МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Майкопский государственный технологический университет»

Факультет информационных систем в экономике и юриспруденции

Кафедра Информационной безопасности и прикладной информатики

УТВЕРЖДАЮ
Проректор по учебной работе
_____Л. И. Задорожная
«25»____10_____ 2017 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине Б1.Б.17 Основы информационной безопасности

по специальности 10.05.04 Информационно-аналитические системы безопасности

специализация №2 Информационная безопасность финансовых и экономических структур

Квалификация (степень) выпускника Специалист

Уровень подготовки Специалитет

Форма обучения Очная

Год начала подготовки 2018

Майкоп

Рабочая программа составлена на основе ФГОС ВО и учебного плана МГТУ по направлению (специальности) 10.05.04 Информационно-аналитические системы безопасности

Составитель рабочей программы:

Старший преподаватель _____ Брикова И.В.
(должность, ученое звание, степень) (подпись) (Ф.И.О.)

Рабочая программа утверждена на заседании кафедры

Информационной безопасности и прикладной информатики
(наименование кафедры)

Заведующий кафедрой
«25»____10_____ 2017 г.. _____ Чефранов С.Г.
(подпись) (Ф.И.О.)

Одобрено учебно-методической комиссией факультета
(где осуществляется обучение) «25»____10_____ 2017 г.

Председатель
учебно-методического
совета направления
(где осуществляется обучение) _____ Чефранов С.Г.
(подпись) (Ф.И.О.)

Декан факультета
(где осуществляется обучение)
«25»____10_____ 2017 г. _____ Доргушаова А.К..
(подпись) (Ф.И.О.)

СОГЛАСОВАНО:
Начальник УМУ
«25»____10_____ 2017 г. _____ Чудесова Н.Н.
(подпись) (Ф.И.О.)

Зав. выпускающей кафедрой
по направлению _____ Чефранов С.Г.
(подпись) (Ф.И.О.)

1. Цели и задачи освоения дисциплины

Цель изучения дисциплины «Основы информационной безопасности» - заложить терминологический фундамент, научить проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, приобрести навыки анализа угроз информационной безопасности, рассмотреть основные общеметодологические принципы теории информационной безопасности; изучение методов и средств обеспечения информационной безопасности, методов нарушения конфиденциальности, целостности и доступности информации. Для реализации поставленной цели необходимо решить следующие **задачи:**

- ознакомление обучающихся с терминологией информационной безопасности;
- развитие мышления обучающихся;
- изучение методов и средств обеспечения информационной безопасности;
- обучение определению причин, видов, источников и каналов утечки, искажения информации.

2. Место дисциплины в структуре ОП специалитета

Дисциплина «Основы информационной безопасности» входит в перечень курсов базовой части ОП специальности «Информационно-аналитические системы безопасности».

Изучение дисциплины базируется на знаниях, полученных обучающимися при изучении дисциплины «Введение в специальность», а также на знаниях научных основ и закономерностей развития общества.

Кроме того, она имеет логические и содержательно-методические связи с дисциплинами по выбору базовой и вариативной частей ОП «Безопасность электронного документооборота», «Безопасность информационно-аналитических систем», «Организационное и правовое обеспечение информационной безопасности», Защита и обработка конфиденциальных документов», «Авторское право», «Защита интеллектуальной собственности и патентоведение».

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

В результате изучения учебной дисциплины у обучающегося формируются компетенции:

- способность проводить обоснование и выбор оптимального решения задач в сфере профессиональной деятельности (ПК-5);
- способность выявлять угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-9);
- способность выявлять условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа, составляющих государственную, банковскую, коммерческую тайну, персональные данные (ПК-18).

В результате освоения дисциплины обучающийся должен:

Знать: состав задач обеспечения информационной безопасности, принципы разработки алгоритмов для оптимального решения типовых задач обеспечения информационной безопасности; теоретические основы исследования информационных процессов предприятий, организаций, их классификацию; угрозы безопасности информации, модели нарушителя информационных систем, возможности проникновения нарушителя в информационную систему; понятия сведений ограниченного доступа; понятия государственной, коммерческой, банковской и других тайн, персональных данных; виды правонарушений в отношении сведений ограниченного доступа.

Уметь: выделять типовые задачи обеспечения информационной безопасности, составлять алгоритмы их решения; определять виды и формы информации, подверженной угрозам, классифицировать и систематизировать информационные массивы предприятий и организаций по совокупности признаков, определять возможные методы и пути реализации угроз; исследовать эффективность создаваемых информационных систем, в том числе средств обеспечения их информационной безопасности; проводить мониторинг и выявлять условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа, составляющих государственную, банковскую, коммерческую тайну, персональные данные.

Владеть: навыками реализации алгоритмов оптимального решения типовых задач обеспечения информационной безопасности; разработки моделей информационных процессов предприятий и организаций, оценки уязвимости информации различных видов и форм, выбора технологий, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых информационных систем; обоснования и принятия решений, связанных с реализацией правовых норм, в пределах должностных обязанностей.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет **2 зачетные единицы (72 часа).**

4.1. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов/з.е.	Семестры			
		3			
Аудиторные занятия (всего)	**51/1,42**	**51/1,42**			
В том числе:					
Лекции (Л)	34/0,95	34/0,95			
Практические занятия (ПЗ)	17/0,47	17/0,47			
Семинары (С)					
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа обучающихся (СРС) (всего)	**21/0,58**	**21/0,58**			
В том числе:					
Курсовой проект (работа)					
Расчетно-графические работы					
Реферат	15/0,42	15/0,42			
Другие виды СРС (если предусматриваются, приводится перечень видов СРС) 1. Составление плана-конспекта первоисточников и другой учебной литературы. 2. Составление плана-конспекта. 3. Проведение мониторинга, подбор и анализ статистических данных. 4. Выполнение расчетных заданий. 5. Подготовка к контрольным работам, КСЗ	6/0,16	6/0,16			
Форма промежуточной аттестации: Зачет	+ +	+ +			
Общая трудоемкость	**72/2**	**72/2**			

5. Структура и содержание дисциплины

5.1. Структура дисциплины

№ п/п	Раздел дисциплины	Виды учебной работы, включая самостоятельную и трудоемкость (в часах)			
		Л	**С/ПЗ**	**ЛР**	**СРС**
1.	Введение. Основные понятия, общеметодологические принципы информационной безопасности.	2			
2.	Информация - наиболее ценный ресурс современного общества. Проблемы информационной войны.	4			5
3.	Организационно-правовое обеспечение информационной безопасности.	4	2		
4.	Информационные системы. Общие положения. Информация как продукт. Информационные услуги.	4	2		6
5.	Угрозы информации	4	2		5
6.	Методы и модели оценки уязвимости информации	2	2		
7.	Методы определения требований к защите информации	4	2		
8.	Анализ существующих методик определения требований к защите информации	4	2		
9.	Функции и задачи защиты информации. Стратегии защиты информации.	2	2		
10.	Способы и средства защиты информации	2	2		5
11.	Архитектура систем защиты информации (СЗИ)	2	1		
12.	Промежуточная аттестация зачет				
	Итого:	**34**	**17**	**-**	**21**
	из них часов в интерактивной форме	**10**	**8**		

5.2. Содержание разделов дисциплины «Основы информационной безопасности», образовательные технологии
Лекционный курс

№ п/п	Наименование темы дисциплины	Трудоемкость (часы / зач. ед.)	Содержание	Формируемые компетенции	Результаты освоения (знать, уметь, владеть)	Образовательные технологии
Тема 1.	Введение. Основные понятия, общеметодологические принципы информационной безопасности	2/0,06	Цели, задачи, предмет, содержание и задачи курса. Место курса среди других дисциплин. Структура курса. Понятие информационной безопасности. Основные определения и термины.	ПК-5	**Знать:** состав задач обеспечения информационной безопасности, принципы разработки алгоритмов для оптимального решения типовых задач обеспечения информационной безопасности. **Уметь:** выделять типовые задачи обеспечения информационной безопасности, составлять алгоритмы их решения. **Владеть:** навыками реализации алгоритмов оптимального решения типовых задач обеспечения информационной безопасности.	Лекция-беседа
Тема 2.	Информация - наиболее ценный ресурс современного общества. Проблемы информационной войны.	4/0,1	Понятие «информационный ресурс». Классы информационных ресурсов. Документы. Информация и ее виды. Информационная война и ее виды. Информационное оружие и его классификация.	ПК-5	**Знать:** состав задач обеспечения информационной безопасности, принципы разработки алгоритмов для оптимального решения типовых задач обеспечения информационной безопасности. **Уметь:** выделять типовые задачи обеспечения информационной безопасности, составлять алгоритмы их решения. **Владеть:** навыками реализации алгоритмов оптимального решения типовых задач обес-	Лекция-беседа

					печения информационной безопасности.	
Тема 3.	Организационно-правовое обеспечение информационной безопасности	4/0,17	Правовое регулирование информационных потоков в различных видах деятельности. Международные и отечественные правовые и нормативные акты обеспечения ИБ процессов переработки информации. Организационное регулирование защиты процессов переработки информации. Информация как объект юридической защиты. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Основные принципы засекречивания информации. Государственная система правового обеспечения защиты информации в Российской Федерации. Ответственность за нарушения законодательства в информационной сфере.	ПК-5 ПК-18	**Знать:** состав задач обеспечения информационной безопасности, принципы разработки алгоритмов для оптимального решения типовых задач обеспечения информационной безопасности; понятия сведений ограниченного доступа; понятия государственной, коммерческой, банковской и других тайн, персональных данных; виды правонарушений в отношении сведений ограниченного доступа. **Уметь:** выделять типовые задачи обеспечения информационной безопасности, составлять алгоритмы их решения; проводить мониторинг и выявлять условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа, составляющих государственную, банковскую, коммерческую тайну, персональные данные. **Владеть:** навыками реализации алгоритмов оптимального решения типовых задач обеспечения информационной безопасности; обоснования и принятия решений, связанных с реализацией правовых норм,	Лекция-беседа

					в пределах должностных обязанностей.	
Тема 4.	Информационные системы. Общие положения. Информация как продукт.	4/0,1	Основные положения теории информационной безопасности информационных систем. Концепция информационной безопасности. Источники конфиденциальной информации в информационных системах. Что приводит к неправомерному овладению конфиденциальной информацией в информационных системах. Виды технических средств информационных систем.	ПК-9	**Знать:** теоретические основы исследования информационных процессов предприятий, организаций, их классификацию; угрозы безопасности информации, модели нарушителя информационных систем, возможности проникновения нарушителя в информационную систему. **Уметь:** определять виды и формы информации, подверженной угрозам, классифицировать и систематизировать информационные массивы предприятий и организаций по совокупности признаков, определять возможные методы и пути реализации угроз; исследовать эффективность создаваемых информационных систем, в том числе средств обеспечения их информационной безопасности. **Владеть:** навыками разработки моделей информационных процессов предприятий и организаций, оценки уязвимости информации различных видов и форм, выбора технологий, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасно-	Лекция-визуализация

					сти создаваемых информационных систем.	
Тема 5.	Угрозы информации	4/0,1	Понятие угрозы. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации. Виды угроз информационным системам. Виды потерь. Убытки, связанные с информационным обменом. Международные стандарты информационного обмена. Виды противников или «нарушителей». Модель нарушителя информационных систем.	ПК-9	**Знать:** теоретические основы исследования информационных процессов предприятий, организаций, их классификацию; угрозы безопасности информации, модели нарушителя информационных систем, возможности проникновения нарушителя в информационную систему. **Уметь:** определять виды и формы информации, подверженной угрозам, классифицировать и систематизировать информационные массивы предприятий и организаций по совокупности признаков, определять возможные методы и пути реализации угроз; исследовать эффективность создаваемых информационных систем, в том числе средств обеспечения их информационной безопасности. **Владеть:** навыками разработки моделей информационных процессов предприятий и организаций, оценки уязвимости информации различных видов и форм, выбора технологий, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасно-	Лекция-визуализация

					сти создаваемых информационных систем.	
Тема 6	Методы и модели оценки уязвимости информации	2/0,06	Классификация нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности. Эмпирический подход к оценке уязвимости информации. Система с полным перекрытием. Модели безопасности и их применение.	ПК-9	**Знать:** теоретические основы исследования информационных процессов предприятий, организаций, их классификацию; угрозы безопасности информации, модели нарушителя информационных систем, возможности проникновения нарушителя в информационную систему. **Уметь:** определять виды и формы информации, подверженной угрозам, классифицировать и систематизировать информационные массивы предприятий и организаций по совокупности признаков, определять возможные методы и пути реализации угроз; исследовать эффективность создаваемых информационных систем, в том числе средств обеспечения их информационной безопасности. **Владеть:** навыками разработки моделей информационных процессов предприятий и организаций, оценки уязвимости информации различных видов и форм, выбора технологий, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасно-	Лекция-беседа

					сти создаваемых информационных систем.	
Тема 7	Методы определения требований к защите информации	4/0,1	Требования, обусловленные спецификой автоматизированной обработки информации. Требования, связанные с размещением защищаемой информации. Требования, определяемые структурой автоматизированной системы обработки данных. Требования, обусловленные видом защищаемой информации. Требования, обусловленные технологическими схемами автоматизированной обработки информации. Требования, обусловленные способом взаимодействия пользователя с комплексом средств автоматизации. Требования, обусловленные режимом функционирования комплексов средств автоматизации. Требования, обусловленные этапом жизненного цикла автоматизированной системы обработки данных.	ПК-5	**Знать:** состав задач обеспечения информационной безопасности, принципы разработки алгоритмов для оптимального решения типовых задач обеспечения информационной безопасности. **Уметь:** выделять типовые задачи обеспечения информационной безопасности, составлять алгоритмы их решения. **Владеть:** навыками реализации алгоритмов оптимального решения типовых задач обеспечения информационной безопасности.	Лекция-беседа
Тема 8	Анализ существующих методик определения требований к защите информации	4/0,1	Требования к безопасности информационных систем в США. Требования к безопасности информационных систем в России. Классы защищенности СВТ от НСД. Оценка состояния безопасности ИС Франции. Факторы, влияющие на требуемый уровень защиты информации. Критерии оценки безопасности информационных технологий.	ПК-9	**Знать:** теоретические основы исследования информационных процессов предприятий, организаций, их классификацию; угрозы безопасности информации, модели нарушителя информационных систем, возможности проникновения нарушителя в информационную систему. **Уметь:** определять виды и	Лекция-визуализация

					формы информации, подверженной угрозам, классифицировать и систематизировать информационные массивы предприятий и организаций по совокупности признаков, определять возможные методы и пути реализации угроз; исследовать эффективность создаваемых информационных систем, в том числе средств обеспечения их информационной безопасности. **Владеть:** навыками разработки моделей информационных процессов предприятий и организаций, оценки уязвимости информации различных видов и форм, выбора технологий, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых информационных систем.	
Тема 9	Функции и задачи защиты информации. Стратегии защиты информации.	2/0,06	Защита. Общие положения. Методы формирования функций защиты. Классы задач защиты информации. Функции защиты. Состояния и функции системы защиты информации. Понятие «стратегия». Проблемы, затрудняющие решение задач обеспечения информационной безопасности. Основные стратегии защиты информации.	ПК-5 ПК-9	**Знать:** состав задач обеспечения информационной безопасности, принципы разработки алгоритмов для оптимального решения типовых задач обеспечения информационной безопасности; теоретические основы исследования информационных процессов предприятий, организаций, их классификацию; угро-	Лекция-беседа

					зы безопасности информации, модели нарушителя информационных систем, возможности проникновения нарушителя в информационную систему. **Уметь:** выделять типовые задачи обеспечения информационной безопасности, составлять алгоритмы их решения; определять виды и формы информации, подверженной угрозам, классифицировать и систематизировать информационные массивы предприятий и организаций по совокупности признаков, определять возможные методы и пути реализации угроз; исследовать эффективность создаваемых информационных систем, в том числе средств обеспечения их информационной безопасности. **Владеть:** навыками реализации алгоритмов оптимального решения типовых задач обеспечения информационной безопасности; разработки моделей информационных процессов предприятий и организаций, оценки уязвимости информации различных видов и форм, выбора технологий, инструментальных средств, средств вычислительной техники и средств обеспечения	

					информационной безопасности создаваемых информационных систем.	
Тема 10	Способы и средства защиты информации	2/0,06	Использование защищенных компьютерных систем. Содержание способов и средств обеспечения безопасности: препятствие, управление, маскировка, регламентация, принуждение, побуждение, нападение. Методы и средства защиты информации. Формальные и неформальные средства защиты.	ПК-9	**Знать:** теоретические основы исследования информационных процессов предприятий, организаций, их классификацию; угрозы безопасности информации, модели нарушителя информационных систем, возможности проникновения нарушителя в информационную систему. **Уметь:** определять виды и формы информации, подверженной угрозам, классифицировать и систематизировать информационные массивы предприятий и организаций по совокупности признаков, определять возможные методы и пути реализации угроз; исследовать эффективность создаваемых информационных систем, в том числе средств обеспечения их информационной безопасности. **Владеть:** навыками разработки моделей информационных процессов предприятий и организаций, оценки уязвимости информации различных видов и форм, выбора технологий, инструментальных средств, средств вычислительной техники и средств обеспечения	Лекция-беседа

					информационной безопасности создаваемых информационных систем.	
Тема 11	Архитектура систем защиты информации (СЗИ)	2/0,06	Требования к архитектуре СЗИ. Построение СРВ. Ядро системы защиты информации. Ресурсы системы защиты информации. Организационное построение.	ПК-5 ПК-9	**Знать:** состав задач обеспечения информационной безопасности, принципы разработки алгоритмов для оптимального решения типовых задач обеспечения информационной безопасности; теоретические основы исследования информационных процессов предприятий, организаций, их классификацию; угрозы безопасности информации, модели нарушителя информационных систем, возможности проникновения нарушителя в информационную систему. **Уметь:** выделять типовые задачи обеспечения информационной безопасности, составлять алгоритмы их решения; определять виды и формы информации, подверженной угрозам, классифицировать и систематизировать информационные массивы предприятий и организаций по совокупности признаков, определять возможные методы и пути реализации угроз; исследовать эффективность создаваемых информационных систем, в том числе средств обеспечения их информационной безопасности.	Лекция-беседа

					Владеть: навыками реализации алгоритмов оптимального решения типовых задач обеспечения информационной безопасности; разработки моделей информационных процессов предприятий и организаций, оценки уязвимости информации различных видов и форм, выбора технологий, инструментальных средств, средств вычислительной техники и средств обеспечения информационной безопасности создаваемых информационных систем.	
	Итого	**34/0,94**				

5.3. Практические и семинарские занятия, их наименование, содержание и объем в часах

№ п/п	№ раздела дисциплины	Наименование практических и семинарских занятий	Объем в часах / трудоемкость в з.е.
1.	Организационно-правовое обеспечение информационной безопасности.	Классификация информационных ресурсов. Категории объектов и защита информационной собственности. Организационное регулирование защиты процессов переработки информации. Информация как объект юридической защиты. Основные принципы засекречивания информации. Государственная система правового обеспечения защиты информации в Российской Федерации.	2/0,06
2.	Информационные системы. Общие положения. Информация как продукт.	Основные положения теории информационной безопасности информационных систем. Концепция информационной безопасности. Источники конфиденциальной информации в информационных системах. Что приводит к неправомерному овладению конфиденциальной информацией в информационных системах. Виды технических средств информационных систем. Информационные службы и информационные услуги. Виды возможных нарушений информационной системы. Основные технологии построения защищенных информационных систем.	2/0,06
3.	Угрозы информации	Понятие угрозы. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации. Виды угроз информационным системам. Виды потерь. Убытки, связанные с информационным обменом. Международные стандарты информационного обмена. Виды противников или «нарушителей». Модель нарушителя информационных систем. Информационные инфекции.	2/0,06
4.	Методы и модели оценки уязвимости информации	Классификация нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. Анализ способов нарушений информационной безопасности. Эмпирический подход к оценке уязвимости информации. Система с полным перекрытием. Модели безопасности и их применение.	2/0,06
5.	Методы определения требований к защите информации	Требования, обусловленные спецификой автоматизированной обработки информации. Требования, связанные с размещением защищаемой информации. Требования, определяемые структурой автоматизированной системы обработки данных. Требования, обу-	2/0,06

		словленные видом защищаемой информации. Требования, обусловленные технологическими схемами автоматизированной обработки информации. Требования, обусловленные способом взаимодействия пользователя с комплексом средств автоматизации. Требования, обусловленные режимом функционирования комплексов средств автоматизации. Требования, обусловленные этапом жизненного цикла автоматизированной системы обработки данных.	
6.	Анализ существующих методик определения требований к защите информации	Требования к безопасности информационных систем в США. Требования к безопасности информационных систем в России. Классы защищенности СВТ от НСД. Оценка состояния безопасности ИС Франции. Факторы, влияющие на требуемый уровень защиты информации. Критерии оценки безопасности информационных технологий.	2/0,06
7.	Функции и задачи защиты информации. Стратегии защиты информации.	Защита. Общие положения. Методы формирования функций защиты. Классы задач защиты информации. Функции защиты. Состояния и функции системы защиты информации. Понятие «стратегия». Проблемы, затрудняющие решение задач обеспечения информационной безопасности. Основные стратегии защиты информации.	2/0,06
8.	Способы и средства защиты информации	Использование защищенных компьютерных систем. Содержание способов и средств обеспечения безопасности: препятствие, управление, маскировка, регламентация, принуждение, побуждение, нападение. Методы и средства защиты информации. Формальные и неформальные средства защиты. Методы криптографии. Информационная безопасность в условиях функционирования в России глобальных сетей.	2/0,06
9.	Архитектура систем защиты информации (СЗИ)	Требования к архитектуре СЗИ. Построение СРВ. Ядро системы защиты информации. Ресурсы системы защиты информации. Организационное построение.	1/0,03
10.	Промежуточная аттестация		
	Итого:		**17/0,47**
	из них часов в интерактивной форме		**8/0,22**

5.4 Лабораторные занятия, их наименование и объем в часах

№ п/п	№ раздела дисциплины	Наименование лабораторных работ	Объем в часах / трудоемкость в з.е.

5.5. Примерная тематика курсовых проектов (работ)
Не предусмотрены.

5.6. Самостоятельная работа обучающихся

Содержание и объем самостоятельной работы обучающихся

№ п/п	Разделы и темы рабочей программы самостоятельного изучения	Перечень домашних заданий и других вопросов для самостоятельного изучения	Сроки выполнения	Объем в часах / трудоемкость в з.е.
1.	Информация - наиболее ценный ресурс современного общества. Проблемы информационной войны.	Написание реферата	2-3 неделя	5/0,14
2.	Информационные системы. Общие положения. Информация как продукт.	Подбор, обобщение и анализ информации из литературных источников и других информационных ресурсов по профилю подготовки Написание реферата	6-7 неделя	6/0,16
3.	Угрозы информации	Написание реферата	8-9 неделя	5/0,14
4.	Способы и средства защиты информации	Написание реферата	16 неделя	5/0,14
5.	зачет	Подготовка к зачету		
	Итого			**21/0,58**

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

6.1. Методические указания (собственные разработки)

6.2 Литература для самостоятельной работы

1. Защита информации [Электронный ресурс]: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - Москва: РИОР: ИНФРА-М, 2015. - 392 с. - ЭБС «Znanium. com» - Режим доступа: http://znanium.com/catalog.php?bookinfo=474838

2. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Нестеров С.А. - СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014. - 322 с. - ЭБС «IPRbooks» - Режим доступа: http://www.iprbookshop.ru/43960

3. Башлы, П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ П.Н. Башлы, А.В. Бабаш, Е.К. Баранова. - М.: РИОР, 2013 - 222с. - ЭБС «Znanium. com» - Режим доступа: http://znanium.com/catalog.php?bookinfo=405000

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Этапы формирования компетенции (номер семестра согласно учебному плану)	**Наименование учебных дисциплин, формирующих компетенции в процессе освоения образовательной программы**
ПК-5: способность проводить обоснование и выбор оптимального решения задач в сфере профессиональной деятельности	
4,5	Методы оптимизации
3	**Основы информационной безопасности**
ПК-9: способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах	
3	**Основы информационной безопасности**
9	Безопасность информационно-аналитических систем
6, 8	Производственная (организационно-технологическая) практика
11	Преддипломная практика
ПК-18: способность выявлять условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа, составляющих государственную, банковскую, коммерческую тайну, персональные данные	
3	**Основы информационной безопасности**
10, 11	Организационное и правовое обеспечение информационной безопасности

7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

Планируемые результаты освоения компетенции	Критерии оценивания результатов обучения				Наименование оценочного средства
	неудовлетворительно	удовлетворительно	хорошо	отлично	
ПК-5: способность проводить обоснование и выбор оптимального решения задач в сфере профессиональной деятельности					
Знать: состав задач обеспечения информационной безопасности, принципы разработки алгоритмов для оптимального решения типовых задач обеспечения информационной безопасности.	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	тесты, рефераты, зачет
Уметь: выделять типовые задачи обеспечения информационной безопасности, составлять алгоритмы их решения.	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть: навыками реализации алгоритмов оптимального решения типовых задач обеспечения информационной безопасности.	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	
ПК-9: способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах					
Знать: теоретические основы исследования информационных процессов предприятий, организаций, их классификацию; угрозы безопасности информации, модели нарушителя информационных систем, возможности проникновения нарушителя в информационную систему.	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	тесты, рефераты, зачет
Уметь: определять виды и формы информации, подверженной угрозам, классифицировать и систематизировать информационные массивы предприятий и организаций по совокупности признаков, определять возможные методы и пути реализации угроз; исследовать эффективность создаваемых информационных систем, в том числе средств обеспечения их информационной безопасности.	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть: навыками разработки моделей информационных процессов предприятий и организаций, оценки уязвимости информации различных видов и форм, выбора технологий, инструментальных средств, средств вычислительной техники и средств обеспече-	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	

ния информационной безопасности создаваемых информационных систем.					
ПК-18: способность выявлять условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа, составляющих государственную, банковскую, коммерческую тайну, персональные данные					
Знать: понятия сведений ограниченного доступа; понятия государственной, коммерческой, банковской и других тайн, персональных данных; виды правонарушений в отношении сведений ограниченного доступа.	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	тесты, рефераты, зачет
Уметь: проводить мониторинг и выявлять условия, способствующие совершению правонарушений в отношении сведений ограниченного доступа, составляющих государственную, банковскую, коммерческую тайну, персональные данные.	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	
Владеть: навыками обоснования и принятия решений, связанных с реализацией правовых норм, в пределах должностных обязанностей.	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	

7.3. Типовые контрольные задания и иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Тестовые задания для текущего контроля знаний по дисциплине

Вариант 1

1. Как называются умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним?
   а) разглашение
   б) утечка
   в) НСД
2. Как называется бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она доверена по техническим каналам утечки информации?
   а) разглашение
   б) утечка
   в) НСД
3. Как называется противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам?
   а) несанкционированный доступ
   б) санкционированный доступ
   в) НСД
4. Как называется вся накопленная информация об окружающей действительности, зафиксированная на любом материальном носителе?
   а) база знаний;
   б) база данных;
   в**)** информационные ресурсы.
5. Сведения, содержащие государственную тайну, относятся к:
   а) конфиденциальной информации;
   б) ценной информации;
   в) секретной информации.
6. Как называется главное средство закрепления информации различным способом на специальном носителе?
   а) база знаний;
   б) база данных;
   в) документ.
7. Сведения, содержащие коммерческую тайну, относятся к:
   а) секретной информации;
   б) конфиденциальной информации;
   в) персональным данным.
8. Как называются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления?
   а) информация;
   б) документ;
   в**)** информационные ресурсы.
9. Что является материальной основой работы информационной системы?
   а) информация;
   б) информационные ресурсы;
   в) информационные процессы.
10. Что является функциональной основой работы информационной системы?
    а) информация;
    б) информационные ресурсы;
    в**)** информационные процессы.

11. Как называется получение лицами в обход системы защиты с помощью программных, технических и др. средств, а также в силу случайных обстоятельств доступа к обрабатываемой и хранимой на объекте информации?
    а) разглашение информации;
    б) утечка информации;
    в) НСД к информации.
12. Как называется возможная опасность?
    а) угрозой;
    б) НСД;
    в) попыткой искажения информации.
13. Как называется умышленное или неосторожное действие должностных лиц и граждан, приведшее к оглашению охраняемых данных, а также передача таких данных по открытым техническим каналам?
    а) разглашение информации;
    б) утечка информации;
    в) НСД к информации.
14. Как называется способность информационной системы обеспечить законным пользователям условия доступа к ресурсам в соответствии с принятым режимом работы?
    а) готовность информационной системы;
    б) надежность информационной системы;
    в) конфиденциальность информационной системы.
15. Как называется бесконтрольный неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация была доверена?
    а) разглашение информации;
    б) утечка информации;
    в) НСД к информации.
16. Как называется способность информационной системы обеспечивать информационные потребности только законным пользователям в рамках их интересов?
    а) готовность информационной системы;
    б) надежность информационной системы;
    в) конфиденциальность информационной системы.
17. Как называется способность информационной системы обеспечивать целостность и сохранность информации ее законных пользователей?
    а) готовность информационной системы;
    б) надежность информационной системы;
    в**)** конфиденциальность информационной системы.
18. Сведения, содержащие личную тайну граждан, относятся к:
    а) секретной информации;
    б) конфиденциальной информации;
    в) персональным данным.
19. Временная комплексность защиты информации предполагает:
    а) непрерывность осуществления мероприятий по ЗИ;
    б) обеспечение требуемого уровня защиты во всех элементах системы обработки информации;
    в) что методы защиты должны быть направлены на все выполняемые функции системы обработки информации.

Вариант 2

1. Как называется вся накопленная информация об окружающей действительности, зафиксированная на любом материальном носителе?
    а) база знаний;
    б) база данных;
    в**)** информационные ресурсы.

2. Как называется противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам?
   а) несанкционированный доступ
   б) санкционированный доступ
   в) НСД

3. Как называется главное средство закрепления информации различным способом на специальном носителе?
   а) база знаний;
   б) база данных;
   в) документ.

4. Как называются умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним?
   а) разглашение
   б) утечка
   в) НСД

5. Сведения, содержащие государственную тайну, относятся к:
   а) конфиденциальной информации;
   б) ценной информации;
   в) секретной информации.

6. Как называются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления?
   а) информация;
   б) документ;
   в) информационные ресурсы.

7. Как называется способность информационной системы обеспечивать информационные потребности только законным пользователям в рамках их интересов?
   а) готовность информационной системы;
   б) надежность информационной системы;
   в) конфиденциальность информационной системы.

8. Что является материальной основой работы информационной системы?
   а) информация;
   б) информационные ресурсы;
   в) информационные процессы.

9. Как называется получение лицами в обход системы защиты с помощью программных, технических и др. средств, а также в силу случайных обстоятельств доступа к обрабатываемой и хранимой на объекте информации?
   а) разглашение информации;
   б) утечка информации;
   в) НСД к информации.

10. Как называется возможная опасность?
   а) угрозой;
   б) НСД;
   в) попыткой искажения информации.

11. Как называется способность информационной системы обеспечивать целостность и сохранность информации ее законных пользователей?
   а) готовность информационной системы;
   б) надежность информационной системы;
   в) конфиденциальность информационной системы.

12. Как называется способность информационной системы обеспечить законным пользователям условия доступа к ресурсам в соответствии с принятым режимом работы?
   а) готовность информационной системы;
   б) надежность информационной системы;
   в) конфиденциальность информационной системы.

13. Что является функциональной основой работы информационной системы?

а) информация;
б) информационные ресурсы;
в) информационные процессы.

14. Временная комплексность защиты информации предполагает:
а) интеграцию всех видов и направлений ИБ для достижения поставленных целей;
б) обеспечение требуемого уровня защиты во всех элементах системы обработки информации;
в) непрерывность осуществления мероприятий по защите информации.

15. Сведения, содержащие коммерческую тайну, относятся к:
а) секретной информации;
б) конфиденциальной информации;
в) персональным данным.

16. Сведения, содержащие личную тайну граждан, относятся к:
а) секретной информации;
б) конфиденциальной информации;
в) персональным данным.

17. Как называется умышленное или неосторожное действие должностных лиц и граждан, приведшее к оглашению охраняемых данных, а также передача таких данных по открытым техническим каналам?
а) разглашение информации;
б) утечка информации;
в) НСД к информации.

18. Как называется бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она доверена по техническим каналам утечки информации?
а) разглашение
б) утечка
в) НСД

19. Функциональная комплексность защиты информации предполагает:
а) интеграцию всех видов и направлений ИБ для достижения поставленных целей;
б) обеспечение требуемого уровня защиты во всех элементах системы обработки информации;
в) что методы защиты должны быть направлены на все выполняемые функции системы обработки информации.

Вариант 3

1. Сведения, содержащие государственную тайну, относятся к:
а) конфиденциальной информации;
б) ценной информации;
в) секретной информации.

2. Как называются умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним?
а) разглашение
б) утечка
в) НСД

3. Как называется способность информационной системы обеспечивать информационные потребности только законным пользователям в рамках их интересов?
а) готовность информационной системы;
б) надежность информационной системы;
в) конфиденциальность информационной системы.

4. Что является материальной основой работы информационной системы?
а) информация;
б) информационные ресурсы;
в) информационные процессы.

5. Как называется главное средство закрепления информации различным способом на специальном носителе?
   а) база знаний;
   б) база данных;
   в) документ.

6. Как называется получение лицами в обход системы защиты с помощью программных, технических и др. средств, а также в силу случайных обстоятельств доступа к обрабатываемой и хранимой на объекте информации?
   а) разглашение информации;
   б) утечка информации;
   в) НСД к информации.

7. Как называется возможная опасность?
   а) угрозой;
   б) НСД;
   в) попыткой искажения информации.

8. Как называется умышленное или неосторожное действие должностных лиц и граждан, приведшее к оглашению охраняемых данных, а также передача таких данных по открытым техническим каналам?
   а) разглашение информации;
   б) утечка информации;
   в) НСД к информации.

9. Как называются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления?
   а) информация;
   б) документ;
   в**)** информационные ресурсы.

10. Что является функциональной основой работы информационной системы?
   а) информация;
   б) информационные ресурсы;
   в**)** информационные процессы.

11. Как называется способность информационной системы обеспечить законным пользователям условия доступа к ресурсам в соответствии с принятым режимом работы?
   а) готовность информационной системы;
   б) надежность информационной системы;
   в) конфиденциальность информационной системы.

12. Как называется вся накопленная информация об окружающей действительности, зафиксированная на любом материальном носителе?
   а) база знаний;
   б) база данных;
   в**)** информационные ресурсы.

13. Сведения, содержащие коммерческую тайну, относятся к:
   а) секретной информации;
   б) конфиденциальной информации;
   в) персональным данным.

14. Как называется противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам?
   а) несанкционированный доступ
   б) санкционированный доступ
   в) НСД

15. Функциональная комплексность защиты информации предполагает:
   а) интеграцию всех видов и направлений ИБ для достижения поставленных целей;
   б) обеспечение требуемого уровня защиты во всех элементах системы обработки информации;
   в) что методы защиты должны быть направлены на все выполняемые функции системы обработки информации.

16. Как называется бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она доверена по техническим каналам утечки информации?
а) разглашение
б) утечка
в) НСД

17. Что является продуктом информационной системы?
а) информация;
б) информационные ресурсы;
в) информационные процессы.

18. Как называется способность информационной системы обеспечивать целостность и сохранность информации ее законных пользователей?
а) готовность информационной системы;
б) надежность информационной системы;
в**)** конфиденциальность информационной системы.

19. Структурная комплексность защиты информации предполагает:
а) интеграцию всех видов и направлений ИБ для достижения поставленных целей;
б) обеспечение требуемого уровня защиты во всех элементах системы обработки информации;
в) что методы защиты должны быть направлены на все выполняемые функции системы обработки информации.

Темы рефератов

1. Информационная война и ее виды.
2. Информационное оружие и его классификация.
3. Примеры ведения информационных войн в истории человечества.
4. Виды возможных нарушений информационной системы.
5. Основные технологии построения защищенных информационных систем.
6. Основные классификационные признаки компьютерных вирусов.
7. Методы и технологии борьбы с компьютерными вирусами.
8. Условия безопасной работы КС и технология обнаружения заражения вирусами.
9. Криптографическая защита информации.
10. Информационная безопасность в условиях функционирования в России глобальных сетей.

Примерный перечень вопросов к зачету по дисциплине для обучающихся

1. Понятие информационной безопасности. Основные определения и термины.
2. Интересы и угрозы в области национальной безопасности.
3. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.
4. Основные понятия, общеметодологические принципы обеспечения информационной безопасности.
5. Информация.
6. Информационная сфера.
7. Информационная безопасность.
8. Национальные интересы в информационной сфере.
9. Источники и содержание угроз в информационной сфере.
10. Основные положения государственной информационной политики Российской Федерации.
11. Первоочередные мероприятия по реализации государственной политики.
12. Понятие «информационный ресурс».
13. Классы информационных ресурсов.
14. Документы.

15. Обобщенная модель документа.
16.Информация и ее виды.
17. Информационное оружие и его классификация.
18. Информационная война.
19. Виды информационных войн.
20. Правовое регулирование информационных потоков в различных видах деятельности.
21. Международные и отечественные правовые и нормативные акты обеспечения ИБ процессов переработки информации.
22. Организационное регулирование защиты процессов переработки информации.
23. Информация как объект юридической защиты.
24. Основные принципы засекречивания информации.
25. Государственная система правового обеспечения защиты информации в Российской Федерации.
26. Общие положения об информационных системах.
27. Информация как продукт.
28. Информационные услуги.
29**.** Источники конфиденциальной информации в информационных системах.
30. Что приводит к неправомерному овладению конфиденциальной информацией в информационных системах.
31. Виды технических средств информационных систем.
32. Классы каналов несанкционированного получения информации**.**
33. Причины нарушения целостности информации.
34. Виды угроз информационным системам.
35 Виды потерь.
36. Убытки, связанные с информационным обменом.
37. Модель нарушителя информационных систем.
38. Методы определения требований к защите информации.
39. Требования к безопасности информационных систем в России.
40. Классы защищенности СВТ от НСД.
41. Факторы, влияющие на требуемый уровень защиты информации.
42. Критерии оценки безопасности информационных технологий.
43. Общие положения о функциях и задачах защиты информации.
44. Методы формирования функций защиты.
45. Классы задач защиты информации.
46. Функции защиты.
47. Состояния и функции системы защиты информации.
48. Содержание способов и средств обеспечения безопасности.
49. Методы и средства защиты информации.
50. Формальные средства защиты.
51. Неформальные средства защиты.
52. Требования к архитектуре СЗИ.
53. Построение СРВ.
54. Ядро системы защиты информации.
55. Ресурсы системы защиты информации.
56. Организационное построение.

Тестовые задания для контроля остаточных знаний по дисциплине

1 вариант

1. Как называется территория вокруг автоматизированной системы обработки данных, на которой персоналом и средствами системы не применяются никакие средства и не осуществляются никакие мероприятия для защиты информации?

а) неконтролируемая зона;

б) внешняя неконтролируемая зона;
в) зона ресурсов.

2. Как называется территория вокруг автоматизированной системы обработки данных, которая непрерывно контролируется персоналом или средствами автоматизированной системы обработки данных?
а) контролируемая зона;
б) внешняя контролируемая зона
в) зона расположения помещений.

3. Как называется внутреннее пространство тех помещений, в которых расположена система?
а) зона расположения помещений;
б) зона ресурсов;
в) контролируемая зона.

4. Как называется та часть помещений, откуда возможен непосредственный доступ к ресурсам системы?
а) зона расположения помещений;
б) зона ресурсов;
в) зона баз данных.

5. Как называется та часть ресурсов системы, с которой возможен непосредственный доступ к защищаемым данным?
а) зона расположения помещений;
б) зона ресурсов;
в) зона баз данных.

6. Сущность какого подхода к оценке уязвимости информации основана на длительном сборе и обработке данных о реальных появлениях угроз информации и о размерах причиненного при этом ущерба?
а) эмпирического;
б) теоретического;
в) теоретико-эмпирического.

7. Оборонительная стратегия применяется для:
а) наиболее опасных угроз;
б) всех известных угроз;
в) всех потенциально возможных угроз.

8. Наступательная стратегия применяется для:
а) наиболее опасных угроз;
б) всех известных угроз;
в) всех потенциально возможных угроз.

9. Упреждающая стратегия применяется для:
а) наиболее опасных угроз;
б) всех известных угроз;
в) всех потенциально возможных угроз.

10. К какой стратегии защиты информации относится разработка для существующего объекта организационных мер использования технических средств по ограничению НСД к объекту?
а) оборонительная;
б) наступательная;
в) упреждающая.

11. Какая стратегия защиты информации предполагает тщательное исследование возможных угроз системы обработки информации и разработку мер по их нейтрализации еще на стадии проектирования и изготовления системы?
а) оборонительная;
б) наступательная;
в) упреждающая.

12. Какая стратегия защиты информации предполагает использование конкретных мер защиты для каждого конкретного вида угроз (например, антивирусные программы – против компьютерных инфекций)?

а) оборонительная;
б) наступательная;
в) упреждающая.

13. К каким средствам защиты информации относятся физические, аппаратные и программные средства?

а) к формальным;
б) к неформальным;
в) к техническим.

14. К каким средствам защиты информации относятся организационные, законодательные и морально-этические средства?

а) к формальным;
б) к неформальным;
в) к техническим.

15. К каким средствам защиты информации относятся физические и аппаратные средства?

а) к формальным;
б) к неформальным;
в) к техническим.

16. К каким средствам защиты относятся механические, электрические, электромеханические устройства и системы, функционирующие автономно, создавая различного рода препятствия на пути дестабилизирующих факторов?

а) к физическим;
б) к аппаратным;
в) к техническим.

17. К каким средствам защиты относятся электронные и электронномеханические устройства, встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации?

а) к физическим;
б) к аппаратным;
в) к техническим.

2 Вариант

1. К каким средствам защиты относятся электронные и электронномеханические устройства, встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации?

а) к программным;
б) к аппаратным;
в) к техническим.

2. К какой стратегии защиты информации относится разработка для существующего объекта организационных мер использования технических средств по ограничению НСД к объекту?

а) оборонительная;
б) наступательная;
в) упреждающая.

3. Какая стратегия защиты информации предполагает тщательное исследование возможных угроз системы обработки информации и разработку мер по их нейтрализации еще на стадии проектирования и изготовления системы?

а) оборонительная;
б) наступательная;
в) упреждающая.

4. Какая стратегия защиты информации предполагает использование конкретных мер защиты для каждого конкретного вида угроз (например, антивирусные программы – против компьютерных инфекций)?

а) оборонительная;

б) наступательная;

в) упреждающая.

5. К каким средствам защиты информации относятся физические, аппаратные и программные средства?

а) к формальным;

б) к неформальным;

в) к техническим.

6. К каким средствам защиты информации относятся организационные, законодательные и морально-этические средства?

а) к формальным;

б) к неформальным;

в) к техническим.

7. К каким средствам защиты информации относятся физические и аппаратные средства?

а) к формальным;

б) к неформальным;

в) к техническим.

8. К каким средствам защиты относятся механические, электрические, электромеханические устройства и системы, функционирующие автономно, создавая различного рода препятствия на пути дестабилизирующих факторов?

а) к физическим;

б) к аппаратным;

в) к техническим.

9. Как называется территория вокруг автоматизированной системы обработки данных, на которой персоналом и средствами системы не применяются никакие средства и не осуществляются никакие мероприятия для защиты информации?

а) неконтролируемая зона;

б) внешняя неконтролируемая зона;

в) зона ресурсов.

10. Как называется территория вокруг автоматизированной системы обработки данных, которая непрерывно контролируется персоналом или средствами автоматизированной системы обработки данных?

а) контролируемая зона;

б) внешняя контролируемая зона

в) зона расположения помещений.

11. Как называется внутреннее пространство тех помещений, в которых расположена система?

а) зона расположения помещений;

б) зона ресурсов;

в) контролируемая зона.

12. Как называется та часть помещений, откуда возможен непосредственный доступ к ресурсам системы?

а) зона расположения помещений;

б) зона ресурсов;

в) зона баз данных.

13. Как называется та часть ресурсов системы, с которой возможен непосредственный доступ к защищаемым данным?

а) зона расположения помещений;

б) зона ресурсов;

в) зона баз данных.

14. Сущность какого подхода к оценке уязвимости информации основана на длительном сборе и обработке данных о реальных появлениях угроз информации и о размерах причиненного при этом ущерба?

а) эмпирического;
б) теоретического;
в) теоретико-эмпирического.

15. Оборонительная стратегия применяется для:
а) наиболее опасных угроз;
б) всех известных угроз;
в) всех потенциально возможных угроз.

16. Наступательная стратегия применяется для:
а) наиболее опасных угроз;
б) всех известных угроз;
в) всех потенциально возможных угроз.

17. Упреждающая стратегия применяется для:
а) наиболее опасных угроз;
б) всех известных угроз;
в) всех потенциально возможных угроз.

3 Вариант

1. Какая стратегия защиты информации предполагает использование конкретных мер защиты для каждого конкретного вида угроз (например, антивирусные программы – против компьютерных инфекций)?

а) оборонительная;
б) наступательная;
в) упреждающая.

2. К каким средствам защиты информации относятся физические, аппаратные и программные средства?

а) к формальным;
б) к неформальным;
в) к техническим.

3. К каким средствам защиты информации относятся организационные, законодательные и морально-этические средства?

а) к формальным;
б) к неформальным;
в) к техническим.

4. К каким средствам защиты информации относятся физические и аппаратные средства?

а) к формальным;
б) к неформальным;
в) к техническим.

5. К каким средствам защиты относятся механические, электрические, электромеханические устройства и системы, функционирующие автономно, создавая различного рода препятствия на пути дестабилизирующих факторов?

а) к физическим;
б) к аппаратным;
в) к техническим.

6. Как называется территория вокруг автоматизированной системы обработки данных, на которой персоналом и средствами системы не применяются никакие средства и не осуществляются никакие мероприятия для защиты информации?

а) неконтролируемая зона;
б) внешняя неконтролируемая зона;
в) зона ресурсов.

7. Как называется территория вокруг автоматизированной системы обработки данных, которая непрерывно контролируется персоналом или средствами автоматизированной системы обработки данных?

а) контролируемая зона;

б) внешняя контролируемая зона

в) зона расположения помещений.

8. К какой стратегии защиты информации относится разработка для существующего объекта организационных мер использования технических средств по ограничению НСД к объекту?

а) оборонительная;

б) наступательная;

в) упреждающая.

9. Какая стратегия защиты информации предполагает тщательное исследование возможных угроз системы обработки информации и разработку мер по их нейтрализации еще на стадии проектирования и изготовления системы?

а) оборонительная;

б) наступательная;

в) упреждающая

10. Как называется внутреннее пространство тех помещений, в которых расположена система?

а) зона расположения помещений;

б) зона ресурсов;

в) контролируемая зона.

11. Как называется та часть помещений, откуда возможен непосредственный доступ к ресурсам системы?

а) зона расположения помещений;

б) зона ресурсов;

в) зона баз данных.

12. Как называется та часть ресурсов системы, с которой возможен непосредственный доступ к защищаемым данным?

а) зона расположения помещений;

б) зона ресурсов;

в) зона баз данных.

13. Сущность какого подхода к оценке уязвимости информации основана на длительном сборе и обработке данных о реальных появлениях угроз информации и о размерах причиненного при этом ущерба?

а) эмпирического;

б) теоретического;

в) теоретико-эмпирического.

14. Оборонительная стратегия применяется для:

а) наиболее опасных угроз;

б) всех известных угроз;

в) всех потенциально возможных угроз.

15. Наступательная стратегия применяется для:

а) наиболее опасных угроз;

б) всех известных угроз;

в) всех потенциально возможных угроз.

16. Упреждающая стратегия применяется для:

а) наиболее опасных угроз;

б) всех известных угроз;

в) всех потенциально возможных угроз.

17. К каким средствам защиты относятся электронные и электронномеханические устройства, встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации?

а) к физическим;

б) к программным;

в) к техническим.

7.1. Методические материалы, определяющие процедуры оценивания знаний, умений и навыков, и опыта деятельности, характеризующих этапы формирования компетенций

Требования к написанию реферата

Продукт самостоятельной работы обучающегося, представляющий собой краткое изложение в письменном виде полученных результатов (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.

Реферат должен быть структурирован (по главам, разделам, параграфам) и включать разделы: введение, основная часть, заключение, список использованных источников. В зависимости от тематики реферата к нему могут быть оформлены приложения, содержащие документы, иллюстрации, таблицы, схемы и т.д. Объем реферата – 15-20 страниц печатного текста, включая титульный лист, введение, заключение и список литературы.

Его задачами являются:

1. Формирование умений самостоятельной работы с источниками литературы, их систематизация;

2. Развитие навыков логического мышления;

3. Углубление теоретических знаний по проблеме исследования.

При оценке реферата используются следующие критерии:

- новизна текста;
- обоснованность выбора источника;
- степень раскрытия сущности вопроса;
- соблюдения требований к оформлению.

Критерии оценивания реферата:	
«отлично»	Выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.
«хорошо»	Основные требования к реферату и его защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; невыдержан объём реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.
«удовлетворительно»	Имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод.
«неудовлетворительно»	Тема реферата не раскрыта, обнаруживается существенное не понимание проблемы.

Тематика рефератов выдается преподавателем в конце семинарского занятия.

Требования к выполнению тестового задания

Тестирование является одним из основных средств формального контроля качества обучения. Это метод, основанный на стандартизированных заданиях, которые позволяют измерить психофизиологические и личностные характеристики, а также знания, умения и навыки испытуемого.

Основные принципы тестирования, следующие:

− связь с целями обучения - цели тестирования должны отвечать критериям социальной полезности и значимости, научной корректности и общественной поддержки;

− объективность - использование в педагогических измерениях этого принципа призвано не допустить субъективизма и предвзятости в процессе этих измерений;

− справедливость и гласность - одинаково доброжелательное отношение ко всем обучающимся, открытость всех этапов процесса измерений, своевременность ознакомления обучающихся с результатами измерений;

− систематичность – систематичность тестирований и самопроверок каждого учебного модуля, раздела и каждой темы; важным аспектом данного принципа является требование репрезентативного представления содержания учебного курса в содержании теста;

- гуманность и этичность - тестовые задания и процедура тестирования должны исключать нанесение какого-либо вреда обучающимся, не допускать ущемления их по национальному, этническому, материальному, расовому, территориальному, культурному и другим признакам;

Важнейшим является принцип, в соответствии с которым тесты должны быть построены по методике, обеспечивающей выполнение требований соответствующего федерального государственного образовательного стандарта.

В тестовых заданиях используются четыре типа вопросов:

− закрытая форма - является наиболее распространенной и предлагает несколько альтернативных ответов на поставленный вопрос. Например, обучающемуся задается вопрос, требующий альтернативного ответа «да» или «нет», «является» или «не является», «относится» или «не относится» и т.п. Тестовое задание, содержащее вопрос в закрытой форме, включает в себя один или несколько правильных ответов и иногда называется выборочным заданием. Закрытая форма вопросов используется также в тестах-задачах с выборочными ответами. В тестовом задании в этом случае сформулированы условие задачи и все необходимые исходные данные, а в ответах представлены несколько вариантов результата решения в числовом или буквенном виде. Обучающийся должен решить задачу и показать, какой из представленных ответов он получил.

− открытая форма - вопрос в открытой форме представляет собой утверждение, которое необходимо дополнить. Данная форма может быть представлена в тестовом задании, например, в виде словесного текста, формулы (уравнения), графика, в которых пропущены существенные составляющие - части слова или буквы, условные обозначения, линии или изображения элементов схемы и графика. Обучающийся должен по памяти вставить соответствующие элементы в указанные места («пропуски»).

− установление соответствия - в данном случае обучающемуся предлагают два списка, между элементами которых следует установить соответствие;

− установление последовательности - предполагает необходимость установить правильную последовательность предлагаемого списка слов или фраз.

Критерии оценки знаний при проведении тестирования

Отметка «отлично» выставляется при условии правильного ответа не менее чем 85% тестовых заданий;

Отметка «хорошо» выставляется при условии правильного ответа не менее чем 70 % тестовых заданий;

Отметка «удовлетворительно» выставляется при условии правильного ответа не менее 50 %;

Отметка «неудовлетворительно» выставляется при условии правильного ответа менее чем на 50 % тестовых заданий.

Результаты текущего контроля используются при проведении промежуточной аттестации.

Критерии оценки знаний на зачете

1. Оценка **«зачтено»** выставляется обучающемуся, 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 занятиях.

2. Оценка **«не зачтено»** выставляется обучающемуся, который не справился с 50% вопросов и заданий билета, в ответах на другие вопросы допустил существенные ошибки. Не может ответить на дополнительные вопросы, предложенные преподавателем. Целостного представления о взаимосвязях, компонентах, этапах развития культуры у обучающегося нет.

Оценивается качество устной и письменной речи, как и при выставлении положительной оценки.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Основная литература

1. Баранова, Е.К. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Е.К. Баранова, А.В. Бабаш. - М.: РИОР, ИНФРА-М, 2016. - 322 с. - ЭБС «Znanium. com» - Режим доступа: http://znanium.com/catalog.php?bookinfo=763644

2. Галатенко, В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 266 с. - ЭБС «IPRbooks» - Режим доступа: http://www.iprbookshop.ru/52209

3. Петров, С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А. - Саратов: Ай Пи Ар Букс, 2015. - 326 с. - ЭБС «IPRbooks» - Режим доступа: http://www.iprbookshop.ru/33857

8.2. Дополнительная литература

1. Защита информации [Электронный ресурс]: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - Москва: РИОР: ИНФРА-М, 2015. - 392 с. - ЭБС «Znanium. com» - Режим доступа: http://znanium.com/catalog.php?bookinfo=474838

2. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Нестеров С.А. - СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014. - 322 с. - ЭБС «IPRbooks» - Режим доступа: http://www.iprbookshop.ru/43960

3. Башлы, П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебник/ П.Н. Башлы, А.В. Бабаш, Е.К. Баранова. - М.: РИОР, 2013 - 222с. - ЭБС «Znanium. com» - Режим доступа: http://znanium.com/catalog.php?bookinfo=405000

8.3. Информационно-телекоммуникационные ресурсы сети «Интернет»

1. Образовательный портал ФГБОУ ВО «МГТУ» [Электронный ресурс]: Режим доступа: https://mkgtu.ru/

2. Официальный сайт Правительства Российской Федерации. [Электронный ресурс]: Режим доступа: http://www.government.ru

3. Информационно-правовой портал «Гарант» [Электронный ресурс]: Режим доступа: http://www.garant.ru/

4. Научная электронная библиотека www.eLIBRARY.RU – Режим доступа: http://elibrary.ru/

5. Электронный каталог библиотеки – Режим доступа: // http://lib.mkgtu.ru:8004/catalog/fol2;

6. Единое окно доступа к образовательным ресурсам: Режим доступа: http://window.edu.ru/

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Б1.Б.17 Основы информационной безопасности

Раздел / Тема с указанием основных учебных элементов	Методы обучения	Способы (формы) обучения	Средства обучения	Формируемые компетенции
Тема 1. Введение. Основные понятия, общеметодологические принципы информационной безопасности	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Учебники, учебные пособия, первоисточники	способность проводить обоснование и выбор оптимального решения задач в сфере профессиональной деятельности (ПК-5)
Тема 2. Информация - наиболее ценный ресурс современного общества. Проблемы информационной войны.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Учебники, учебные пособия	способность проводить обоснование и выбор оптимального решения задач в сфере профессиональной деятельности (ПК-5)
Тема 3. Организационно-правовое обеспечение информационной безопасности	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродук-	Домашние задания	Учебники, учебные пособия, первоисточники	способность проводить обоснование и выбор оптимального решения задач в сфере профессиональной деятельности (ПК-5); способность выявлять условия, способствующие совершению

	тивный			правонарушений в отношении сведений ограниченного доступа, составляющих государственную, банковскую, коммерческую тайну, персональные данные (ПК-18).
Тема 4. Информационные системы. Общие положения. Информация как продукт.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Учебники, учебные пособия, раздаточный материал	способность выявлять угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-9)
Тема 5. Угрозы информации	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Учебники, учебные пособия, , раздаточный материал	способность выявлять угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-9)
Тема 6. Методы и модели оценки уязвимости информации	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной дея-**	Домашние задания	Учебники, учебные пособия	способность выявлять угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-9)

	тельности: объяснительно-иллюстративный, репродуктивный			
Тема 7. Методы определения требований к защите информации	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Учебники, учебные пособия	способность проводить обоснование и выбор оптимального решения задач в сфере профессиональной деятельности (ПК-5)
Тема 8. Анализ существующих методик определения требований к защите информации	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Учебники, учебные пособия, , раздаточный материал	способность выявлять угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-9)
Тема 9. Функции и задачи защиты информации. Стратегии защиты информации.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Учебники, учебные пособия	способность проводить обоснование и выбор оптимального решения задач в сфере профессиональной деятельности (ПК-5); способность выявлять угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-

				9)
Тема 10. Способы и средства защиты информации	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Учебники, учебные пособия	способность выявлять угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-9)
Тема 11. Архитектура систем защиты информации (СЗИ)	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Учебники, учебные пособия	способность проводить обоснование и выбор оптимального решения задач в сфере профессиональной деятельности (ПК-5); способность выявлять угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-9)

Учебно-методические материалы по практическим (лабораторным) занятиям дисциплины
Б1.Б.17 Основы информационной безопасности

№ раздела дисциплины	Наименование практических работ	Методы обучения	Способы (формы) обучения	Средства обучения
1		2	3	4
Тема 1. Организационно-правовое обеспечение информационной безопасности.	Классификация информационных ресурсов. Категории объектов и защита информационной собственности. Организационное регулирование защиты процессов переработки информации. Информация как объект юридической защиты. Основные принципы засекречивания информации. Государственная система правового обеспечения защиты информации в Российской Федерации.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Устная речь, учебники, учебные пособия, первоисточники
Тема 2. Информационные системы. Общие положения. Информация как продукт.	Основные положения теории информационной безопасности информационных систем. Концепция информационной безопасности. Источники конфиденциальной информации в информационных системах. Что приводит к неправомерному овладению конфиденциальной информацией в инфор-	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Устная речь, учебники, учебные пособия, раздаточный материал

	мационных системах. Виды технических средств информационных систем. Информационные службы и информационные услуги. Виды возможных нарушений информационной системы. Основные технологии построения защищенных информационных систем.			
Тема 3. Угрозы информации	Понятие угрозы. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации. Виды угроз информационным системам. Виды потерь. Убытки, связанные с информационным обменом. Международные стандарты информационного обмена. Виды противников или «нарушителей». Модель нарушителя информационных систем. Информационные инфекции.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Устная речь, учебники, учебные пособия, раздаточный материал
Тема 4. Методы и модели оценки уязвимости информации	Классификация нарушений информационной безопасности вычислительной системы и причины, обуславливающие	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**:	Домашние задания	Устная речь, учебники, учебные пособия

	их существование. Анализ способов нарушений информационной безопасности. Эмпирический подход к оценке уязвимости информации. Система с полным перекрытием. Модели безопасности и их применение.	объяснительно-иллюстративный, репродуктивный		
Тема 5. Методы определения требований к защите информации	Требования, обусловленные спецификой автоматизированной обработки информации. Требования, связанные с размещением защищаемой информации. Требования, определяемые структурой автоматизированной системы обработки данных. Требования, обусловленные видом защищаемой информации. Требования, обусловленные технологическими схемами автоматизированной обработки информации. Требования, обусловленные способом взаимодействия пользователя с комплексом средств автоматизации. Требования, обусловленные режимом функционирования комплексов	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Устная речь, учебники, учебные пособия

	средств автоматизации. Требования, обусловленные этапом жизненного цикла автоматизированной системы обработки данных.			
Тема 6. Анализ существующих методик определения требований к защите информации	Требования к безопасности информационных систем в США. Требования к безопасности информационных систем в России. Классы защищенности СВТ от НСД. Оценка состояния безопасности ИС Франции. Факторы, влияющие на требуемый уровень защиты информации. Критерии оценки безопасности информационных технологий.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Устная речь, учебники, учебные пособия, раздаточный материал
Тема 7. Функции и задачи защиты информации. Стратегии защиты информации.	Защита. Общие положения. Методы формирования функций защиты. Классы задач защиты информации. Функции защиты. Состояния и функции системы защиты информации. Понятие «стратегия». Проблемы, затрудняющие решение задач обеспечения информационной безопасности. Основные стратегии защиты информации.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Устная речь, учебники, учебные пособия

Тема 8. Способы и средства защиты информации	Использование защищенных компьютерных систем. Содержание способов и средств обеспечения безопасности: препятствие, управление, маскировка, регламентация, принуждение, побуждение, нападение. Методы и средства защиты информации. Формальные и неформальные средства защиты. Методы криптографии. Информационная безопасность в условиях функционирования в России глобальных сетей.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Самостоятельная работа обучающегося, домашние задания	Устная речь, учебники, учебные пособия
Тема 9. Архитектура систем защиты информации (СЗИ)	Требования к архитектуре СЗИ. Построение СРВ. Ядро системы защиты информации. Ресурсы системы защиты информации. Организационное построение.	**по источнику знаний:** лекция, чтение, конспектирование **по назначению:** приобретение знаний, анализ, закрепление, проверка знаний **по типу познавательной деятельности**: объяснительно-иллюстративный, репродуктивный	Домашние задания	Устная речь, учебники, учебные пособия

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, позволяют:

- организовать процесс образования путем визуализации изучаемой информации посредством использования презентаций, учебных фильмов;
- контролировать результаты обучения на основе компьютерного тестирования;
- автоматизировать расчеты аналитических показателей, предусмотренные программой научно-исследовательской работы;
- автоматизировать поиск информации посредством использования справочных систем.

Для осуществления учебного процесса используется свободно распространяемое (бесплатное не требующее лицензирования) программное обеспечение и лицензионное программное обеспечение компаний Microsoft и Kaspersky:

1. Операционная система на базе Linux;
2. Офисный пакет Open Office;
3. Тестовая система собственной разработки, правообладатель ФГБОУ ВО «МГТУ», свидетельство №2013617338.
4. Программные продукты компании Microsoft для государственных образовательных учреждений (Microsoft Open Value Subscription Education Solutions Agreement № V8209819. Срок действия до 07.2018 г.). Пакет включает в себя весь спектр программ (операционные системы разного класса, СУБД, средства разработки, офисный пакет).
5. Антивирусные программы: Endpoint Security - № лицензии 17E0-160128131746407 72.

11. Описание материально-технической базы необходимой для осуществления образовательного процесса по дисциплине (модулю)

Наименования специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
Специальные помещения		
Учебные аудитории, оснащенные мультимедийным оборудованием 3-1 Лаборатория программирования и защиты информационных процессов в компьютерных системах 3-2	мультимедийный проектор; компьютеры, оргтехника, аудио-, видеотека, справочная литература; таблицы и слайды по специальности; видеофильмы, учебно-методические пособия, плакаты, видеокейсы	Соглашение (подписка) на программные продукты компании Microsoft для государственных образовательных учреждений (Microsoft Open Value Subscription Education Solutions Agreement № V8209819. Срок действия до 07.2018 г.). Пакет включает в себя весь спектр программ (операционные системы разного класса, СУБД, средства разработки, офисный пакет). Антивирусные программы: Kaspersky Endpoint Security - № лицензии 17E0160128-13174640772. Количество: 400 рабочих мест. Срок действия

		1 год.
Помещения для самостоятельной работы		
Читальный зал ФГБОУ ВО «МГТУ»: ул. Первомайская, 191, 3 этаж.	Читальный зал имеет 150 посадочных мест, компьютерное оснащение с выходом в Интернет на 30 посадочных мест; оснащен специализированной мебелью (столы, стулья, шкафы, шкафы выставочные), стационарное мультимедийное оборудование, оргтехника (принтеры, сканеры, ксероксы)	Свободно распространяемое (бесплатное не требующее лицензирования) программное обеспечение: 1. Операционная система на базе Linux; 2. Офисный пакет Open Office; 3. Графический пакет Gimp; 4. Векторный редактор Inkscape; Антивирусные программы: Kaspersky Endpoint Security - № лицензии 17E0160128-13174640772. Количество: 400 рабочих мест. Срок действия 1 год.

Дополнения и изменения в рабочей программе
за _____/_____ учебный год

В рабочую программу _____
(наименование дисциплины)

для направления (специальности) _____
(номер направления (специальности)

Приложение 4

вносятся следующие дополнения и изменения:

Дополнения и изменения внес _____
(должность, Ф.И.О., подпись)

Рабочая программа пересмотрена и одобрена на заседании кафедры
_____
(наименование кафедры)

«____»_____20 __г.

Заведующий кафедрой _____ _____
(подпись) (Ф.И.О.)