МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета _____ Бурковский А.В.

31 08 2018г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Информационная безопасность и защита информации»

Направление подготовки 27.03.04 Управление в технических системах

Профиль Управление и информатика в технических системах

Квалификация выпускника бакалавр

Нормативный период обучения 4 года

Форма обучения очная

Год начала подготовки 2021

Автор программы _____ /Васильев Е.М./

Заведующий кафедрой
Электропривода,
автоматики и управления в
технических системах _____ /Бурковский В.Л/

Руководитель ОПОП _____ /Мурзинов Ю.В./

Воронеж 2021

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

- формирование у студентов способности понимать сущность и значения информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны.

1.2. Задачи освоения дисциплины

изучение доктрины информационной безопасности Российской Федерации, структуры государственной системы информационной безопасности;

ознакомление с законодательной базой по вопросам информационной безопасности и соответствующими нормативными документами;

владение криптографическими методами защиты информации;

приобретение навыков защиты информации криптографическими средствами.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Информационная безопасность и защита информации» относится к дисциплинам части, формируемой участниками образовательных отношений блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Информационная безопасность и защита информации» направлен на формирование следующих компетенций:

ПК-2 - Способен осуществлять разработку методического обеспечения автоматизированных систем управления производством, планирование предварительных испытаний автоматизированных систем.

ПК-5 - Способен к разработке отдельных разделов проекта на различных стадиях проектирования автоматизированных систем управления технологическими процессами

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-2	Знать методическое обеспечение автоматизированных систем управления производством
	Уметь осуществлять планирование предварительных испытаний автоматизированных систем
	Владеть способностью разрабатывать методику обеспечения автоматизированными системами управления производств
ПК-5	Знать отдельные разделы проекта автоматизированных систем управления технологическими процессами
	Уметь разрабатывать проект на различных стадиях

	Владеть способностью разрабатывать проект автоматизированных систем управления технологическими процессами

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Информационная безопасность и защита информации» составляет 3 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		2
Аудиторные занятия (всего)	72	72
В том числе:		
Лекции	18	18
Практические занятия (ПЗ)	18	18
Лабораторные работы (ЛР)	36	36
Самостоятельная работа	36	36
Курсовая работа	+	+
Виды промежуточной аттестации - зачет	+	+
Общая трудоемкость: академические часы зач.ед.	 108 3	 108 3

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	Лаб. зан.	СРС	Всего, час
1	Введение	Основные понятия об информационной безопасности и защите информации. Доктрина информационной безопасности Российской Федерации. Структура государственной системы информационной безопасности	4	2	6	6	18
2	Государственные стандарты РФ в области защиты информации	Государственные стандарты РФ в области защиты информации	4	2	6	6	18
3	Архитектура криптографических систем защиты информации	Основные понятия и определения криптографии стоинства и недостатки. Протоколы передачи данных в симметричных и несимметричных системах передачи данных	4	2	6	6	18
4	Криптографические алгоритмы	Структура законодательной базы по вопросам информационной безопасности. Способы защиты информации.	2	4	6	6	18
5	Протоколы цифровой подписи и разделения ключа.	Шифры одноалфавитной и многоалфавитной замены. Анализ стойкости этих шифров. Абсолютно стойкий шифр замены.	2	4	6	6	18
6	Шифры перестановок	Шифры перестановок. Достоинства и недостатки этих шифров. Методы генерации случайных ключей.	2	4	6	6	18

		Способы проверки статистической независимости элементов ключа.					
		Итого	**18**	**18**	**36**	**36**	**108**

5.2 Перечень лабораторных работ

1. Шифры замены и криптоанализ зашифрованных сообщений
2. Программирование криптографических алгоритмов перестановок
3. Шифрование на основе однонаправленных функций
4. Генерирование криптографических ключей

5.3. Практические занятия

1. Криптографические системы
2. Криптографические протоколы
3. Шифры замены
4. Многоалфавитные шифры замены
5. Шифры перестановок
6. Шифры на основе односторонних функций

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсовой работы в 2 семестре для очной формы обучения.

Примерные темы курсовых работ:

1. • Разработка критерия криптографической стойкости шифров перестановок.
2. Анализ стойкости криптографического протокола голосования.
3. Разработка криптографического алгоритма порогового разделения секрета.
4. Анализ стойкости криптографического протокола цифровой подписи.
5. Разработка криптографического алгоритма многоалфавитной замены.
6. Разработка криптографического алгоритма маршрутной перестановки.
7. Исследование алгоритмов генерации случайных ключей.
8. Анализ криптографической системы без передачи ключей.
9. Разработка абсолютно стойкого шифра замены.

Курсовая работа включат в себя графическую часть и расчетно-пояснительную записку.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

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

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации

оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-2	Знать методическое обеспечение автоматизированных систем управления производством	Работа на лекциях, ответы на теоретические вопросы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь осуществлять планирование предварительных испытаний автоматизированных систем	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть способностью разрабатывать методику обеспечения автоматизированными системами управления производств	Решение прикладных задач в конкретной предметной области,	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-5	Знать отдельные разделы проекта автоматизированных систем управления технологическими процессами	Работа на лекциях, ответы на теоретические вопросы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь разрабатывать проект на различных стадиях	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть способностью разрабатывать проект автоматизированных систем управления технологическими процессами	Решение прикладных задач в конкретной предметной области,	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 2 семестре для очной формы обучения по двухбалльной системе:

«зачтено»

«не зачтено»

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
ПК-2	Знать методическое обеспечение автоматизированных систем управления производством	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	Уметь осуществлять планирование предварительных испытаний автоматизированных систем	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

	Владеть способностью разрабатывать методику обеспечения автоматизированными системами управления производств	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-5	Знать отдельные разделы проекта автоматизированных систем управления технологическими процессами	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	Уметь разрабатывать проект на различных стадиях	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	Владеть способностью разрабатывать проект автоматизированных систем управления технологическими процессами	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Основные понятия об информационной безопасности и защите информации. Доктрина информационной безопасности Российской Федерации.
2. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности.
3. Способы защиты информации. Государственные стандарты РФ в области защиты информации.
4. Основные понятия и определения криптографии.
5. Системы с открытым и закрытым ключом. Порядок их функционирования. Достоинства и недостатки.
6. Протоколы передачи данных в симметричных и несимметричных системах передачи данных.
7. Протоколы цифровой подписи и разделения ключа. Области применения этих протоколов
8. Протоколы электронных платежей.
9. Протоколы голосования.
10. Протоколы обмена без передачи ключей.
11. Шифры одноалфавитной и многоалфавитной замены. Анализ стойкости этих шифров.
12. Абсолютно стойкий шифр замены.
13. Шифры перестановок. Достоинства и недостатки этих шифров.
14. Методы генерации случайных ключей. Способы проверки статистической независимости элементов ключа.

15. Криптографические алгоритмы на основе односторонних функций.

7.2.2 Примерный перечень заданий для решения стандартных задач

1.Что такое информационная безопасность:

а) действия по обеспечению информационной безопасности;
б) состояние защищённости в информационной сфере;
в) ограничение доступа к информации посторонним лицам;
г) скрытность хранения и передачи информации.

2. Что относится к защите информации?

а) действия по обеспечению информационной безопасности;
б) состояние защищённости;
в) ограничение доступа к информации посторонним лицам;
г) скрытность хранения и передачи информации.

3. Расположите способы защиты информации в порядке возрастания их стойкости:

а) скрытие факта передачи информации ;
б) ограничение доступа к носителю информации;
в) шифрование информации.
г) кодирование информации.

4. Что такое криптография?

а) способ кодирования сообщения;
б) способ шифрования сообщения;
в) способ передачи сообщения.

5. Что является количественной мерой стойкости шифра?

а) количество возможных вариантов ключа;
б) продолжительность времени, необходимого для перебора всех вариантов ключа ;
в) степень неизвестности принципа шифрования;
г) степень неизвестности протокола передачи информации

6. Что характерно для криптографической системы с закрытым ключом:

а) закрытый канал передачи информации;
б) закрытый канал для передачи ключа;
в) закрытый способ шифрования;
г) закрытый ключ.

7. Что характерно для криптографической системы с открытым ключом:

а) открытый канал передачи информации;
б) открытый канал для передачи ключа;
в) открытый способ шифрования;
г) открытый ключ.

8. Какую систему передачи информации использует протокол цифровой подписи:

а) систему с открытым ключом;
б) систему с закрытым ключом;
в) система с разделением секрета;
г) система анонимной передачи данных.

9. Количество вариантов ключа длиной 5 в шифре много алфавитной замены для сообщения, содержащего 10 символов:

а) 5

б) 10^5
в) 5*10;
г) (10-5)!

10. Количество вариантов ключа в шифре замены для алфавита мощностью 10 символов:
а) 10;
б) 10!;
в) 9;
г) (10-1)!

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Что характерно для криптографической системы с закрытым ключом:
а) закрытый канал передачи информации;
б) закрытый канал для передачи ключа;
в) закрытый способ шифрования;
г) закрытый ключ.

2. Что характерно для криптографической системы с открытым ключом:
а) открытый канал передачи информации;
б) открытый канал для передачи ключа;
в) открытый способ шифрования;
г) открытый ключ.

3. Какую систему передачи информации использует протокол цифровой подписи:
а) систему с открытым ключом;
б) систему с закрытым ключом;
в) система с разделением секрета;
г) система анонимной передачи данных.

4. Количество вариантов ключа длиной 5 в шифре многоалфавитной замены для сообщения,
содержащего
10 символов:
а) 5
б) 10^5
в) 5*10;
г) (10-5)!

5. Количество вариантов ключа в шифре замены для алфавита мощностью 10 символов:
а) 10;
б) 10!;
в) 9;
г) (10-1)!

7.2.4 Примерный перечень вопросов для подготовки к зачету

1. Основные понятия об информационной безопасности и защите информации. Доктрина информационной безопасности Российской Федерации.
2. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности.

3. Способы защиты информации. Государственные стандарты РФ в области защиты информации.
4. Основные понятия и определения криптографии.
5. Системы с открытым и закрытым ключом. Порядок их функционирования. Достоинства и недостатки.
6. Протоколы передачи данных в симметричных и несимметричных системах передачи данных.
7. Протоколы цифровой подписи и разделения ключа. Области применения этих протоколов
8. Протоколы электронных платежей.
9. Протоколы голосования.
10. Протоколы обмена без передачи ключей.
11. Шифры одноалфавитной и многоалфавитной замены. Анализ стойкости этих шифров.
12. Абсолютно стойкий шифр замены.
13. Шифры перестановок. Достоинства и недостатки этих шифров.
14. Методы генерации случайных ключей. Способы проверки статистической независимости элементов ключа.
15. Криптографические алгоритмы на основе односторонних функций.

7.2.5 Примерный перечень заданий для решения прикладных задач

Не предусмотрено учебным планом

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Например: Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Основные понятия об информационной безопасности и защите информации. Доктрина информационной безопасности Российской Федерации. Структура	ПК-2, ПК-5	Тесты, проверочные задания

	государственной системы информационной безопасности		
2	Государственные стандарты РФ в области защиты информации	ПК-2, ПК-5	Тесты, проверочные задания
3	Основные понятия и определения криптографии стоинства и недостатки. Протоколы передачи данных в симметричных и несимметричных системах передачи данных	ПК-2, ПК-5	Тесты, проверочные задания
4	Структура законодательной базы по вопросам информационной безопасности. Способы защиты информации.	ПК-2, ПК-5	Тесты, проверочные задания
5	Шифры одноалфавитной и многоалфавитной замены. Анализ стойкости этих шифров. Абсолютно стойкий шифр замены.	ПК-2, ПК-5	Тесты, проверочные задания
6	Шифры перестановок. Достоинства и недостатки этих шифров. Методы генерации случайных ключей. Способы проверки статистической независимости элементов ключа.	ПК-2, ПК-5	Тесты, проверочные задания

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Защита курсовой работы, курсового проекта или отчета по всем видам практик осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

1. Радько Н.М. Защита информации в беспроводных сетях [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (835 072 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2010

2. Кольцов А.С. Информационная безопасность и защита информации [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (4,5 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2013.

3. Матвеев Б.В Защита информации в телекоммукационных системах : учеб. пособие. - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2007. - 282 с.
4. Радько Н.М. Защита информации в беспроводных сетях [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (835 072 байт). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2010
5. Чопоров О.Н. Защита информации и информационная безопасность [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (1,8 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2012.
6. Матвеев Б.В Защита информации в каналах связи : Лабораторный практикум: Учеб. пособие. - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2008. - 249 с.
7. Паринов А.В. Информационная безопасность и защита информации [Электронный ресурс] : Учеб. пособие. - Электрон. дан. (1 файл : 811 Кб). - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2007.
8. Паринов А.В. Информационная безопасность и защита информации : Учеб. пособие. - Воронеж : ГОУВПО "Воронежский государственный технический университет", 2009. - 113 с.
9. Алексеев В.А. Методы и средства криптографической защиты информации [Электронный ресурс]: методические указания к проведению лабораторных работ по курсу «Методы и средства защиты компьютерной информации»/ Алексеев В.А.— Электрон. текстовые данные.— Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2009.— 16 с.— Режим доступа: http://www.iprbookshop.ru/17710.html.— ЭБС «IPRbooks»
10. Качановский Ю.П. Основные технические, программные и организационные меры защиты информации при работе с компьютерными системами [Электронный ресурс] : методические указания к проведению лабораторной работы по курсу «Информатика»/ Качановский Ю.П., Широков А.С.— Электрон. текстовые данные.— Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2014.— 24 с.— Режим доступа: http://www.iprbookshop.ru/55120.html.— ЭБС «IPRbooks»

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Лицензионное программное обеспечение

MicrosoftOfficeWord 2013/2007 MicrosoftOfficeExcel 2013/2007 MicrosoftOfficePowerPoint 2013/2007 MatLab
Windows Professional 8.1 (7 и 8) Single Upgrade MVL A Each Academic

Свободное ПО

OpenOffice Mozilla Firefox Zip

Ресурсы информационно-телекоммуникационной сети «Интернет»

http: //www.edu.ru/
Образовательный портал ВГТУ https: //electrono .ru
https: //www.tehnari .ru/
https://ieeexplore.ieee.org/Xplore/home.jsp https: //www.sql.ru/

Информационные справочные системы

http://window.edu.ru https: //wiki .cchgeu.ru/

Современные профессиональные базы данных База данных zbMath

Адрес ресурса: https://lib.tusur.ru/ru/resursy/bazy-dannyh/zbmath **Association for Computing Machinery, ACM** Адрес ресурса: https://dl.acm.org/contents_dl.cfm **Единый портал инноваций и уникальных изобретений** Адрес ресурса: http://innovationportal.ru/

Инновации в России

Адрес ресурса: http://innovation.gov.ru/

Росстандарт. Федеральное агентство по техническому регулированию и метрологии

Адрес ресурса: https://www.gost.ru/portal/gost/

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Дисплейный класс, оснащенный компьютерами с доступом в Интернет и программным обеспечением, необходимым для выполнения заданий и лабораторных работ

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

По дисциплине «Информационная безопасность и защита информации» читаются лекции, проводятся практические занятия и лабораторные работы, выполняется курсовая работа.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Практические занятия направлены на приобретение практических навыков логического синтеза. Занятия проводятся путем решения конкретных задач в аудитории.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Методика выполнения курсовой работы изложена в учебно-методическом пособии. Выполнять этапы курсовой работы должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсовой работы, защитой курсовой работы.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь.

	Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом три дня эффективнее всего использовать для повторения и систематизации материала.