Министерство образования и науки Российской Федерации
Филиал Федерального государственного бюджетного образовательного учреждения высшего образования
«Кубанский государственный университет»
в г.Тихорецке

Кафедра социально-гуманитарных дисциплин

УТВЕРЖДАЮ
Проректор по работе с филиалами
ФГБОУ ВО «Кубанский государственный университет»
_____ А.А.Евдокимов
«__» 08 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.03.02 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки 38.03.02 Менеджмент
Направленность (профиль) Финансовый менеджмент
Программа подготовки: прикладная
Форма обучения: заочная
Квалификация (степень) выпускника: бакалавр
Год начала подготовки: 2016

Тихорецк
2017

Рабочая программа дисциплины составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 38.03.02 Менеджмент

Программу составили:
Доцент кафедры социально-гуманитарных дисциплин, канд. пед. наук
29 августа 2017 г. Е.А. Дегтярева

Ст.преподаватель кафедры социально-гуманитарных дисциплин, канд. пед. наук
29 августа 2017 г. Н.В. Чебышева

Рабочая программа дисциплины утверждена на заседании кафедры социально-гуманитарных дисциплин (разработчика)
Протокол № 1 29 августа 2017 г.
Заведующий кафедрой, канд. экон. наук, доц. Е.В. Мезенцева

Рабочая программа дисциплины обсуждена на заседании кафедры экономики и менеджмента (выпускающей)
Протокол № 1 29 августа 2017 г.
И.о. заведующего кафедрой, д-р экон. наук, доц. Е.В. Королюк

Утверждена на заседании учебно-методической комиссии филиала по УГН «Экономика и управление»
Протокол № 1 29 августа 2017 г.
Председатель УМК филиала по УГН «Экономика и управление», канд. экон. наук, доц. М.Г. Иманова

Рецензенты:
Э.П. Черняева, заведующий кафедрой математики и информатики филиала ФГБОУ ВО КубГУ в г. Армавире, канд. пед. наук

В.Е. Бельченко, заведующий кафедрой информатики и информационных технологий обучения ФГБОУ ВО «Армавирский государственный педагогический университет», канд. тех. наук, доц.

1. ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

1.1. Цель освоения дисциплины:

формирование знаний – основных составляющих информационной безопасности государства, общества и личности, а так же умений и навыков использования организационных, правовых, инженерно-технических и аппаратно-программных методов и средств при построении систем информационной безопасности в области выбранного профиля подготовки.

1.2. Задачи дисциплины:

– освоение основ теории информационной безопасности, знакомство с современными задачами, научной терминологией, моделями и концепциями защиты прав на информатизацию государства, общества и личности и построения систем информационной безопасности;

– изучение основных положений стратегии информационной войны; основных видов обеспечения систем информационной безопасности, методов оценки уровня защищенности компьютерных систем, методов и средств комплексной защиты объектов информатизации;

– применение организационных, правовых, инженерно-технических и аппаратно-программных методов и средств информационной безопасности в научно-исследовательских и практических разработках в области защиты объектов информатизации.

1.3. Место дисциплины (модуля) в структуре образовательной программы

Данная дисциплина относится к вариативной части Блока 1 «Дисциплины (модули)» учебного плана.

Курс «Информационная безопасность» находится в логической и содержательно-методической взаимосвязи с дисциплинами «Информационные технологии в менеджменте», «Информатика».

Предметом изучения курса «Информационная безопасность» являются принципы организации и обеспечения информационной безопасности в телекоммуникационных и компьютерных сетях и информационных системах.

1.4. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной дисциплины направлено на формирование у обучающихся общепрофессиональных и профессиональных компетенций: ОПК-7, ПК-11.

Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
		знать	**уметь**	**владеть**
ОПК-7	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	– основные подходы и естественнонаучные методы решения стандартных задач профессиональной деятельности с применением требований информационной безопасности для обработки и обобщения экономической информации	– решать стандартные задачи профессиональной деятельности с применением требований информационной безопасности для обработки и обобщения экономической информации	– навыками решения стандартных задач профессиональной деятельности с применением требований информационной безопасности для обработки и обобщения экономической информации
ПК-11	Владение навыками анализа информации о функционировании системы внутреннего документооборота	– понятие информации; – общую характеристику процессов сбора, передачи, обра-	– использовать информационные системы и средства вычислительной техники в решении	– приемами работы с современными программными средствами

Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
		знать	**уметь**	**владеть**
	организации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов	ботки и накопления информации	задач сбора, передачи, хранения и обработки экономической информации; – работать в качестве пользователя персонального компьютера; – создавать резервные копии и архивы данных и программ	

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 3 зач.ед. (108 часов), их распределение по видам работ представлено в таблице (для студентов ЗФО).

Вид учебной работы		Всего часов	Семестры (часы)			
			3	4		
Контактная работа (всего), в том числе:		**8,2**	**4**	**4,2**		
Аудиторные занятия (всего):		**8**	**4**	**4**		
Занятия лекционного типа		4	4	-		
Лабораторные занятия		-	-	-		
Занятия семинарского типа (семинары, практические занятия)		4	-	4		
Иная контактная работа (всего):		**0,2**	**-**	**0,2**		
Контроль самостоятельной работы (КСР)		-	-	-		
Промежуточная аттестация (ИКР)		0,2	-	0,2		
Самостоятельная работа (всего), в том числе:		**96**	**32**	**64**		
Курсовая работа		-	-	-		
Проработка учебного (теоретического) материала			20	40		
Выполнение индивидуальных заданий (выполнение контрольной работы, выполнение упражнений и задач)			12	10		
Подготовка к текущему контролю			-	14		
Контроль:		**3,8**	**-**	**3,8**		
Подготовка к зачету		3,8	-	3,8		
Общая трудоемкость	**час.**	**108**	**36**	**72**		
	в том числе контактная работа	**8,2**	**4**	**4,2**		
	зач. ед	**3**	**1**	**2**		

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы дисциплины, изучаемые в 3,4 семестре (заочная форма).

№	Наименование разделов	Количество часов

		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	Введение в дисциплину «Информационная безопасность»	24	2	2		20
2	Основы государственной политики РФ в области информационной безопасности	22		2		20
3	Информационная война	30				30
4	Основы обеспечения информационной безопасности корпоративных информационных систем	28	2			26
	Итого по дисциплине:		*4*	*4*		*96*

2.3. Содержание разделов дисциплины

В данном подразделе приводится описание содержания дисциплины, структурированное по разделам, с указанием по каждому разделу формы текущего контроля: В – вопросы для устного опроса; К – кейсы; Т – тесты; З – упражнения и задачи.

2.3.1 Занятия лекционного типа

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	Тема 1. Введение в дисциплину «Информационная безопасность»	Понятие национальной безопасности РФ. Виды безопасности. Информационная безопасность в системе национальной безопасности РФ. Роль информационной безопасности в обеспечении национальной безопасности государства.	В
2	Тема 4. Основы обеспечения информационной безопасности корпоративных информационных систем	Организационно-правовые основы информационной безопасности корпоративных информационных систем Организационно-технические основы информационной безопасности корпоративных информационных систем Аппаратно-программные средства обеспечения информационной безопасности корпоративных информационных систем. Основы комплексного обеспечения информационной безопасности корпоративных информационных систем. Антивирусные средства защиты информации в корпоративных информационных системах	В

2.3.2 Занятия семинарского типа

№	Наименование раздела	Тематика лабораторных занятий	Форма текущего контроля
1	Тема 1. Введение в дисциплину «Информационная безопасность»	1. Понятие национальной безопасности РФ. 2. Виды безопасности. 3. Информационная безопасность в системе национальной безопасности РФ. 4. Роль информационной безопасности в обеспечении национальной безопасности государства.	З, Т
2	Тема 2. Основы государственной политики РФ в области информационной безопасности	1. Национальные интересы РФ в информационной сфере и их обеспечение. 2. Виды угроз информационной безопасности РФ. 3. Источники угроз информационной безопасности. 4. Основные направления обеспечения информационной безопасности государства.	З, Т

2.3.3 Лабораторные занятия

Лабораторные занятия не предусмотрены.

2.3.4 Примерная тематика курсовых работ

Курсовые работы не предусмотрены.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	Проработка учебного (теоретического) материала	Самостоятельная работа студентов: методические рекомендации для бакалавров направления подготовки 38.03.02 Менеджмент, утвержденные кафедрой экономики и менеджмента (протокол №1 от 29.08.2017 г.)
2	Подготовка к текущему контролю	
3	Выполнение упражнений и задач	Письменные работы студентов: методические рекомендации для бакалавров направления подготовки 38.03.02 Менеджмент, утвержденные кафедрой экономики и менеджмента (протокол №1 от 29.08.2017 г.)

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом;

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме;

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме;

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе изучения дисциплины занятия лекционного типа и лабораторные занятия являются ведущими формами обучения в рамках лекционно-семинарской образовательной системы.

В учебном процессе используются следующие образовательные технологии:

– технология проблемного обучения: последовательное и целенаправленное выдвижение перед студентом познавательных задач, разрешая которые студенты активно усваивают знания;

– технология развивающего обучения: ориентация учебного процесса на потенциальные возможности человека и их реализацию;

– технология дифференцированного обучения: усвоение программного материала на различных планируемых уровнях, но не ниже обязательного;

– технология активного (контекстного) обучения: моделирование предметного и социального содержания будущей профессиональной деятельности;

Также при освоении дисциплины в учебном процессе используются активные и интерактивные (взаимодействующие) формы проведения занятий.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1 Фонд оценочных средств для проведения текущего контроля

Фонд оценочных средств по дисциплине оформлен как отдельное приложение к рабочей программе.

Примерные вопросы для устного опроса

Тема 1. Введение в дисциплину «Информационная безопасность»

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.
3. Какие существуют модели информационной безопасности?
4. Какие методы защиты информации выделяют?
5. Что такое правовые методы защиты информации?
6. Что такое организационные методы защиты информации?
7. Что такое технические методы защиты информации?
8. Что такое программно-аппаратные методы защиты информации?
9. Что такое криптографические методы защиты информации?
10. Что такое физические методы защиты информации?
11. Какие главные государственные органы в области обеспечения информационной безопасности?
12. Перечислите виды защищаемой информации.

Примерные упражнения и задачи

Тема 1. Введение в дисциплину «Информационная безопасность»

Задание 1. Пусть имеем множество из трёх пользователей {Администратор, Гость, Пользователь_1} и множество из четырёх объектов {Файл_1, Файл_2, CD-RW, Дисковод}. Множество возможных действий включает следующие: {Чтение, Запись, Передача прав другому пользователю}. Действие «Полные права» разрешает выполнение всех трёх действий, действие «Запрет» запрещает выполнение всех перечисленных действий. В данном случае, матрица доступа, описывающая дискреционную политику безопасности, может выглядеть следующим образом.

Таблица 1. Пример матрицы доступа

Объект / Субъект	Файл_1	Файл_2	CD-RW	Дисковод
1. Администратор	Полные права	Полные права	Полные права	Полные права
2. Гость	Запрет	Чтение	Чтение	Запрет
3. Пользователь_1	Чтение, передача прав	Чтение, запись	Полные права	Запрет

Например, Пользователь_1 имеет права на чтение и запись в Файл_2. Передавать же свои права другому пользователю он не может.

Пользователь, обладающий правами передачи своих прав доступа к объекту другому пользователю, может сделать это. При этом, пользователь, передающий права, может указать непосредственно, какие из своих прав он передает другому.

Например, если Пользователь_1 передает право доступа к Файлу_1 на чтение пользователю Гость, то у пользователя Гость появляется право чтения из Файла_1.

Задание 2. Пусть множество S возможных операций над объектами компьютерной системы задано следующим образом: S = {«Доступ на чтение», «Доступ на запись», «Передача прав»}.

1. Получить данные о количестве пользователей и объектов компьютерной системы из табл. 2, соответственно варианту.

2. Реализовать программный модуль, создающий матрицу доступа пользователей к объектам компьютерной системы. Реализация данного модуля подразумевает следующее:

2.1. Необходимо выбрать идентификаторы пользователей, которые будут использоваться при их входе в компьютерную систему (по одному идентификатору для каждого пользователя, количество пользователей указано для варианта). Например, множество из трёх идентификаторов пользователей {Ivan, Sergey, Boris}. Один из данных идентификаторов должен соответствовать администратору компьютерной системы (пользователю, обладающему полными правами доступа ко всем объектам).

2.2. Реализовать программное заполнение матрицы доступа, содержащей количество пользователей и объектов, соответственно Вашему варианту.

2.2.1. При заполнении матрицы доступа необходимо учитывать, что один из пользователей должен являться администратором системы (допустим, Ivan). Для него права доступа ко всем объектам должны быть выставлены как полные.

2.2.2. Права остальных пользователей для доступа к объектам компьютерной системы должны заполняться случайным образом с помощью датчика случайных чисел. При заполнении матрицы доступа необходимо учитывать, что пользователь может иметь несколько прав доступа к некоторому объекту компьютерной системы, иметь полные права, либо совсем не иметь прав.

2.2.3. Реализовать программный модуль, демонстрирующий работу в дискреционной модели политики безопасности.

3. Данный модуль должен выполнять следующие функции:

3.1. При запуске модуля должен запрашиваться идентификатор пользователя (проводится идентификация пользователя), при успешной идентификации пользователя должен осуществляться вход в систему, при неуспешной – выводиться соответствующее сообщение.

3.2. При входе в систему после успешной идентификации пользователя на экране должен распечатываться список всех объектов системы с указанием перечня всех доступных прав доступа идентифицированного пользователя к данным объектам. Вывод можно осуществить, например, следующим образом:

User: Boris
Идентификация прошла успешно, добро пожаловать в систему
Перечень Ваших прав:
Объект1: Чтение
Объект2: Запрет
Объект3: Чтение, Запись
Объект4: Полные права
Жду ваших указаний >

3.3. После вывода на экран перечня прав доступа пользователя к объектам компьютерной системы, необходимо организовать ожидание указаний пользователя на осуществление действий над объектами в компьютерной системе. После получения команды от пользователя, на экран необходимо вывести сообщение об успешности либо не успешности операции. При выполнении операции передачи прав (grant) должна модифицироваться матрица доступа. Программа должна поддерживать операцию выхода из системы (quit), после которой запрашивается идентификатор пользователя. Диалог можно организовать, например, так:

Жду ваших указаний > read
Над каким объектом производится операция? 1
Операция прошла успешно
Жду ваших указаний > write
Над каким объектом производится операция? 2
Отказ в выполнении операции. У Вас нет прав для ее осуществления
Жду ваших указаний > grant
Право на какой объект передается? 3
Отказ в выполнении операции. У Вас нет прав для ее осуществления
Жду ваших указаний > grant
Право на какой объект передается? 4
Какое право передается? read
Какому пользователю передается право? Ivan
Операция прошла успешно
Жду ваших указаний > quit
Работа пользователя Boris завершена. До свидания.
User:

4. Выполнить тестирование разработанной программы, продемонстрировав реализованную модель дискреционной политики безопасности.

Таблица 2. Варианты заданий

Вариант	Количество субъектов доступа (пользователей)	Количество объектов доступа
1	3	3
2	4	4
3	5	4
4	6	5
5	7	6
6	8	3
7	9	4
8	10	4
9	3	5
10	4	6

Примерные тесты

Тема 1. Введение в дисциплину «Информационная безопасность»

1. Что включает в себя концепция «Защищенные информационные системы»?

1) законодательные инициативы, научные, технические и технологические решения;
2) законодательные инициативы, фильтр пакетов данных;
3) технические и технологические решения, сканер для выявления уязвимости в узлах сети;
4) нет правильного ответа.

2. Какую общую цель включает в себя трёхуровневая модель проблемы защищённости ИС?

1) безопасность;
2) безотказность;
3) защищенные информационные системы;
4) деловое взаимодействие.

3. Наличие и полнота политики безопасности это…

1) активный компонент защиты, включающий в себя анализ возможных угроз и рисков, выбор мер противодействия и методологию их применения;
2) набор внешних корпоративных стандартов, правил и норм поведения, отвечающих законодательным актам страны и регламентирующих сбор, обработку и защиту информации;
3) мера доверия, которая может быть оказана архитектуре, инфраструктуре, программно-аппаратной реализации системы;
4) нет правильного ответа.

4. Политика безопасности это…

1) активный компонент защиты, включающий в себя анализ возможных угроз и рисков, выбор мер противодействия и методологию их применения;
2) набор внешних корпоративных стандартов, правил и норм поведения, отвечающих законодательным актам страны и регламентирующих сбор, обработку и защиту информации;
3) мера доверия, которая может быть оказана архитектуре, инфраструктуре, программно- аппаратной реализации системы;
4) нет правильного ответа.

5. Гарантированность безопасности это…

1) активный компонент защиты, включающий в себя анализ возможных угроз и рисков, выбор мер противодействия и методологию их применения;
2) набор внешних корпоративных стандартов, правил и норм поведения, отвечающих законодательным актам страны и регламентирующих сбор, обработку и защиту информации;
3) мера доверия, которая может быть оказана архитектуре, инфраструктуре, программно- аппаратной реализации системы;
4) нет правильного ответа.

6. Основное назначение надёжной вычислительной базы

1) выполнить функции монитора обращения и действия, т.е. контролировать допустимость выполнения пользователями определённых операций;
2) международные, отраслевые и внутренние стандарты;
3) методы взаимоотношения с внешней и внутренней средой;
4) нет правильного ответа.

7. Выберите правильные ответы. В трёхуровневую модель проблемы защищённости ИС, подтверждение включает:

1) внутренняя оценка;
2) аккредитация;
3) внешний аудит;
4) нет правильного ответа.

8. Гарантированность показывает

1) надёжность обеспечивается всей совокупностью защитных механизмов;
2) насколько конкретны механизмы, отвечающие за проведение в жизни безопасности;
3) функции монитора обращения и действия;
4) нет правильного ответа.

9. Надёжная система должная…

1) обеспечивать совокупность защитных механизмов;
2) выполнять функции монитора;
3) фиксировать все события, касающиеся безопасности;
4) нет правильного ответа.

10. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:

1) меры обеспечения целостности;
2) административные меры;
3) меры административного воздействия.

4.2 Фонд оценочных средств для проведения промежуточной аттестации

Вопросы для подготовки к зачету

1. Понятие национальной безопасности РФ.
2. Виды безопасности.
3. Информационная безопасность в системе национальной безопасности РФ.
4. Роль информационной безопасности в обеспечении национальной безопасности государства.
5. Информационная безопасность человека и общества и государства.
6. Уровни защиты информационных ресурсов. Признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности.
7. Компьютерные преступления. Основные технологии, использующиеся при совершении компьютерных преступлений.
8. Объекты защиты информации. Защита информации ограниченного доступа: государственная тайна, коммерческая тайна.
9. Основные каналы утечки информации. Защита от утечки информации под техническим каналам.
10. Национальные интересы РФ в информационной сфере и их обеспечение.
11. Виды угроз информационной безопасности РФ.
12. Источники угроз информационной безопасности.
13. Основные направления обеспечения информационной безопасности государства.
14. Политика безопасности. Основные типы политики безопасности.
15. Политика безопасности. Модели безопасности.
16. Стандарты информационной безопасности.
17. Правовое обеспечение защиты информации. Нормативные документы.
18. Методы и средства ведения информационной войны.
19. Информационная безопасность и информационное противоборство.
20. Информационное оружие, его классификация и возможности.
21. Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны.

22. Организационно-правовые основы информационной безопасности корпоративных информационных систем (ИБ КИС).
23. Организационно-технические основы ИБ КИС.
24. Аппаратно-программные средства обеспечения ИБ КИС.
25. Основы комплексного обеспечения ИБ КИС.
26. Методы и средства защиты информации.
27. Содержание способов и средств обеспечения безопасности информации.
28. Реализация методов и средств защиты информации.
29. Средства опознания и разграничения доступа к информации.
30. Криптография. Симметричные криптосистемы.
31. Криптография. Асимметричные криптосистемы.
32. Обзор и классификация методов шифрования информации.
33. Основные алгоритмы шифрования данных: ГОСТ.
34. Защита данных в вычислительных сетях. Межсетевые экраны. Сканеры.
35. Антивирусные средства.

Критерии оценивания ответа на зачете

Студенты обязаны сдать зачет в соответствии с расписанием и учебным планом. Зачет по дисциплине преследует цель оценить работу студента за курс, получение теоретических знаний, их прочность, развитие творческого мышления, приобретение навыков самостоятельной работы, умение применять полученные знания для решения практических задач.

Зачет - форма промежуточной аттестации, в результате которого обучающий получает оценку в двухбалльной шкале («зачтено», «не зачтено»).

Оценка «зачтено» ставится студенту, который прочно усвоил предусмотренный программный материал; правильно, аргументировано ответил на все вопросы, с приведением примеров; показал глубокие систематизированные знания, владеет приемами рассуждения и сопоставляет материал из разных источников: теорию связывает с практикой, другими темами данного курса, других изучаемых предметов; без ошибок выполнил практическое задание. Обязательным условием выставленной оценки является правильная речь в быстром или умеренном темпе. Дополнительным условием получения оценки «зачтено» могут стать хорошие успехи при выполнении самостоятельной и контрольной работы, систематическая активная работа на семинарских (практических) занятиях.

Оценка «не зачтено» ставится студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на зачете;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Основная литература:

1 Нестеров С.А. Информационная безопасность: учебник и практикум для академического бакалавриата / С.А. Нестеров. — М.: Издательство Юрайт, 2017. — 321 с. – Режим доступа: www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7

2 Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры / Т.А. Полякова, А.А. Стрельцов, С.Г. Чубукова, В.А. Ниесов; под ред. Т.А. Поляковой, А.А. Стрельцова. — М.: Издательство Юрайт, 2017. — 325 с. – Режим доступа: www.biblio-online.ru/book/D056DF3D-E22B-4A93-8B66-EBBAEF354847

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечной системе «Юрайт».

5.2 Дополнительная литература:

1 Бабенко Л.К. Криптографическая защита информации: симметричное шифрование: учебное пособие для вузов / Л.К. Бабенко, Е.А. Ищукова. — М.: Издательство Юрайт, 2017. — 220 с. – Режим доступа: www.biblio-online.ru/book/6946C235-8650-4A29-B75B-68E0EF829422

2 Васильева И.Н. Криптографические методы защиты информации: учебник и практикум для академического бакалавриата / И.Н. Васильева. — М.: Издательство Юрайт, 2017. — 349 с. – Режим доступа: www.biblio-online.ru/book/59BABD78-5536-4ED4-BB9D-55E2F19F80B2

3 Внуков А.А. Защита информации: учебное пособие для бакалавриата и магистратуры / А.А. Внуков. — 2-е изд., испр. и доп. — М.: Издательство Юрайт, 2017. — 261 с. – Режим доступа: www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1

4 Запечников С.В. Криптографические методы защиты информации: учебник для академического бакалавриата / С.В. Запечников, О.В. Казарин, А.А. Тарасов. — М.: Издательство Юрайт, 2017. — 309 с. – Режим доступа: www.biblio-online.ru/book/B27D8A2B-F86C-4F18-9F21-3E0695C0A4C0

5 Информационные технологии в менеджменте (управлении): учебник и практикум для академического бакалавриата / Ю.Д. Романова [и др.]; под общ. ред. Ю.Д. Романовой. – М.: Издательство Юрайт, 2017. – 478 с. – Режим доступа: www.biblio-online.ru/book/F293BFB1-C447-4AD2-B8A3-56F85FE5C980

6 Информационные технологии в менеджменте: учебник и практикум для академического бакалавриата / Е.В. Майорова [и др.]; под ред. Е. В. Черток. – М.: Издательство Юрайт, 2017. – 368 с. – Режим доступа: www.biblio-online.ru/book/478DE08C-289F-48A2-8FF9-2AC28C1A0AFC

7 Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О.В. Казарин, А.С. Забабурин. — М.: Издательство Юрайт, 2017. — 312 с. – Режим доступа : www.biblio-online.ru/book/E458AFCD-826E-4A1F-9BAB-68BB83EA616F

8 Лось А.Б. Криптографические методы защиты информации: учебник для академического бакалавриата / А.Б. Лось, А.Ю. Нестеренко, М.И. Рожков. — 2-е изд., испр. — М.: Издательство Юрайт, 2017. — 473 с. – Режим доступа: www.biblio-online.ru/book/27397D56-C8A1-4970-9F39-28E7FA40632A

9 Поляков В. П. Информатика для экономистов. Практикум: учебное пособие для академического бакалавриата / В.П. Поляков, В.П. Косарев; под ред. В.П. Полякова, В.П. Косарев. – 2-е изд., перераб. и доп. – М.: Издательство Юрайт, 2017. – 271 с. – Режим доступа: www.biblio-online.ru/book/FB1F6466-040B-498F-B168-AB6B73CEBCDF

10 Поляков В.П. Информатика для экономистов: учебник для академического бакалавриата / В.П. Поляков, В.П. Косарев; отв. ред. В.П. Поляков. – М.: Издательство Юрайт, 2017. – 524 с. – Режим доступа: www.biblio-online.ru/book/8F1A6C34-4C52-44E7-B8C7-16BC40452D20

11 Фомичёв В.М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты: учебник для академического бакалавриата / В.М. Фомичёв, Д.А. Мельников; под ред. В.М. Фомичёва. — М.: Издательство Юрайт, 2017. — 209 с. – Режим доступа: www.biblio-online.ru/book/C0328DC2-2A46-4945-994F-04F661095B83

12 Фомичёв В.М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты: учебник для академического бакалавриата / В.М. Фомичёв, Д.А. Мельников; под

ред. В.М. Фомичёва. — М.: Издательство Юрайт, 2017. — 245 с. – Режим доступа: www.biblio-online.ru/book/AF99BBDE-AF3A-43A9-A90F-B99806553C25

13 Царев, Р.Ю. Программные и аппаратные средства информатики: учебник / Р.Ю. Царев, А.В. Прокопенко, А.Н. Князьков; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск: Сибирский федеральный университет, 2015. - 160 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=435670

14 Щеглов А.Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А.Ю. Щеглов, К.А. Щеглов. — М.: Издательство Юрайт, 2017. — 309 с. – Режим доступа: www.biblio-online.ru/book/9CD7BE3A-F9DC-4F6D-8EC6-6A90CB9A4E0E

5.3 Периодические издания:

Прикладная информатика
Программирование
Хакер
Высшее образование сегодня
Вопросы экономики

6. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде организации и к профессиональным базам данных, электронным образовательным ресурсам, Интернет-сайтам специализированных ведомств.

Наименование сайта	Адрес сайта
Электронная библиотека диссертаций РГБ	http://diss.rsl.ru/
Электронная библиотека grebennikon.ru	www.grebennikon.ru
Базы данных компании «Ист Вью Информейшн Сервисиз,Инк»	http://dlib.eastview.com
УИС «Россия»	http://uisrussia.msu.ru
«Лекториум» (Минобрнауки России, Департамент стратразвития)	http://www.lektorium.tv/
Национальная электронная библиотека	http://нэб.рф/
Электронный архив документов КубГУ	http://docspace.kubsu.ru
Федеральная служба государственной статистики	http://www.gks.ru
Территориальный орган Федеральной службы государственной статистики по Краснодарскому краю	http://www.krsdstat.ru
Министерство образования и науки Российской Федерации	http://минобрнауки.рф
Федеральная служба по надзору в сфере образования и науки	http://obrnadzor.gov.ru/
Федеральная служба по интеллектуальной собственности	http://rupto.ru
Федеральная служба государственной статистики	http://gks.ru/
Официальный интернет-портал правовой информации	http://pravo.gov.ru
Конституция Российской Федерации	http://constitution.ru/

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

При изучении дисциплины используются следующие формы работы.

1. Лекции, на которых рассматриваются основные теоретические вопросы данной дисциплины. Лекции проводятся в следующих формах: лекция.

2. Практические занятия, на которых разбираются проблемные ситуации, решаются задачи, заслушиваются доклады, проводятся научные дискуссии, опрос по теоретическим вопросам изучаемых тем и тестирование. При подготовке к практическому занятию следует:

– использовать рекомендованные преподавателями учебники и учебные пособия - для закрепления теоретического материала;

– подготовить доклады и сообщения, разобрать проблемные ситуации;

– разобрать совместно с другими студентами и обсудить вопросы по теме практического занятия и т.д.

3. Самостоятельная работа, которая является одним из главных методов изучения дисциплины.

Цель самостоятельной работы – расширение кругозора и углубление знаний в области теории и практики вопросов изучаемой дисциплины.

Контроль за выполнением самостоятельной работы проводится при изучении каждой темы дисциплины на практических занятиях. Это текущий опрос, тестовые задания.

Самостоятельная работа студента в процессе освоения дисциплины включает в себя:

– изучение основной и дополнительной литературы по курсу;

– работу с электронными библиотечными системами;

– изучение материалов периодической печати, Интернет - ресурсов;

– индивидуальные и групповые консультации;

– подготовку к зачету.

4. Зачет по дисциплине. Зачет сдается в устной форме. Представляет собой структурированное задание по всем разделам дисциплины. Для подготовки к зачету следует воспользоваться рекомендованным преподавателем учебниками, методическими указаниями к практическим занятиям и самостоятельной контролируемой работе студента по дисциплине, глоссарием, своими конспектами лекций и практических занятий, выполненными самостоятельными работами.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

8. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

8.1 Перечень информационных технологий

1. Проверка домашних заданий и индивидуальное консультирование посредством электронной почты.

2. Использование электронных презентаций при проведении лекционных занятий.

3. Консультирование студентов и контроль выполнения лабораторных работ посредством электронной почты.

8.2 Перечень необходимого программного обеспечения

При изучении дисциплины может быть использовано следующее программное обеспечение:

– комплекс взаимосвязанных программ, предназначенных для управления ресурсами ПК и организации взаимодействия с пользователем (операционная система Windows XP PRO);

– пакет приложений для выполнения основных задач компьютерной обработки различных типов документов (Microsoft Office 2010) в состав которого входят:

MS Word – текстовый процессор – для создания и редактирования текстовых документов;

MS Excel – табличный процессор – для обработки табличный данных и выполнения сложных вычислений;

MS Access – система управления базами данных – для организации работы с большими объемами данных;

MS Power Point – система подготовки электронных презентаций – для подготовки и проведения презентаций;

MS Outlook – менеджер персональной информации – для обеспечения унифицированного доступа к корпоративной информации;

MS FrontPage – система редактирования Web-узлов – для создания и обновления Web-узлов;

MS Publisher – настольная издательская система – для создания профессионально оформленных публикаций:

– программа для комплексной защиты ПК, объединяющая в себе антивирус, антишпион и функцию удаленного администратора (Kaspersky endpoint Security 10);

– пакет программ для создания и просмотра электронных публикаций в формате PDF (Adobe Reader);

– прикладное программное обеспечение для просмотра веб-страниц, содержания веб-документов, компьютерных файлов и их каталогов, управления веб-приложениями, а также для решения других задач (Google Chrome);

– программы, предназначенные для архивации, упаковки файлов путем сжатия хранимой в них информации (7zip).

8.3 Перечень информационных справочных систем

Обучающимся обеспечен доступ к современным профессиональным базам данных, справочным и поисковым системам.

1. Справочно-правовая система «Консультант Плюс» (http://www.consultant.ru).
2. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)/

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1	Занятия лекционного типа	Учебная аудитория оснащенная оборудованием (мультимедийный проектор, экран, персональный компьютер, выход в Интернет, учебная мебель, доска учебная, учебно-наглядные пособия, обеспечивающие тематические иллюстрации)
2	Занятия семинарского типа	
3	Групповые и индивидуальные консультации	
4	Текущий контроль и промежуточная аттестация	
5	Самостоятельная работа	Кабинет оснащен компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета