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

УТВЕРЖДАЮ
Начальник отдела лицензирования и аккредитации
_____Чаленко К.Н.
«____» _____ 20___г.

Рабочая программа дисциплины
Основы информационной безопасности

38.03.01 Экономика
38.03.01.04 "Мировая экономика"

Для набора 2023 года

Квалификация
Бакалавр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**5 (3.1)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	4	4	4	4
Лабораторные	4	4	4	4
Итого ауд.	8	8	8	8
Контактная работа	8	8	8	8
Сам. работа	96	96	96	96
Часы на контроль	4	4	4	4
Итого	108	108	108	108

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 27.06.2023 протокол № 12.

Программу составил(и): к.т.н., доцент, Севастьянов И.Т. _____

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

Методическим советом направления: д.э.н., профессор, Е.Н. Тищенко _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	приобретение знаний по правовой защите коммерческой, служебной, профессиональной тайны, персональных данных; приобретение знаний по организационно-правовым основам защиты экономической информации; развитие умений и формирование практических навыков организации процесса сбора, анализа и систематизации информации по формированию системы защиты экономической информации; приобретение умений и навыков по организации контроля за состоянием защиты конфиденциальной информации в организации.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-5:Способен использовать современные информационные технологии и программные средства при решении профессиональных задач.

ОПК-6:Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

В результате освоения дисциплины обучающийся должен:

Знать:

цели, задачи и процессы поиска и анализа источников информации для проведения финансово-экономических расчетов при построении системы защиты информации;
способы организации процесса сбора,анализа и систематизации информации по формированию системы защиты информации в организациях с различными формами собственности.

Уметь:

разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации на основе анализа нормативно-правовых актов в области информационной безопасности;
анализировать эффективность систем организационной защиты информации и определять направления ее совершенствования.

Владеть:

способностью по разработке комплекса организационно--технических мер по обеспечению информационной безопасности объекта защиты;
методологией организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами ФСТЭК России и ФСБ России.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература
	Раздел 1. Правовое и организационное обеспечение информационной безопасности				
1.1	Тема 1."Правовое обеспечение информационной безопасности в системе национальной безопасности РФ". Основные направления обеспечения информационной безопасности и защиты информации в РФ. /Лек/	5	2	ОПК-5 ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
1.2	Тема 1."Правовое обеспечение информационной безопасности в системе национальной безопасности РФ". Организация работы со сведениями, отнесенными к государственной тайне и конфиденциальной информации. Использовать Libreoffice. /Ср/	5	12	ОПК-5 ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
1.3	Тема 1."Правовое обеспечение информационной безопасности в системе национальной безопасности РФ". Юридическая ответственность за нарушение законодательства в области защиты информации. /Ср/	5	12	ОПК-5 ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
	Раздел 2. Основы защиты коммерческой тайны и конфиденциальной информации				
2.1	Тема 1. «Правовые основы защиты коммерческой тайны». Порядок отнесения информации к коммерческой тайне. Права обладателя коммерческой тайны. Использовать Libreoffice. /Ср/	5	16	ОПК-5 ОПК-6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4

2.2	Тема 2. «Правовые основы защиты конфиденциальной информации». Разработка политики безопасности предприятия. /Лаб/	5	2	ОПК-5 ОПК -6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
2.3	Тема 2. «Правовые основы защиты конфиденциальной информации». Права и обязанности работника и работодателя по защите конфиденциальной информации. /Ср/	5	12	ОПК-5 ОПК -6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
	Раздел 3. Правовые основы защиты персональных данных				
3.1	Тема 1. «Обработка и защита персональных данных». Права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные. /Лек/	5	2	ОПК-5 ОПК -6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
3.2	Тема 1. «Обработка и защита персональных данных». Требования нормативно-правовых актов по организации и обработка персональных данных. /Ср/	5	10	ОПК-5 ОПК -6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
	Раздел 4. Организация контроля за состоянием защиты конфиденциальной информации на предприятии				
4.1	Тема 1. «Деятельность руководства и должностных лиц по проверке состояния защиты конфиденциальной информации». Организация аудита информационной безопасности предприятия. /Лаб/	5	2	ОПК-5 ОПК -6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
4.2	Тема 1. «Деятельность руководства и должностных лиц по проверке состояния защиты конфиденциальной информации». Основные этапы аналитической работы. Содержание и основные виды аналитических отчетов. /Ср/	5	18	ОПК-5 ОПК -6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
	Раздел 5. Конфиденциальное делопроизводство и документооборот в организации				
5.1	Тема 1. «Организация конфиденциального делопроизводства и документооборота в организации». Построение системы защищенного электронного документооборота. /Ср/	5	16	ОПК-5 ОПК -6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
5.2	/Зачёт/	5	4	ОПК-5 ОПК -6	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4

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, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Руденков Н. А., Пролетарский А. В., Смирнова Е. В., Суровов А. М.	Технологии защиты информации в компьютерных сетях	Москва: Национальный Открытый Университет «ИНТУИТ», 2016	https://biblioclub.ru/index.php?page=book&id=428820 неограниченный доступ для зарегистрированных пользователей

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.2	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	http://www.iprbookshop.ru/87995.html неограниченный доступ для зарегистрированных пользователей
Л1.3	Кубашева Е. С., Малашкевич И. А., Чекулаева Е. Н.	Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: учебно-методическое пособие к прохождению производственной практики: учебно-методическое пособие	Йошкар-Ола: Поволжский государственный технологический университет, 2019	https://biblioclub.ru/index.php?page=book&id=562246 неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Тищенко Е. Н.	Инструментальные методы анализа потребительского качества защищенных информационных систем: учеб. пособие	Ростов н/Д: Изд-во РГЭУ (РИНХ), 2016	68
Л2.2	Братановский С. Н.	Специальные правовые режимы информации: монография	Москва: Директ-Медиа, 2012	https://biblioclub.ru/index.php?page=book&id=131866 неограниченный доступ для зарегистрированных пользователей
Л2.3	Заляжных, В. А., Гирик, А. В.	Экспертные системы комплексной оценки безопасности автоматизированных информационных и коммуникационных систем	Санкт-Петербург: Университет ИТМО, 2014	http://www.iprbookshop.ru/65733.html неограниченный доступ для зарегистрированных пользователей
Л2.4		БИТ. Бизнес & Информационные технологии: журнал	Москва: Положевец и партнеры, 2019	https://biblioclub.ru/index.php?page=book&id=562409 неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

ЭБС "IPR Books" http://www.iprbookshop.ru/

ФСТЭК России/fstec.ru

http://biblioclub.ru/

5.4. Перечень программного обеспечения

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 (МОДУЛЯ)

Помещения для проведения всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения. Для проведения лекционных занятий используется демонстрационное оборудование. Практические занятия проводится в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными программными средствами и выходом в Интернет.

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

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 использовать современные информационные технологии и программные средства при решении профессиональных задач.			
З: - цели, задачи и процессы поиска и анализа источников информации для проведения финансово-экономических расчетов при построении системы защиты информации.	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов.	полнота собранной информации по анализу опасных ситуаций.	О (вопросы 1-29) З (вопросы1-29)
У: разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации на основе анализа нормативно-правовых актов в области информационной безопасности.	использование информационных технологий в практической деятельности при оформлении необходимых нормативно-правовых документов.	правильность оформления нормативно-правовых документов по регламентации системы организационной защиты информации	ЛЗ (раздел 2, тема 2, лабораторное задание)
В: способностью по разработке комплекса организационно--технических мер по обеспечению информационной безопасности объекта защиты.	использование современных информационно-коммуникационных технологий и различных информационных ресурсов	полнота и содержательность ответа, умение самостоятельно находить решение поставленных задач	ЛЗ (раздел 2, тема 2, лабораторное задание)
ОПК-6: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности			

З: способы организации процесса сбора, анализа и систематизации информации по формированию системы защиты информации в организациях с различными формами собственности.	знание способов решения стандартных задач профессиональной деятельности в области информационной безопасности при формировании системы защиты информации с применением современных информационных технологий.	полнота и содержательность предлагаемых способов оценивания защищенности информации на объектах информатизации	О (вопросы 30-54) З (вопросы30-54)
У: анализировать эффективность систем организационной защиты информации и определять направления ее совершенствования.	решение лабораторных заданий в области системы защиты информации, выявление ее уязвимых мест и определение направления ее совершенствования с применением современных информационных технологий.	полнота решения, соответствие результатов текущему состоянию системы защиты информации.	ЛЗ (раздел 4, тема 1, лабораторное задание)
В: методологией организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами ФСТЭК России и ФСБ России.	использование методов и средств защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами с применением современных информационных технологий.	полнота оценивания комплекса организационно-технических мер по обеспечению информационной безопасности и качества функционирования объекта информатизации.	ЛЗ (раздел 4, тема 1, лабораторное задание)

О – опрос; ЛЗ – лабораторные задания; З – вопросы к зачету

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

В разделе приводятся типовые варианты оценочных средств: вопросы к зачету, практические задания.

Вопросы к зачету
по дисциплине Основы информационной безопасности

1. Информация как объект правового регулирования.
2. Структура законодательства РФ в области информационной безопасности и защиты информации.
3. Основные цели и методы обеспечения ИБ РФ. Источники и виды угроз ИБ РФ.
4. Основные направления обеспечения информационной безопасности и защиты информации в РФ.
5. Структура организационной защиты информации.
6. Виды информации, защищаемой законодательством РФ.
7. Перечень сведения конфиденциального характера.
8. Организация работы со сведениями, отнесенные к конфиденциальной информации.
9. Правовой режим защиты конфиденциальной информации.
10. Угрозы утечки информации по техническим каналам.
11. Классификация технических каналов утечки информации.
12. Технические мероприятия по защите информации от утечки по техническим каналам.
13. Организационные мероприятия по защите информации от утечки по техническим каналам.
14. Классификации угроз безопасности информации в информационных системах.
15. Требования к организации защиты информации в информационной системе.
16. Формирование требований к защите информации в информационной системе.
17. Определение класса защищенности информационной системы.
18. Порядок отнесения информации к информации, составляющей коммерческую тайну, и ее предоставление.
19. Понятие коммерческой тайны. Правовое обеспечение защиты коммерческой тайны.
20. Сведения, составляющие коммерческую тайну. Сведения, которые не могут составлять коммерческую тайну.
21. Права обладателя коммерческой тайны.
22. Организация защиты информации на предприятии.
23. Обеспечение сохранности документов, дел и изданий.
24. Обязанности лиц, допущенных к сведениям, составляющих коммерческую тайну.
25. Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну.
26. Обязанности персонала организации по сохранению коммерческой тайны.
27. Политика безопасности предприятия как основа организационного управления защитой информации.
28. Права и обязанности работника и работодателя по защите конфиденциальной информации.
29. Ответственность за нарушение конфиденциальности информации.
30. Права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные.
31. Организация защиты персональных данных в организации.
32. Планирование мероприятий по организационной защите информации на предприятии.
33. Структура и основное содержание плана мероприятий по защите конфиденциальной информации.

34. Организация аналитической работы в области защиты информации на предприятии.
35. Основные объекты и формы контроля за состоянием защиты информации.
36. Основные задачи и методы контроля.
37. Основные направления аналитической работы.
38. Организация аудита информационной безопасности предприятия.
39. Функции аналитического подразделения в области защиты информации на предприятии.
40. Основные этапы аналитической работы в области защиты информации на предприятии.
41. Содержание и основные виды аналитических отчетов.
42. Классификация методов анализа информации.
43. Компьютерные преступления в электронной коммерции.
44. Информационная безопасность в электронной коммерции.
45. Юридическая ответственность за нарушение правовых норм защиты информации.
46. Обосновать основные направления обеспечения информационной безопасности и защиты информации в РФ.
47. Сформулировать технические и организационные мероприятия по защите информации от утечки по техническим каналам.
48. Разработка требований к мерам защиты информации, содержащейся в информационной системе.
49. Правовое обеспечение защиты коммерческой тайны на предприятии.
50. Разработка политики безопасности предприятия.
51. Определение прав и обязанностей оператора, обрабатывающего персональные данные.
52. Определение уровня защищенности ИСПДн.
53. Определить основные объекты и формы контроля за состоянием защиты информации.
54. Сформулировать основные задачи и методы контроля.

Критерии оценивания:
50-100 баллов (зачет) – изложенный материал верен, наличие знаний в объёме пройденной программы дисциплины в соответствии с постановлеbнными программой курса целями и задачами обучения; правильные действия по применению полученных знаний на практике, 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 знания на практике, неточность ответов на дополнительные вопросы.

Содержание опроса:

1. Информация как объект правового регулирования.
2. Структура законодательства РФ в области информационной безопасности и защиты информации.
3. Основные цели и методы обеспечения ИБ РФ. Источники и виды угроз ИБ РФ.
4. Основные направления обеспечения информационной безопасности и защиты информации в РФ.
5. Структура организационной защиты информации.
6. Виды информации, защищаемой законодательством РФ.
7. Перечень сведения конфиденциального характера.
8. Организация работы со сведениями, отнесенные к конфиденциальной информации.
9. Правовой режим защиты конфиденциальной информации.
10. Угрозы утечки информации по техническим каналам.
11. Классификация технических каналов утечки информации.
12. Технические мероприятия по защите информации от утечки по техническим каналам.
13. Организационные мероприятия по защите информации от утечки по техническим каналам.

14. Классификации угроз безопасности информации в информационных системах.
15. Требования к организации защиты информации в информационной системе.
16. Формирование требований к защите информации в информационной системе.
17. Определение класса защищенности информационной системы.
18. Порядок отнесения информации к информации, составляющей коммерческую тайну, и ее предоставление.
19. Понятие коммерческой тайны. Правовое обеспечение защиты коммерческой тайны.
20. Сведения, составляющие коммерческую тайну. Сведения, которые не могут составлять коммерческую тайну.
21. Права обладателя коммерческой тайны.
22. Организация защиты информации на предприятии.
23. Обеспечение сохранности документов, дел и изданий.
24. Обязанности лиц, допущенных к сведениям, составляющих коммерческую тайну.
25. Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну.
26. Обязанности персонала организации по сохранению коммерческой тайны.
27. Политика безопасности предприятия как основа организационного управления защитой информации.
28. Права и обязанности работника и работодателя по защите конфиденциальной информации.
29. Ответственность за нарушение конфиденциальности информации.
30. Права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные.
31. Организация защиты персональных данных в организации.
32. Планирование мероприятий по организационной защите информации на предприятии.
33. Структура и основное содержание плана мероприятий по защите конфиденциальной информации.
34. Организация аналитической работы в области защиты информации на предприятии.
35. Основные объекты и формы контроля за состоянием защиты информации.
36. Основные задачи и методы контроля.
37. Основные направления аналитической работы.
38. Организация аудита информационной безопасности предприятия.
39. Функции аналитического подразделения в области защиты информации на предприятии.
40. Основные этапы аналитической работы в области защиты информации на предприятии.
41. Содержание и основные виды аналитических отчетов.
42. Классификация методов анализа информации.
43. Компьютерные преступления в электронной коммерции.
44. Информационная безопасность в электронной коммерции.
45. Юридическая ответственность за нарушение правовых норм защиты информации.
46. Обосновать основные направления обеспечения информационной безопасности и защиты информации в РФ.
47. Сформулировать технические и организационные мероприятия по защите информации от утечки по техническим каналам.
48. Разработка требований к мерам защиты информации, содержащейся в информационной системе.
49. Правовое обеспечение защиты коммерческой тайны на предприятии.
50. Разработка политики безопасности предприятия.
51. Определение прав и обязанностей оператора, обрабатывающего персональные данные.
52. Определение уровня защищенности ИСПДн.
53. Определить основные объекты и формы контроля за состоянием защиты информации.
54. Сформулировать основные задачи и методы контроля

Критерии оценивания:

Оценка качества знаний в течении семестра проводится путем анализа качества ответов по 20 вопросам, выбранных из перечня вопросов:
правильный ответ на 1 вопрос – 1 балл;
неправильный ответ на 1 вопрос – 0 баллов.
Количество баллов за семестр – 20 баллов.

Лабораторные задания

1.Тематика лабораторных заданий по разделам и темам
Раздел 2. Основы защиты коммерческой тайны и конфиденциальной информации
Тема 2. «Правовые основы защиты конфиденциальной информации».
Лабораторная работа. Разработка политики безопасности предприятия. Оформление работы в Libreoffice.
Раздел 4. Организация контроля за состоянием защиты конфиденциальной информации на предприятии
Тема 1. «Деятельность руководства и должностных лиц по проверке состояния защиты конфиденциальной информации».
Лабораторная работа. Организация аудита информационной безопасности предприятия. Оформление работы в Libreoffice.

Критерии оценивания:

Правильное выполнение каждого лабораторного задания – 40 баллов.
Неправильное решение практического задания – 0 баллов.
Количество баллов за семестр – 80 баллов.

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 расписанию промежуточной аттестации в письменном виде. Количество вопросов в задании – 2. Проверка ответов и объявление результатов производится в день зачета. Результаты аттестации заносятся в 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;
- лабораторные занятия.

В ходе лекционных занятий рассматриваются основные понятия в области информационной безопасности и защиты информации, методы обнаружения и организации противодействия атак на информационные сети, требования по защите конфиденциальной информации,даются рекомендации для самостоятельной работы и подготовке к лабораторным занятиям.

В ходе лабораторных занятий углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки решения задач по защите информационных объектов.

При подготовке к лабораторным занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- ознакомиться с описанием лабораторной работы;
- подготовить ответы на контрольные вопросы по изучаемой теме.

В процессе подготовки к лабораторным занятиям студенты могут воспользоваться консультациями преподавателя. При оформлении отчетов по выполненным лабораторным работам использовать программное обеспечение Libreoffice: шрифт Times New Roman; размер шрифта -12; междустрочный интервал – одинарный: отступ – 1,25.

Вопросы, не рассмотренные на лекциях и лабораторных занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой дисциплины осуществляется в ходе занятий методом опроса. 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 источников.Выделить непонятные термины и найти их значение в энциклопедических словарях.

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.