Network Association, (http:/www.mcaffe.com) и пакет Microsoft PLUS' 98 (http:/www. microsoft.com).

Фирма Microsoft в свою стандартную поставку Windows 98 включает некоторые программы по обслуживанию компьютера из пакета Microsoft PLUS' 98. По сути, этот пакет частично дублирует действие программ из пакета Norton Utilities, частично является купленной и переработанной версией программы из пакета Norton Utilities. Следует, однако, помнить, что пакет программ Norton Utilities работает гораздо «интеллектуальнее» и, часто так бывает, что ошибки, обнаруженные при помощи этого пакета, не удается найти и исправить с помощью служебных программ Microsoft.

Пакет служебных программ Microsoft, входящий в стандартную поставку Windows, предназначен для обслуживания компьютера (программной среды и аппаратной части) при минимальном участии пользователя. Он обеспечивает обслуживание операционной системы, проверку и оптимизацию работы жестких и гибких дисков, оптимизацию работы прикладных программ, защиту данных и программ от повреждений и потерь.

1.1. Программа ScanDisk

ScanDisk (аналогом является программа Norton Disk Doctor из пакета Norton Utilities или Disk Minder из пакета Nuts & Bolts) — программа, предназначенная для тестирования целостности таблицы разделов магнитного диска и исправности физической поверхности

диска. Под проверкой целостности таблицы разделов понимается отслеживание и ликвидация различных повреждений файловой системы, «потерянных» фрагментов данных, которые могут появиться при некорректном завершении работы некоторых программ. Под проверкой физической целостности следует понимать контроль на наличие физических повреждений магнитного слоя на жестком или гибком диске. При обнаружении ошибок прежде, чем начать исправление, программа обычно информирует о них пользователя. Но ее можно настроить и на автоматическое исправление без каких-либо запросов.

Для запуска этой программы следует нажать кнопку *Пуск* и выбрать команды *Программы → Стандартные → Служебные → ScanDisk.* В окне программы следует, установив флажки, выбрать метод проверки: *Полная,* установленная как правило, по умолчанию, предусматривает проверку поверхности диска и проверку папок и файлов на наличие ошибок или *Стандартная* — проверка только папок и файлов (рис. 3.1).

Настройка тестов, установленная по умолчанию, подходит обычно всем пользователям, но при желании ее можно изменить, нажав кнопку *Дополнительно.* При этом открывается окно *Дополнительные параметры настройки диска. В* этом окне предлагаются варианты, как вы водить итоговые результаты, как показать файл протокола, какие меры следует предпринять, если система обнаружит файлы с общими кластерами, потерянные цепочки кластеров и т.д.

Кроме того, при проверке качества магнитной поверхности диска система предлагает выбрать параметры проверки. Параметры задают проверку определенных областей данных: проверку только системной области диска либо области данных, либо той и другой. Выбор режима осуществляется при нажатии кнопки *Настройка.*
В результате проверки программа выведет на экран сообщение о размере дискового пространства, о том, какой объем на диске занимают файлы и папки, сколько байт занято поврежденными секторами, размер кластера в байтах и количество кластеров на диске.

1.2. Программа Defrag

Defrag (аналогом является программа Norton Speed Disk из пакета Norton Utilities или Disk Типе из пакета Nuts & Bolts) — средство для ускорения работы программ посредством правильной организации
данных на диске.

Операционная система распределяет пространство диска на области, называемые кластерами, связывает их посредством элементов в таблице размещения файлов (FAT). Файл записывается на диск посредством связанной последовательности кластеров.

Если внести информацию в существующий файл после записи другого файла на диск, то в конечном счете первоначальный файл наверняка станет фрагментированным.
Обычно операционные системы скрывают все это от пользователя и предоставляют ему данные всякий раз, когда это потребуется. Однако иногда возникают проблемы из-за слишком большого числа фрагментированных файлов, особенно, когда дело доходит до восстановления случайно удаленных файлов. Кроме того, фрагментированные файлы существенно снижают производительность работы персонального компьютера.
Поэтому настоятельно рекомендуется регулярно выполнять дефрагментацию файлов на жестких дисках.
Существует множество способов оптимизации расположения файлов на диске. Дефрагментация — только начало работы. Можно прибегнуть к размещению файлов, которые содержат часто используемые программы, ближе к началу диска. Это позволит операционной системе намного быстрее находить и загружать их. Файлы данных, к которым приходится часто обращаться, тоже лучше разместить ближе к началу диска. Defrag предполагает, что окончательная оптимизация диска достигается, если файлы дефрагментированы и перемещены как можно ближе к началу диска.
Перед запуском программы рекомендуется: удалить ненужные файлы;

восстановить случайно удаленные файлы; программой ScanDisk проверить и при необходимости устранить нарушения в логической структуре диска, иначе программа Defrag, обнаружив нарушения, прекратит дефрагментацию.

Для запуска программы следует нажать кнопку *Пуск* и выбрать команды *Программы → Стандартные → Служебные →Defrag.* В открывшемсяокне программа предлагает либо сразу начать дефрагментацию, согласившись с выбранными по умолчанию установками, либо выбрать дополнительные настройки. При первом запуске рекомендуется согласиться с принятыми по умолчанию установками и щелкнуть на кнопке <*ОК*>. После этого открывается окно, в котором показано, какой процент поверхности программа обработала в настоящий момент времени. Программа предлагает также карту поверхности диска, на которой представлены результаты работы в каждом кластере.

На диске большого объема и сильно фрагментированном оптимизация может занять несколько часов, поэтому проводить ее лучше в конце работы с компьютером.

1.3. Программа Disk Cleanup

Disk Cleanup (аналогом является программа Norton Space Wizard из пакета NU или Cleanup Wizard из пакета Nuts & Bolts) — интеллектуальный чистильщик дисков от засоряющих его ненужных файлов. К таким относятся файлы с расширением .tmp, создаваемые при работе самой Windows и другими программами (вообще-то эти файлы должны удаляться автоматически после завершения работы программы, но часто система «забывает» сделать это), «резервные копии» документов и системных файлов, а также лишние копии файлов.

Для запуска программы следует нажать кнопку *Пуск* и выбрать команды *Программы —> Стандартные —> Служебные —> Disk Cleanup.*

В открывшемся окне предлагается указать имя диска, который будет подвергаться чистке, в следующем окне (рис.3.3) нужно установить флажки, соответствующие выбранному методу чистки диска:

В зависимости от того, сколько будет установлено флажков, программа будет разыскивать временные файлы и папки, файлы из *Корзины* или файлы иных типов, например некоторые web-страницы, хранящиеся на диске для быстрого просмотра.

1.4. Программа Un Erase Wizard

UnErase Wizard из пакета Norton Utilities восстанавливает удаленные файлы, если они защищены средствами Norton Protection или программой SalVage фирмы Novell (для сетевых файлов), или они находятся в *Корзине* Windows(аналогом является программа Undelete из пакета Nuts & Bolts, в пакете Microsoft PLUS' 98 программа для восстановления случайно удаленных файлов отсутствует). Если файл пригоден для восстановления, но автоматически восстановить его не удается, программа UnErase Wizard поможет сделать это вручную. Чтобы шансов на восстановление было больше, нужно всегда пользоваться Norton Protection.

При удалении файла операционная система не стирает сами данные с диска, а заменяет код символа в соответствующем имени на свой код. Вся остальная информация о файле и каталоге, включая номер первого занятого файлом кластера, остается без изменения.

Таким образом, чтобы восстановить файл, программа должна восстановить запись о файле в каталоге.

Для успешного восстановления стертых файлов и каталогов очень важно, чтобы после удаления на диск не производилась никакая запись и чтобы файлы не были фрагментированы.

Для восстановления можно осуществлять поиск файла по имени или по содержащемуся в нем тексту.

Лабораторная работа №3 (4 ч.)

№ 1. Тестирование диска

Задание №1.1. Произвести проверку поверхности диска [C:]. Во время проверки требуется освобождать потерянные цепочки кластеров, итоговые результаты выводить на экран.

Методика выполнения работы:

1. Произведите запуск программы ScanDisk.
2. Откройте окно *Дополнительные параметры проверки диска* (клавиша *Дополнительно* в окне программы ScanDisk) и установите флажки *Всегда* во вкладке *Выводить итоговые результаты* и *Освобождать* во вкладке *Потерянные цепочки кластеров.*
3. Закройте *окно Дополнительные параметры проверки диска* и нажмите кнопку *Запуск.*
4. В отчете, представляющем собой текстовый файл, созданный любым текстовым редактором, укажите, сколько кластеров находится на диске, размер одного кластера в байтах, сколько кластеров свободно и количество потерянных кластеров.

Задание № 1.2. Произвести проверку файлов и папок диска на наличие ошибок. При этом требуется удалять файлы с общими кластерами и проверять уникальность имен файлов. Итоговые результаты выводить на экран.

Методика выполнения работы:

1. Произведите запуск программы ScanDisk.
2. В окне программы ScanDisk установите флажок *Стандартная проверка файлов и папок.*
3. В окне Дополнительные параметры установите флажки: во вкладке Выводить итоговые результаты — флажок Всегда; во вкладке Файлы с общими кластерами → флажок Удалять; во вкладке Проверять → флажок Уникальность имен файлов.
4. Нажмите кнопку <*OK*>.
5. В отчете, представляющем собой файл, созданный любым текстовым редактором, укажите размер свободного пространства на диске, сколько места занято программа.

Задание № 1.3. Произвести проверку на наличие ошибок системной области диска.

Методика выполнения работы:

1. Произведите запуск программы ScanDisk.
2. В основном окне программы ScanDisk установите флажок *Полная проверка диска.*
3. В окне *Режим проверки поверхности диска* (клавиша *Настройка)* во вкладке *Выполнить проверку следующих областей* установите флажок *Только системная область.*
4. Нажмите кнопку <*OK*>.
5. В отчете, представляющем собой файл, созданный любым текстовым редактором, укажите размер общего пространства на диске, сколько имеется кластеров, ошибки, обнаруженные программой.

№ 2. Дефрагментация дискового пространства

Задание №2.1. Произвести дефрагментацию жесткого диска, не перемещая файлы программ в начало диска.

Методика выполнения работы

1. Произведите запуск программы Defrag.
2. Выберите кнопку *Настройка.*
3. В окне *Настройка дефрагментации* снимите флажок *Переместить файлы программ для ускорения и запуска.*
4. В этом же окне установите флажок *Использовать эти параметры только один раз.*
5. Нажмите кнопку <*OK*>.

№3. Очистка диска от ненужных файлов

Цель работы. Изучение методики очистки диска от ненужных файлов.

Задание №3.1. Произвести очистку диска, удалив файлы из *Корзины* и временные файлы.

Методика выполнения работы:

1. Произведите запуск программы Disk Cleanup.
2. Выберите диск, предназначенный для очистки.
3. В окне Удалить следующие файлы установите флажки Корзина и Временные файлы.
4. Нажмите кнопку <OK>.

№ 4. Восстановление случайно удаленных файлов

Задание №4.1. Программой UnErase Wizard произвести восстановление удаленного файла, созданного при помощи текстового редактора Word.

Методика выполнения работы:

1. Произведите запуск программы Norton Utilities.
2. В левом окне выберите группу программ *Устранение неполадок.*
3. В правом окне одним щелчком запустите программу UnErase Wizard.
4. В следующем окне программы UnErase Wizard установите флажок *Восстановимые файлы по критериям.*
5. В окне *Тип файла* выберите файл типа *Документ Word* и нажмите кнопку *Далее.*
6. Программа выберет удаленные файлы, соответствующие выбранному критерию, и представит их в окне с указанием имени, размещения, даты удаления, размера.
7. Выберите файл, который требуется восстановить, и нажмите кнопку *Восстановить.*

Самостоятельная работа

1. Произвести проверку магнитного диска только в области данных.
2. Произвести полную проверку поверхности диска. При этом проверять дату и время создания файлов, правильность и уникальность имен файлов.
3. Произвести стандартную проверку поверхности диска. При этом сообщать об ошибках длины имен файлов для режима MS DOS.
4. Восстановить файлы, удаленные из каталога C:\WIN\TEMP.
5. Восстановить все удаленные файлы, созданные при помощи программы Excel.
6. Восстановить все удаленные файлы.

Контрольные вопросы

1. Какие виды повреждений файлов и дисков Вам известны?
2. Каково назначение программы проверки поверхности диска ScanDisk?
3. Как обнаружить и устранить логические дефекты дисков?
4. В какие файлы помещается информация из цепочек потерянных кластеров?
5. Какие тесты выполняет программа ScanDisk?
6. В какие файлы помещается информация из цепочек потерянных кластеров, где они располагаются и для чего предназначены?
7. Что такое фрагментация диска и каковы причины ее появления?
8. На что влияет фрагментация файлов?
9. Какие программы используются для устранения фрагментации?
10. Какие методы оптимизации предлагает программа Defrag?
11. Как защитить информацию от случайного удаления?
12. Какие способы поиска удаленных файлов предлагает программа UnErase Wizard?
13. С какой целью производится очистка диска от ненужных файлов?
14. Назовите программы, производящие очистку диска.
15. Какие файлы подлежат удалению как ненужные?

16. Какие программы для восстановления случайно удаленных файлов Вы знаете?

17. Какие меры следует предпринять для 100% -ного восстановления случайно удаленных файлов?

18. На чем основан принцип восстановления удаленных файлов и каталогов?

19. Какие существуют способы управления программой UnErase?

20. Какие возможны прогнозы восстановления удаленных файлов?

21. Что надо сделать, чтобы восстановить один удаленный файл, группу файлов или каталог?

Лабораторная работа №4 (4 ч.)

1. Архивирование файлов

Задание №1.1. Помещение файлов в архив.

С помощью программы WinRAR поместить в архив файлы с расширением .COM из каталога C:\Windows\COMMAND.

Методика выполнения работы:

1. Запустите программу WinRAR.
2. При помощи команды меню *File* выберите диск [C:].
3. В окне каталога откройте папку Windows\COMMAND.
4. Выберите файлы с расширением .corn (клавиша *Spacebare* или при помощи команды меню *File).*
5. Нажмите кнопку *Add* .
6. В диалоговом окне *Enter archive name... (Введите имя архива)* в командной строке *Archive* введите имя архива myarch.
7. Нажмите кнопку <*OK*>.
8. Просмотрите содержимое архивного файла (установите курсор на имя архивного файла, нажмите клавишу *Enter).*
9. Просмотрите информацию об архивном файле (кнопка *Info).*
10. В отчете укажите суммарный размер файлов с расширением .corn и размер архивного файла, а также сколько файлов содержит архив, степень сжатия.

Задание №1.2. Создание многотомных архивов.

С помощью программы WinRAR создать многотомный solid-архив, в который поместить все файлы из каталога C:\ Windows\COMMAND. Размер тома — 1213800.

Методика выполнения работы:

1. Запустите программу WinRAR.
2. При помощи команды меню *File* выберите диск [C:].
3. В окне каталога откройте папку Windows\COMMAND.
4. Пометьте все файлы (клавиша *Grey+).*
5. Нажмите кнопку *Add.*
6. В открывшемся диалоговом окне в строке *Archive* введите имя архивного файла arcl.
7. В строке Volume size выберите размер тома 1213800.
8. Установите флажок *Solid archiv.*
9. Нажмите кнопку <*OK*>.
10. Просмотрите содержимое архивного файла (установите курсор іа имя архивного файла, нажмите клавишу *Enter).*

11. Просмотрите информацию об архивном файле (кнопка *Info).*

12. В отчете укажите количество томов созданного архива и раз-іер последнего тома, сколько файлов в нем

содержится, суммарный размер исходных файлов и размер сжатого файла, степень сжатия файла.

Задание №1.3. Создание самораскрывающихся архивов

С помощью программы WinRAR создать самораскрывающийся архив, в который поместить файлы с расширением .exe из каталога C:\ Windows\COMMAND.

Методика выполнения работы:

1. Запустите программу WinRAR.
2. При помощи команды меню *File* выберите диск [C:].
3. В окне каталога откройте папку Windows\COMMAND.
4. Пометьте файлы с расширением .exe (клавиша *Grey* +).
5. Нажмите кнопку *Add.*
6. В открывшемся диалоговом окне в строке *Archive* введите имя архивного файла arcl.
7. Снимите флажок *Solid archiv.*
8. Установите флажок *SFX_archiv.*
9. Нажмите кнопку <*OK*>.
10. Просмотрите содержимое архивного файла (установите курсор на имя архивного файла, нажмите клавишу *Enter).*
11. Просмотрите информацию об архивном файле (кнопка *Info).*
12. В отчете укажите количество томов созданного архива и размер последнего тома, сколько файлов в нем содержится, суммарный размер исходных файлов и размер сжатого файла, степень сжатия файла.

Самостоятельная работа

Задание №1.

1. С помощью архиватора WinRAR поместите в архив файлы с расширением .hlp из каталога WINDOWS\HELP. Архивному файлу присвойте имя myarh.
2. Добавьте в архив myarh файлы с расширением .chm из каталога MNDOWS\HELP.
3. В отчете укажите размер архивных файлов до и после добавления второй группы файлов, количество файлов в архивах, степень сжатия.

Задание№2.

1. С помощью архиватора WinRAR создайте архивы myarh1, myarh2 и т.д., в которые поместите файлы с расширением .cnt из каталога WINDOWS\HELP.
2. Исследуйте, как на размер файла влияет настройка метода сжатия: очень быстрое сжатие, быстрое сжатие, нормальное сжатие, хорошее сжатие, лучшее сжатие.
3. Отчет должен содержать информацию о размерах архивных файлов, полученных при использовании различных методов сжатия.

Задание №3.

1. С помощью архиватора WinRAR создайте архивы myarh1, myarh2 и т.д., в который поместите все файлы с расширением .gid из каталога WINDOWS\HELP .
2. Исследуйте влияние различных значений параметра Dictionery Size [Область поиска повторяющихся последовательностей символов}: 64 Кбт, 128 Кбт, 256 Кбт, 512 Кбт, 1024 Кбт.

3. Отчет должен содержать сведения о размерах полученных архивных файлов и степени их сжатия.

Задание № 4.

1. С помощью архиватора WinRAR создайте архив myarh, в который поместите файлы с расширением .hlp из каталога WINDOWS\HELP.

2. Откройте архивный файл и пометьте все файлы, размер которых до сжатия превышал 10 000 байт.

3. Извлеките из архива помеченные файлы и поместите их в предварительно созданный на своем рабочем диске каталог.

4. Отчет должен быть представлен в виде фотографии экрана каталога с извлеченными файлами.

Задание № 5.

1. При помощи программы-архиватора WinRAR создайте два solid-архива, используя значения параметра Dictionery Size 256 и 1024. В архив поместите все файлы каталога WINDOWS \HELP.

2. Сравните влияние параметра Dictionery Size на размер архива.

3. Отчет представьте в виде фотографий экранов с изображением окон, содержащих информацию об архивах.

Задание №6.

1. При помощи архиватора WinRAR создайте два многотомных архива, используя нормальный и лучший метод сжатия. Установить размер тома — 1475500. В архив поместите все файлы из каталога WINDOWS\HELP.

2. Сравните два метода сжатия.

3. В отчете представьте информацию о количестве томов двух архивов, а также фотографии экранов с изображением окон, содержащих информацию о последних томах архивов.

Лабораторная работа №5 (4 ч.)

1. Архивирование файлов

Задание №1. Помещение файлов в ZIP-архив.

Поместить в ZIP-архив файлы из своей рабочей папки.

Методика выполнения работы:

1. На своем рабочем диске создайте две папки для экспериментов *Мои эксперименты* и *Мой архив.*

2. Скопируйте в папку *Мои эксперименты* несколько файлов из любого каталога.

3. Запустите программу WinZIP.

4. В окне программы WinZIP нажмите кнопку *New* на панели инструментов или выполните команду меню *File —> New Archive (Файл —> Новый архив).*

5. В открывшемся окне выберите папку, в которой будет храниться новый архив, пусть это будет папка *Мой архив.*

6. Введите имя архива в поле *Имя файла.* Пусть архив называется myarc.

7. В поле *Тип файла* должен быть установлен тип *Zip files.*

8. Установите флажок *Add Dialog (Открывать окно включения в архив)*. Нажмите кнопку <*OK*>.

9. Откроется диалоговое окно *Add.*

10. В диалоговом окне *Add (Включение в архив)* в раскрывающемся списке *Action (Действие)* выберите пункт *Add (and replase) files (Добавлять и заменять файлы).*

11. В раскрывающемся списке *Compression (Степень сжатия)* выберите пункт *Normal (обычное).*

12. В группе элементов управления *Folders (Папки)* установите флажок *Include Subfolders (Включая вложенные папки).*

13. Выделите файлы, включаемые в архив: а) выделить все файлы — комбинация клавиш *Ctrl + A;*

б) выделить группу файлов — левая кнопка мыши совместно с клавишей *Shift.*

14. Щелкните на командной кнопке *Add (Добавить в архив)* — начнется процесс архивации.

15. После окончания архивации WinZIP представит окно архивного файла myarc.zip. В этом окне будет показано содержание архива, размер файлов до архивации и после, степень сжатия файлов в архиве.

16. Отчет следует предоставить в виде фотографии экрана с изображением содержания архивного файла.

Задание №2. Просмотр архивного файла в формате ZIP

Просмотреть содержание архивного файла, а также содержание файла, находящегося внутри архива.

Методика выполнения работы

1. Запустите программу WinZIP.

2. Выполните команду *File —> Open Archive (Файл —> Открыть архив)* или нажмите кнопку *Open* на панели инструментов архиватора.

3. В диалоговом окне *Open* при помощи раскрывающегося списка *Папка* найдите папку *Мой архив,* созданную в предыдущей работе (Работа № 1, задание № 2) и откройте ее.

4. Выделите значок файла myarc.zip и щелкните на кнопке *Отрыть.*

5. В окне программы WinZIP откроется список файлов, входящих в архив (см. рис. 3.8), размер файлов до архивации и после и т.д.

6. Выделите значок того файла, который хотите просмотреть. Дважды щелкните на этом значке, и файл откроется в окне ассоциированной программы, которую архиватор выберет сам. Для файлов с расширением .doc это будет Word, для файлов *.txt* — программа Блокнот и т.д.

7. Если нужно просмотреть файл при помощи другой программы, выполните команду *Actions —> View* или нажмите кнопку *View* на панели инструментов. Вам будет предложен перечень программ, при помощи которых можно просматривать файлы.

Задание №3. Извлечение файлов из ZIP-архива

Извлечь файлы из Zip-архива, созданного в задании № 2.

Методика выполнения работы:

1. Запустите программу WinZIP.
2. Откройте ранее созданный архивный файл myarc.zip (меню *File -> Open* или кнопка на панели инструментов).
3. Выделите файлы, которые хотите извлечь. Если требуется выделить группу файлов, используйте комбинацию *левая кнопка мыши + <Shift>.*

4. Выполните команду *Actions -> Extract.* Откроется диалоговое окно *Extract.*
5. Выберите папку для размещения извлекаемых файлов, пусть это будет папка *Мои документы.*
6. Щелчком на командной кнопке *Extract* запустите процесс извлечения файлов.
7. При помощи *Проводника* убедитесь в том, что файлы, извлеченные из архива, поступили в папку *Мои документы.*

Задание №4. Создание самораскрывающегося Zip-архива.

Создать самораскрывающийся Zip-архив на базе архивного файла Myarc.zip, созданного в задании 2.1..
Методика выполнения работы:

1. Запустите программу WinZIP одним из способов.
2. Откройте архив myarc.zip (кнопка *Open* на панели инструментов).
3. Выполните команду *Actions -> Make.Exe File (Действия -> Создать исполняемый файл).* Откроется диалоговое окно *WinZIP Self — >Extractor Personal Edition (Создание самораспаковывающегося архива).*
4. В поле *Create Self— Extracting Zip files from* должен быть установлен адрес имеющегося исходного архива myarc.zip. Если это не так, воспользуйтесь кнопкой *Brouse (Просмотр)* для поиска нужного Zip-файла.
5. В группе *Self — Extracting Type (Тип самораспаковывающегося файла)* включите переключатель, соответствующий операционной системе Вашего компьютера.
6. В группе *Spanning Support (Поддержка распределенного архива)* установите флажок *No spanning (Без распределения).*
7. Нажмите кнопку <*OK*>.

5.4. Практические занятия (10 час)

На практическихх занятиях проводятся следующие **интерактивные работы**:

1. Прослушивание докладов по темам рефератов, вопросы к докладчику, обсуждение, оценка реферата, доклада, презентации к докладу, тесту, дискуссия.
2. Пробное тестирование и оценка качества представляемых тестов.

Домашнее задание № 1. – для практического занятия по теме 1.
Создать Дневник наблюдений за состоянием своего ПК при установке и использовании антивирусного программного обеспечения.

Домашнее задание № 2. для практического занятия по теме 2.
Разработать модель защищенной локальной сети, имеющей один сервер и несколько рабочих станций.

Домашнее задание № 3. для практического занятия по теме 3,4.
Разработать административные меры (Политику безопасности) по защите информации небольшого предприятия.

Домашнее задание № 4. для практического занятия по теме 5.
Разработать политику информационной безопасности – меры по защите личной, персональной и финансовой информации.

Тесты для практических занятий студентов

1. Основным законом РФ по защите информации является:
а. Конституция
б. Уголовный кодекс
в. Закон о защите информации
г. Гражданское право

2. Разграничивает права доступа пользователей к информационной системе:
а. Руководитель предприятия
б. Системный администратор
в. Бухгалтер
г. Налоговый инспектор

3. Современное офисное информационное обеспечение состоит из::
а. ПК
б. Нескольких ПК
в. Сервера
г. Сервера и нескольких ПК

4. Программный метод защиты информации:
а. Средства ОС
б. Ручная настройка утилит
в. Антивирусное РО
г. Форматирование дисков

5. NOD 32 относится:
а. Стандарт информационной отрасли
б. Антивирусное ПО
в. Модель материнской платы
г. Код доступа в Windows

6. Установка металлических дверей в серверной относится к какому уровню защиты::
а. Административному
б. Программному
в. Механическому
г. Правовому

7. Вирус это:
а. Вредоносная программа
б. Медицинский термин
в. Инструмент восстановления ОС после сбоя
г. Программа защиты данных

8. Антивирусное программное обеспечение защищает:
а. Только программы пользователя
б. Файлы и утилиты ОС
в. Все файлы в программной системе

9. Код и шифр отличаются:
а. Это одно и то же
б. Код использовался до изобретения шифров
в. Код представляет некоторое сообщение короче чем шифр

г. Код не относится к засекречиванию информации

10. В фильме Шерлок Холмс приводится шифр:
а. Перестановки
б. Замены
в. Основанный на случайных последовательностях
г. Простой

11. Симметричные ключи используются:
а. Для шифрования и дешифрования
б. Только для шифрования
в. Только для дешифрования
г. Для проверки информации

12. Ассиметричные ключи:
а. Один у отправителя другой у получателя
б. Вариант симметричных ключей
в. В настоящее время не применяются
г. Используются в некоторых ОС

13. Цифровая подпись:
а. Ставится на бумажные документы
б. Используется в рамках офиса
в. Удостоверяет отправителя информации
г. Удостоверяет получателя информации

14. После шифрования документ становится
а. Намного короче
б. Намного длиннее
в. Остается примерно такого же размера
г. Увеличивается в 2*sin(w) раз

15. В информационном обществе руководители предприятий обмениваются:
а. Заказными письмами
б. Электронными документами
в. Гиперссылками

5.5. Самостоятельная работа студентов, ее содержание, объем в часах и формы контроля

1. Изучить самостоятельно правовые аспекты, связанные с лицензированием программного обеспечения (6ч.).
2. Исследовать на предмет защищенности информации компьютерную систему на каком-либо предприятии (10 ч.)
3. Изучить средства защиты сети в ГАГУ (10 ч.)
4. Найти в Интернете материалы о последних версиях вирусов (4 ч.)
5. Узнать, каким способом защищена информационная система 1С:Бухгалтерия (4 ч.)
6. Установить на компьютер антивирусную программу NOD32 и с ее помощью просканировать диски компьютера на предмет наличия вирусов. (6 ч.)

7. Найти в литературе и Интернете материалы об устройстве и функционировании немецкой шифровальной машинки «Энигма» времен второй мировой войны (6 ч.)

8. Изучить вопрос, каким способом использовались книги художественного содержания для шифрации сообщений (4 ч.)

9. Разработать проект информационной защиты типового офиса, где имеются несколько пользовательских ПК, работающих на один сервер, и имеется выход в Интернет (8ч.)

Контрольная работа для самостоятельной работы

Задание № 1.

1. Требуется создать архив для файлов из Вашей рабочей папки, при помощи архиватора WinZIP.
2. Архив защитите паролем.
3. Отчет предоставьте в виде текстового файла с описанием методики выполнения работы.

Задание № 2.

1. В свою рабочую папку скопируйте несколько текстовых файлов.
2. Используя нормальный и максимальный методы сжатия, создайте два архива из файлов своей рабочей папки при помощи двух архиваторов: WinRAR и WinZIP.
3. Проанализируйте эффективность работы двух программ архивации
4. Отчет предоставьте в виде таблицы, содержащей информацию о годах сжатия и размерах файлов до и после сжатия.

Задание № 3.

1. В свою рабочую папку скопируйте несколько текстовых файлов.
2. Используя два архиватора WinRAR и WinZIP, создайте два архива, содержащие файлы из Вашей рабочей папки,— RAR и ZIP.
3. Зафиксируйте время, потраченное на выполнение команд.
4. Сравните время создания архивов, степень сжатия, а также размер файлов до и после упаковки.
5. Удалите исходные файлы из своей рабочей папки.
6. Извлеките файлы из архивов RAR и ZIP. При извлечении засеките время, потраченное на выполнение команды.
7. Выполните эту же работу относительно файлов с расширением и файлов с расширением .bmp.
8. Отчет представьте в виде таблицы, содержащей информацию размерах архивных файлов, полученных при архивации разными программами, времени, потраченного на создание архивов и на распаковку.
9. Сравните действие двух архиваторов для создания архивов, содержащих разные типы файлов.
10. Отчет представьте в виде таблицы, содержащей информацию о размерах архивных файлов, полученных при архивации разными программами, времени, потраченного на создание архивов и на распаковку.

Контрольные вопросы

1. Для чего предназначены программы-архиваторы?
2. За счет чего происходит сжатие файла при архивации?
3. Какие виды программ упаковки файлов Вы знаете?
4. Что такое самораспаковывающийся архив?
5. Чем отличается solid-архив от обычного?

6. Что характеризует показатель — степень сжатия файла? Какие типы файлов сжимаются больше, а какие меньше?

7. Какие существуют виды программ-архиваторов?

8. Для чего создаются многотомные архивы?

9. Как защитить файлы в архиве от несанкционированного доступа?

10. Как проверить сохранность архивного файла?

11. Как просмотреть содержимое архивного файла?

12. Сравните достоинства и недостатки двух программ-архиваторов WinRAR и WinZIP.

Форма контроля самостоятельной работы студентов

В конце каждого раздела предусмотрено тестирование и проверка домашних заданий.

6. Тематика рефератов (16 час - самостоятельной работы)

Задание на составление реферата включает в себя: сбор материала, изучение литературы, интернет-источников, электронных журналов; разработка реферата, презентации к защите проекта, доклада к выступлению на 5-7 минут, разработка теста и тест-презентации.

1. Сравнение зарубежного и отечественного законодательств по защите информации.
2. Внешние средства защиты информационных комплексов.
3. От отдельных программ к комплексным мерам защиты информации.
4. Вирусы: классификация, функциональность.
5. Сравнительная характеристика антивирусных программ.
6. Защита информации в сетях.
7. Особенности защиты информации в крупных информационных предприятиях, таких как банки.
8. Сравнительная характеристика методов шифрования информации.
9. Методы защиты от взломщиков.
10. Защита от нежелательных сообщений (спам) в Интернет.
11. Информационная защита операционных систем.
12. Способы защиты баз данных.
13. Криптографические алгоритмы.
14. Защита информации в ГАГУ.
15. Защита информации в социальных сетях.
16. Законодательно-правовой аспект ИБ.

Защита реферата

Публичная защита реферата проводится во время практических занятий (для отставших студентов – на зачете) в аудитории, оснащенной мультимедийным проектором, ноутбуком, экраном. Оцениваются все компоненты проекта: реферат, доклад, презентация к докладу, тест по теме реферата, тест-презентация, дискуссия, тестирование.

7 Учебно-методическое обеспечение дисциплины

7.1 Интернет-источники, интернет-сервисы, энциклопедии, кодексы

1. **Конституция РФ.**
2. **Уголовный кодекс РФ.**
3. www.consultant.ru – информационно-правовое обеспечение «КонсультантПлюс»
4. www.student.garant.ru – информационно-правовое обеспечение «ГАРАНТ» (доступно как для стационарных компьютеров, так и для мобильных устройств с выходом в Интернет).
5. www.edu.garant.ru - актуальный выпуск «ГАРАНТ-Студент» (скачать и установить на свой компьютер).
6. http://diss.rsl.ru - Электронная Библиотека Диссертаций Российской государственной библиотеки ЭБД РГБ. Включает полнотекстовые базы данных диссертаций.
7. http://www.cir.ru – Университетская информационная система России «УИС Россия».
8. www.public.ru – Интернет-библиотека СМИ Public.ru.
9. www.biblioclub.ru – электронная библиотека.
10. www.elibrary.ru – электронная библиотека.
11. www.Intuit.ru – электронный институт информационных технологий.
12. www.jetinfo.ru – информационный бюллетень компании "Инфосистемы Джет"
13. www.infotecs.ru/gts/ – Сервер Государственной технической комиссии при Президенте Российской Федерации.

7.2 Рекомендуемая литература

7.2.1 Основная литература

1. Башлы П. Н. , Баранова Е. К. , Бабаш А. В. Информационная безопасность: учебно-практическое пособие. М.: Евразийский открытый институт, 2011, 375 с. Режим доступа: http://biblioclub.ru/index.php?page=book&id=90539&sr=1. Дата обращения (02.02.16)
2. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации , М., Берлин: Директ-Медиа, 2015, 253 с., Режим доступа http://biblioclub.ru/index.php?page=book&id=276557&sr=1, Дата обращения (02.02.16)
3. Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс]/ Скрипник Д.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 424 с.— Режим доступа: http://www.iprbookshop.ru/16710. , Дата обращения (02.02.16)
4. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2014.— 702 с.— Режим доступа: http://www.iprbookshop.ru/29257 . Дата обращения (02.02.16)

7.2.2 Дополнительная литература

1. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
2. Глобальное исследование утечек информации (отчеты). http://www.infowatch.ru/analytics/reports/3866.
3. Конфиденциальное делопроизводство и защищенный электронный документооборот [Электронный ресурс]: учебник/ Н.Н. Куняев [и др.].—

Электрон. текстовые данные.— М.: Логос, 2013.— 452 с.— Режим доступа: http://www.iprbookshop.ru/9083. Дата обращения ((02.02.16))
4. Таненбаум Э. «Компьютерные сети», 5-е изд., 2012 г.
5. Уэррол Б. Операционные системы и компьютерные сети, 3-е изд., 2010 г.
6. Электронный ресурс «http://opennet.ru»
7. Информационная безопасность. Журнал, № 1, 2, 3, 4, М.: ГРОТЕК, 2014
8. Ярочкин,В. Информационная безопасность : Учебник / В.И. Ярочкин. - 3-е изд. - Москва : Академический проект: Трикста, 2008. - 544 с. (НТБ ГАГУ, 15 экз.) Точка доступа http://biblioclub.ru/index.php?page=book&id=211164&sr=1, Дата обращения (02.02.16)

8 Контроль знаний студентов

8.1 Формы текущего контроля

Текущий контроль осуществляется в ходе учебного процесса и консультирования студентов, по результатам выполнения самостоятельных работ. Основными формами текущего контроля знаний являются: обсуждение вынесенных в планах практических занятий вопросов, обсуждение докладов, защита отчетов по лабораторным работам.
Примерные баллы по различным видам работ, выставляемые преподавателем:

- Выполнение и Отчет по плановой лабораторной работе – 2-3 балла.
- Выступление на семинаре 1-2 балла.
- Участие в конференции с докладом 5-7 баллов.
- Разработка теста 2-5 баллов.
- Разработка реферата и теста - 10 баллов.
- ИРС: разработка и апробация лабораторной работы – 10 баллов.
- Разработка и публикация научно-исследовательской статьи – 10 баллов.

8.2 Вопросы к зачету

№	Перечень вопросов	Компетенции
		ОПК-4
1	Законодательно-правовой уровень защиты информации	+
2	Права собственника информации	+
3	Понятие государственной тайны	+
4	Основные положения закона РФ о защите информации	+
5	Защита информации на административном уровне	+
6	Разграничение доступа сотрудников при работе в информационной системе	+
7	Идентификация и аутентификация	+
8	Правила формирования паролей	+
9	Роль менеджера предприятия в организации защиты информации. Политика безопасности.	+
10	Программный уровень защиты информации.	+
11	Защита прикладного программного обеспечения	+
12	Защита операционной системы	+
13	Аппаратный уровень защиты информации	+
14	Физический уровень защиты информации	+
15	Защита информации в локальных сетях.	+
16	Защита информации в сети Интернет	+

17	Возможные способы защиты типового офиса: один сервер, несколько рабочих станций и выход в Интернет	+
18	Понятие вируса, его функциональные возможности	+
19	Классификация вирусов	+
20	Антивирусное программное обеспечение, его функции	+
21	Методика изучения ПО. Сравнительный анализ известных антивирусных программ	+
22	Сетевые антивирусные фильтры	+
23	Использование буферных компьютеров для фильтрации вирусов	+
24	Шифрование и кодирование как способ защиты информации	+
25	Понятие цифровой подписи, методы использования	+

9. Образовательные технологии

9.1 Использование информационных технологий

Программное обеспечение и Интернет-ресурсы

Персональный компьютер с ОС Windows, MS Office, MS SQL Server 2005, NOD32, программ-архиваторов WinRAR.

Составитель, к.ф.-м.н., ст. преподаватель Кайгородов Е.В.

И.о. зав кафедрой экономики предприятия
и прикладной информатики _____Е.А. Петрова, к.э.н., доцент