Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Платонова Т.К.
«25» июня 2024 г.

Рабочая программа дисциплины
Основы управления информационной безопасностью

Направление 10.03.01 "Информационная безопасность"
Направленность 10.03.01.02 Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

Для набора 2023 года

Квалификация
Бакалавр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	32	32	32	32
Итого ауд.	64	64	64	64
Контактная работа	64	64	64	64
Сам. работа	44	44	44	44
Итого	108	108	108	108

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 25.06.2024 г. протокол № 18.

Программу составил(и): к.т.н., доцент, Лапсарь А.П.

Зав. кафедрой: к.э.н., доцент Радченко Ю.В.

Методический совет направления: д.э.н., профессор Тищенко Е.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	получение обучаемыми теоретических знаний по организации управления информационной безопасностью на объектах информатизации и в организациях, использующих в своей деятельности информационные системы;
1.2	изучение и последующее освоение современных технологий защиты информации ограниченного доступа на объектах;
1.3	оптимизация организационных и технических мероприятий по обеспечению информационной безопасности организации

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;

ОПК-10: Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;

ОПК-2.4: Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами;

В результате освоения дисциплины обучающийся должен:

Знать:

состав и назначение нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации (соотнесено с индикатором ОПК- 5.1);
основные методы и технологии формирования политики информационной безопасности (соотнесено с индикатором ОПК-10.1);
требования нормативных документов по оценке защищенности объекта информатизации и правила проведения их аудита (соотнесено с индикатором ОПК- 2.4.1)

Уметь:

применять нормативные правовые акты, нормативные и методические докумены, регламентирующие деятельность по защите информации в процессе управления информационной безопасностью (соотнесено с индикатором ОПК- 5.2);
оценивать эффективность реализации систем защиты информации и политик безопасности в компьютерных системах, организовывать реализацию мер в области информаационной безопасности, формировать политику безопасности объектов защиты (соотнесено с индикатором ОПК-10.2);
организовывать подготовку и проведение аудита информационной безопасности объекта зыщиты, формировать отчетные материалы и обоснованные предложения по совершенствованию системы защиты информации (соотнесено с индикатором ОПК- 2.4.2)

Владеть:

навыки внедрения требований нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации (соотнесено с индикатором ОПК- 5.3);
навыками разработки политики информационной безопасности объекта защиты, планировать, организовывать и выполнять комплекс мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты (соотнесено с индикатором ОПК-10.3);
торганизовывать подготовку и проведение аудита информационной безопасности навыками планирования и организации аудита объекта зыщиты, формирования отчетных материалов, работы по реализации предложений по совершенствованию системы защиты информации (соотнесено с индикатором ОПК- 2.4.3)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Системы управления информационной безопасности

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
1.1	1 "Основные положения теории информационной безопасности». Исследование архитектуры построения систем управления информационной безопасностью. Оформление при помощи LibreOffice / Лек /	7	6	ОПК-5, ОПК-10, ОПК-2.4	Л1.1, Л1.2
1.2	1 "Основные положения теории информационной безопасности». Управление информационной безопасностью объекта информатизации. / Пр /	7	4	ОПК-5, ОПК-10, ОПК-2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л2.4, Л2.5
1.3	1 "Основные положения теории информационной безопасности». Информационная безопасность: основные определения. Понятие конфиденциальности, целостности, доступности информации. Формальные модели управления доступом: модель Харрисона-	7	8	ОПК-5, ОПК-10, ОПК-2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

	Руззо-Ульмана, модель Белла Ла-Падулы. Формальные модели целостности: модель Кларка-Вилсона, модель Биба. Совместное использование моделей безопасности. Ролевое управление доступом. / Ср /				
1.4	2 «Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз». Исследование свойств локальной политики безопасности. Оформление при помощи LibreOffice / Лек /	7	10	ОПК-5, ОПК-10, ОПК-2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.5	2 «Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз». Управление средствами защиты информации на объекте. / Пр /	7	8	ОПК-5, ОПК-10, ОПК-2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л2.4, Л2.5
1.6	2 «Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз». Классификация угроз информационной безопасности. Построение систем защиты от угроз нарушения конфиденциальности информации: модель системы защиты, организационное обеспечение ИБ, идентификация и аутентификация, разграничение доступа, криптографические методы, контроль внешнего периметра, протоколирование, аудит. Построение систем защиты от угроз нарушения целостности информации: модель обеспечения целостности, криптографические методы. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. / Ср /	7	12	ОПК-5, ОПК-10, ОПК-2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

Раздел 2. Методы и технологии информационной безопасности

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
2.1	Тема 1 "Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы». Исследование функционирования систем управления информационной безопасностью на объекте защиты. / Лек /	7	8	ОПК-5, ОПК-10, ОПК-2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.2	Тема 1 "Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы». Контроль и аудит состояния информационной безопасности на объектах информатизации. Мониторинг состояния информационной безопасности. Формы представления результатов контроля. / Пр /	7	12	ОПК-5, ОПК-10, ОПК-2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л2.4, Л2.5
2.3	Тема 1 "Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы». Классификация возможных каналов утечки информации. Технологии зашиты акустической информации от утечки. Технологии зашиты информации от утечки по каналам ПЭМИН. Технологии зашиты видовой информации от утечки. / Ср /	7	8	ОПК-5, ОПК-10, ОПК-2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.4	Тема 2 «Управление безопасностью в компьютерной системе». Классификация методов зашиты информации от программно-математических воздействий. Категорирование объектов информатизации. Деятельность администратора безопасности по предотвращению программно-математических воздействий. Деятельность администратора безопасности по минимизации последствий программно-математических воздействий. / Лек /	7	8	ОПК-5, ОПК-10, ОПК-2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.5	Тема 2 «Управление безопасностью в компьютерной системе». Оценка эффективности проводимых мероприятий по совершенствованию системы управления информационной безопасностью. Экспертные методы оценки эффективности систем информационной безопасности. Расчетно-аналитические методы оценки эффективности систем информационной безопасности. / Пр /	7	8	ОПК-5, ОПК-10, ОПК-2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л2.4, Л2.5
2.6	Тема 2 «Управление безопасностью в компьютерной системе». Термины и определения. Системы удаленного управления безопасности: в отсутствии локального объекта управления, при	7	16	ОПК-5, ОПК-10, ОПК-2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

	локальном объекте управления и удаленном управляющем объекте, при распределенном объекте управления. Модели воздействия внешнего злоумышленника на локальный сегмент компьютерной системы. / Ср /				
2.7	/ Зачёт /	7	0	ОПК-5, ОПК-10, ОПК-2.4	Л1.1, Л1.2, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.1	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	https://www.iprbookshop.ru/87995.html неограниченный доступ для зарегистрированных пользователей
Л1.2	Чекулаева Е. Н., Кубашева Е. С.	Управление информационной безопасностью: учебное пособие	Йошкар-Ола: Поволжский государственный технологический университет, 2020	https://biblioclub.ru/index.php?page=book&id=612591 неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1	Шейдаков Н. Е., Серпенинов О. В., Тищенко Е. Н.	Физические основы защиты информации: учеб. пособие для студентов высш. учеб. заведений, обучающихся по напр. подгот. "Информ. безопасность"	М.: РИО□, 2016	111
Л2.2	Рытенкова О.	Информационная безопасность: журнал	Москва: ГРОТЕК, 2013	https://biblioclub.ru/index.php?page=book&id=210607 неограниченный доступ для зарегистрированных пользователей
Л2.3	Катанова, Т. Н., Галкина, Л. С., Жданов, Р. А.	Информационная безопасность: лабораторный практикум	Пермь: Пермский государственный гуманитарно-педагогический университет, 2018	https://www.iprbookshop.ru/86357.html неограниченный доступ для зарегистрированных пользователей
Л2.4	Морозов, А. В., Филатова, Л. В., Полякова, Т. А.	Информационное право и информационная безопасность. Часть 2: учебник для магистров и аспирантов	Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016	https://www.iprbookshop.ru/66771.html неограниченный доступ для зарегистрированных пользователей
Л2.5	Морозов, А. В., Филатова, Л. В., Полякова, Т. А.	Информационное право и информационная безопасность. Часть 1: учебник для магистров и аспирантов	Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016	https://www.iprbookshop.ru/72395.html неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы
Информационная справочная система "КонсультантПлюс" База данных действующих стандартов по направлению "Информационная Безопасность" https://www.gost.ru/portal/gost/home/standarts/InformationSecurity Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России)//fstec.ru
5.4. Перечень программного обеспечения
Операционная система РЕД ОС LibreOffice
5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья
При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:
- столы, стулья;
- персональный компьютер / ноутбук (переносной);
- проектор;
- экран / интерактивная доска.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности			
З.состав и назначение нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации	объем и глубина изучения нормативных правовых актов, нормативных и методических документов по вопросам защиты информации	полнота и содержательность ответа, обоснованность выбора конкретного документа при ответах на вопросы опроса, на зачете	З (1-29) О (1-26)
У. применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в процессе управления информационной безопасностью	решение лабораторных заданий по управлению информационной безопасностью на базе требований нормативных правовых актов, нормативных и методических документов	правильность выполнения задания, обоснованность применения нормативных правовых актов, нормативных и методических документов	ПОЗЗ (1-4) ПЗ (1-4)
В. навыки внедрения требований нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации	навыки внедрения требований нормативных правовых актов, нормативных и методических документов в профессиональную деятельность	правильность выполнения задания по внедрению требований нормативных правовых актов, нормативных и методических документов в ходе выполнения практических заданий	ПОЗЗ (1-4) ПЗ (1-4)
ОПК-10: Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты			
З. основные методы и технологии формирования политики информационной безопасности	знает общие понятия о методах и технологиях формирования политики информационной безопасности	содержание основных методов и технологий формирования политики информационной безопасности	З (1-29) О (1-26)
У. оценивать эффективность реализации систем защиты информации и политик безопасности в компьютерных системах, организовывать реализацию мер в области информационной безопасности, формировать политику безопасности объектов защиты	практическая реализация политики безопасности в компьютерных системах, организация выполнения мер защиты в области информационной безопасности	правильность оценивания эффективности реализации систем защиты информации и политик безопасности в компьютерных системах, эффективность организации выполнения мер в области информационной безопасности при выполнении практических заданий	ПОЗЗ (1-4) ПЗ (1-4)
В. навыками разработки политики информационной безопасности объекта защиты, планировать, организовывать и выполнять комплекс мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	использование основных положений концепции построения систем управления информационной безопасностью при выполнении лабораторных заданий	умение самостоятельно находить решение поставленных задач информационной безопасности при выполнении практических заданий	ПОЗЗ (1-4) ПЗ (1-4)
ОПК-2.4: Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами			
З. требования нормативных документов по оценке защищенности объекта информатизации и правила проведения их аудита	знание требований нормативных документов по оценке защищенности объекта информатизации и правила проведения их аудита	полнота и содержательность ответа, обоснованность формирования набора требований по оценке защищенности	З (1-29) О (1-26)
У. организовывать подготовку и проведение аудита информационной безопасности объекта защиты, формировать отчетные материалы и обоснованные предложения по совершенствованию системы защиты информации	формирование отчетных материалов и обоснование предложений по совершенствованию системы защиты информации при выполнении практических заданий	правильность подготовки отчетных материалов и подготовки предложений по совершенствованию системы защиты информации при выполнении практических заданий	ПОЗЗ (1-4) ПЗ (1-4)
В. организовывать подготовку и проведение аудита информационной безопасности, навыками планирования и	проведение аудита информационной безопасности, формирование	правильность проведения аудита информационной безопасности, формирования отчетных материалов,	ПОЗЗ (1-4) ПЗ (1-4)

организации аудита объекта защиты, формирования отчетных материалов, работы по реализации предложений по совершенствованию системы защиты информации	отчетных материалов, подготовка предложений по совершенствованию системы защиты информации при выполнении лабораторных заданий	обоснованность предложений по совершенствованию системы защиты информации при выполнении лабораторных заданий	

З- вопросы к зачету, О – опрос, ПОЗЗ- практико-ориентированные задания к зачету, ПЗ- практические задания

1.2 Шкалы оценивания:
Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале:
50-100 баллов (зачет)
0-49 баллов (незачет)

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

Вопросы к зачету

1. Общие понятия управления информационной безопасностью
2. Цели управления информационной безопасностью объекта.
3. Задачи управления информационной безопасностью объекта информатизации.
4. Задачи управления информационной безопасностью организации.
5. Основные концепции построения систем управления информационной безопасностью.
6. Основные архитектуры построения систем управления информационной безопасностью.
7. Концепции глобального управления безопасностью.
8. Глобальная политика безопасности. Локальные политики безопасности.
9. Классификация основных средств защиты информации.
10. Назначение основных средств защиты информации на объекте.
11. Управление информационными ресурсами. Управление средствами защиты информации.
12. Управление средствами защиты от несанкционированного доступа.
13. Управление средствами защиты акустической информации.
14. Управление средствами защиты информации, обрабатываемой на ПЭВМ.
15. Аудит состояния информационной безопасности на объектах информатизации.
16. Методы экспертного анализа состояния информационной безопасности на объектах информатизации.
17. Расчетно-аналитические методы анализа состояния информационной безопасности на объектах информатизации.
18. Использование результатов аудита для повышения эффективности системы управления информационной безопасностью
19. Виды контроля состояния информационной безопасности объектов.
20. Межведомственный контроль состояния информационной безопасности объектов.
21. Ведомственный контроль состояния информационной безопасности объектов.
22. Объектовый мониторинг состояния информационной безопасности.
23. Формы представления результатов контроля информационной безопасности.
24. Методы оценки эффективности мероприятий информационной безопасности.
25. Экспертные методы оценки эффективности систем информационной безопасности.
26. Расчетно-аналитические методы оценки эффективности систем информационной безопасности.
27. Системы централизованного управления безопасностью.
28. Средства управления безопасностью локальных сетей.
29. Продукты для управления безопасностью кампании Cisco и IBM.

Практико-ориентированные задания к зачету

1. Виды контроля состояния информационной безопасности объектов. Межведомственный и ведомственный контроль состояния информационной безопасности объектов.

2. Объектовый мониторинг состояния информационной безопасности. Формы представления результатов контроля.

3. Методы оценки эффективности проводимых мероприятий. Экспертные методы оценки эффективности систем информационной безопасности. Расчетно-аналитические методы оценки эффективности систем информационной безопасности.

4. Системы централизованного управления безопасностью. Средства управления безопасностью локальных сетей. Продукты ведущих производителей для управления безопасностью.

Критерии оценивания:
- 50-100 баллов («зачет»): – изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленной программой курса целью обучения; правильные, уверенные действия по применению полученных навыков и умений при решении практико-ориентированного задания, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;
- 0-49 баллов («незачет») – ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять навыки и умения при решении практико-ориентированного задания, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Опрос

1. Основные понятия управления информационной безопасностью
2. Цели и задачи управления информационной безопасностью объекта.
3. Основные концепции построения систем управления информационной безопасностью.
4. Основные архитектуры построения систем управления информационной безопасностью.
5. Концепции глобального управления безопасностью.
6. Глобальная политика безопасности. Локальные политики безопасности.
7. Классификация основных средств защиты информации.
8. Назначение основных средств защиты информации на объекте.
9. Управление информационными ресурсами. Управление средствами защиты информации.
10. Управление средствами защиты от несанкционированного доступа.
11. Управление средствами защиты акустической информации.
12. Управление средствами защиты информации, обрабатываемой на ПЭВМ.
13. Аудит состояния информационной безопасности на объектах информатизации.
14. Методы экспертного анализа состояния информационной безопасности на объектах информатизации.
15. Расчетно-аналитические методы анализа состояния информационной безопасности на объектах информатизации.
16. Использование результатов аудита для повышения эффективности системы управления информационной безопасностью
17. Виды контроля состояния информационной безопасности объектов.
18. Межведомственный контроль состояния информационной безопасности объектов.
19. Ведомственный контроль состояния информационной безопасности объектов.
20. Объектовый мониторинг состояния информационной безопасности.
21. Формы представления результатов контроля информационной безопасности.
22. Методы оценки эффективности мероприятий информационной безопасности.
23. Экспертные методы оценки эффективности систем информационной безопасности.
24. Расчетно-аналитические методы оценки эффективности систем информационной безопасности.

25. Системы централизованного управления безопасностью.
26. Средства управления безопасностью локальных сетей.

Критерии оценивания:

- 2 балла выставляется обучающемуся, если изложенный материал фактически верен и логически обоснован.
- 0-1 баллов, если ответ неверный или имеет неточности.

Максимальное количество баллов за семестр: 40 баллов.

Практические задания
по дисциплине Основы управления информационной безопасностью

Практическое задание №1 (15 баллов)
Управление информационной безопасностью объекта информатизации.

Практическое задание №2 (15 баллов)
Управление средствами защиты информации на объекте.

Практическое задание №3 (15 баллов)
Контроль и аудит состояния информационной безопасности на объектах информатизации. Мониторинг состояния информационной безопасности. Формы представления результатов контроля.

Практическое задание №4 (15 баллов)
Оценка эффективности проводимых мероприятий по совершенствованию системы управления информационной безопасностью. Экспертные методы оценки эффективности систем информационной безопасности. Расчетно-аналитические методы оценки эффективности систем информационной безопасности.

Критерии оценивания:
- (для каждого задания):
15 б. – задание выполнено верно;
14-10 б. – при выполнении задания были допущены неточности, не влияющие на результат;
9-6 б. – при выполнении задания были допущены ошибки;
5 - 1 б. – при выполнении задания были допущены существенные ошибки;
0 б. – задание не выполнено.
Максимальное количество баллов, которые могут быть получены обучающимся в течение семестра - 60

3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.
Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме зачета.
Зачет проводится по окончании теоретического обучения до начала экзаменационной сессии. Количество вопросов в билете – 3. Проверка ответов и объявление результатов производится в день зачета. Результаты аттестации заносятся в экзаменационную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:
- лекции;
- практические занятия.

В ходе лекционных занятий рассматриваются теоретические вопросы с учетом практико-ориентированности изучаемой дисциплины, даются рекомендации для самостоятельной работы и подготовке к лабораторным занятиям.

В ходе практических занятий углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки работы с компьютером, применения методов и технологий защиты информации.

При подготовке к практическим занятиям каждый обучающийся должен:
– изучить рекомендованную учебную литературу;
– изучить практические примеры, рассмотренные на лекциях;
– подготовить ответы на все вопросы по изучаемой теме.

В процессе подготовки к практическим занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на лекциях, лабораторных занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий методом опроса и посредством выполнения практических заданий. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных первоисточников. Выделить непонятные термины, найти их значение в энциклопедических словарях.

Студент должен готовиться к предстоящему практическому занятию по всем, обозначенным в рабочей программе дисциплины вопросам.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.