

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ  
ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета  С.М. Пасмурнов  
«31» августа 2017 г.

**РАБОЧАЯ ПРОГРАММА**  
дисциплины

«Социальные сети: риски и обеспечение безопасности»

Специальность 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ  
АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2016

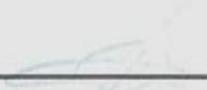
Автор программы

 /Паринова Л.В./

Заведующий кафедрой  
Систем информационной  
безопасности

  
/ А.Г. Остапенко /

Руководитель ОПОП

  
/ А.Г. Остапенко /

Воронеж 2017

## 1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

### 1.1. Цели дисциплины

Основная цель изучения данной дисциплины заключается в ознакомлении с проблемой социальных сетей с точки зрения повышения защищённости пользователей путём анализа моделей распространения вредоносного программного обеспечения, а также с помощью построения риск-моделей информационно-психологического воздействия на пользователей социальных сетей.

### 1.2. Задачи освоения дисциплины

- способность управлять информационными рисками;
- прогнозировать эффективность защиты распределённых информационных систем, подвергающихся деструктивному воздействию;

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Социальные сети: риски и обеспечение безопасности» относится к дисциплинам вариативной части блока Б1.

## 3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Социальные сети: риски и обеспечение безопасности» направлен на формирование следующих компетенций:

ПК-5 - способность проводить анализ рисков информационной безопасности автоматизированной системы;

ПК-13 - способность участвовать в проектировании средств защиты информации автоматизированной системы;

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-5	знать основные уязвимости социальных сетей для атак вредоносного ПО и информационно-психологического воздействия на пользователей опасные и вредоносные факторы воздействия на элементы социальных сетей и пользователей
	уметь применять основные меры и средства защиты социальных сетей от атак вредоносного ПО и воздействия на пользователей
	владеть навыками построения математических моделей осуществления атак на социальных сетей и воздействий на пользователей
ПК-13	знать основные виды ущерба при реализации атак и воздействии на пользователей социальных сетей

	уметь оценивать вероятностные и временные характеристики реализации атак вредоносного ПО и воздействия на пользователей социальных сетей
	владеть методикой анализа рисков при реализации атак вредоносного ПО и воздействий на пользователей социальных сетей

#### 4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Социальные сети: риски и обеспечение безопасности» составляет 123 е.

Распределение трудоемкости дисциплины по видам занятий  
**очная форма обучения**

Виды учебной работы	Всего часов	Семестры		
		7	8	9
<b>Аудиторные занятия (всего)</b>	148	72	36	40
В том числе:				
Лекции	74	36	18	20
Практические занятия (ПЗ)	74	36	18	20
<b>Самостоятельная работа</b>	248	90	90	68
<b>Курсовой проект</b>	+		+	
Часы на контроль	36	-	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+	+
Общая трудоемкость: академические часы	432	162	126	144
зач. ед.	12	4.5	3.5	4

#### 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.	СРС	Всего, час
1	Модели формирования и роста сетей	Модели формирования и роста сетей	14	12	40	66
2	Анализ структуры связей и роли узлов	Анализ структуры связей и роли узлов. Понятия центральности и престижа. Модельные графы. Degree centrality, closeness centrality, betweenness centrality, статус/rank prestige (eigenvector centrality). Центральность сети. Анализ связей. Алгоритм PageRank. Стохастические матрицы. Теорема Perron-Frobenius. Степенные итерации. Нахождение собственного вектора. Hubs и Authorities.	12	12	40	64
3	Метрики структурной эквивалентности узлов.	Метрики структурной эквивалентности узлов. Эвклидово расстояние. Расстояние Хэмминга. Корреляционный коэффициент. Сходство по	12	12	42	66

		косинусу). Ассортативное смешивание МодулярностьАссортативный коэффициент. Смешиваниепостепенямузлов .				
4	Сетевые сообщества	Сетевые сообщества. Понятие сетевых сообществ (networkcommunities). Плотность связей. Метрики. Разделение графа на части (graphpartitioning). Разрезы (cuts) в графе. Min-cut, quotient and normalized cuts метрики. Divisive and agglomerative algorithms. Repeatedbisection. Корреляционная матрица. Классификация алгоритмов нахождения сообществ. EdgeBetweenness. Newman-Girvin.	12	12	42	66
5	Диффузия и распространение эпидемий.	Уравнение диффузии. Диффузия на сетях. Дискретный оператор Лапласа, Матрица Лапласа, решение уравнения диффузии на графе. Случайные блуждания на графе. Модели SI, SIR, SIS. Решения дифференциальных уравнений. Предельные случаи.	12	12	42	66
6	Модели распространения влияния	Модели распространения влияния. Пороговые модели принятия решений. Granovetter's Threshold model коллективного поведения. Определения наиболее влиятельных узлов.	12	14	42	68
<b>Итого</b>			<b>74</b>	<b>74</b>	<b>248</b>	<b>396</b>

## 5.2 Перечень лабораторных работ Непредусмотрено учебным планом

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

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсового проекта в 8 семестре в очной форме обучения.

Примерная тематика курсового проекта: «Основные направления исследования компьютерных социальных сетей»

Задачи, решаемые при выполнении курсового проекта:

- Определение актуального статуса социальных сетей.
- Оценка их эффективности в рекламной деятельности компаний.
- Анализ деятельности музыкальной группы «Perpetum Mobile».

Курсовой проект включает 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 шкалы оценивания

#### 7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются в следующей системе:

«аттестован»;

«неаттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Неаттестован
ПК-5	знать основные уязвимости социальных сетей для атак вредоносного ПО и информационно-психологического воздействия на пользователей	Презентация, устный опрос	Выполнение работ в срок, предусмотренный в рабочих	Невыполнение работ в срок, предусмотренный в рабочих

	опасные и вредоносные факторы воздействия на элементы социальных сетей и пользователей		программах	программах
	уметь применять основные меры и средства защиты социальных сетей от атак вредоносного ПО и воздействия на пользователей	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками построения математических моделей осуществления атак на социальных сетях и воздействий на пользователей	Решение прикладных задач в конкретной предметной области	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-13	знать основные виды ущерба при реализации атак и воздействии на пользователей социальных сетей	Презентация, устный опрос	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь оценивать вероятностные и временные характеристики реализации атак вредоносного ПО и воздействия на пользователей социальных сетей	Решение стандартных практических задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть методикой анализа рисков при реализации атак вредоносного ПО и воздействий на пользователей социальных сетей	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 7, 8, 9 семестр для очной формы обучения по двух/четырёхбалльной системе:

«зачтено»

«незачтено»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Незачтено
ПК-5	знать основные уязвимости социальных сетей для атак вредоносного ПО и информационно-психологического воздействия на пользователей опасные и вредоносные факторы воздействия на элементы социальных сетей и пользователей	Презентация, устный опрос	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь применять основные меры и средства защиты социальных сетей от атак вредоносного ПО и воздействия на пользователей	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками построения математических моделей осуществления атак на социальных сетях и воздействий на пользователей	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-13	знать основные виды ущерба при реализации атак и воздействии на пользователей социальных сетей	Презентация, устный опрос	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь оценивать вероятностные и временные характеристики	Решение стандартных практических задач	Продемонстрирован верный ход решения в	Задачи не решены

	реализации атак вредоносного ПО и воздействия на пользователей социальных сетей		большинстве задач	
	владеть методикой анализа рисков при реализации атак вредоносного ПО и воздействий на пользователей социальных сетей	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи решены

ИЛИ

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ПК-5	знать основные уязвимости социальных сетей для атак вредоносного ПО и информационно-психологического воздействия на пользователей опасные и вредоносные факторы воздействия на элементы социальных сетей и пользователей	Презентация, устный опрос	Выполнено естана 90-100%	Выполнено естана 80-90%	Выполнено естана 70-80%	В тесте менее 70% правильных ответов
	уметь применять основные меры и средства защиты социальных сетей от атак вредоносного ПО и воздействия на пользователей	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи решены
	владеть навыками построения математических моделей осуществления атак на социальных сетях и воздействий на пользователей	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи решены
ПК-13	знать основные виды ущерба при реализации атак и воздействия на пользователей социальных сетей	Презентация, устный опрос	Выполнено естана 90-100%	Выполнено естана 80-90%	Выполнено естана 70-80%	В тесте менее 70% правильных ответов
	уметь оценивать вероятностные и временные характеристики реализации атак вредоносного ПО и воздействия на пользователей социальных сетей	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи решены
	владеть методикой анализа	Решение прикладных задач в	Задачи решены в	Продемонстрирован	Продемонстрирован	Задачи решены

	рисков при реализации атак вредоносного ПО и воздействий на пользователей социальных сетей	конкретной предметной области	полном объеме и получены верные ответы	верный ход решения всех, но не получен верный ответ во всех задачах	верный ход решения в большинстве задач	
--	--	-------------------------------	--	---	--	--

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

### **7.2.1 Примерный перечень заданий для подготовки к тестированию**

Непредусмотрено учебным планом

### **7.2.2 Примерный перечень заданий для решения стандартных задач**

Непредусмотрено учебным планом

### **7.2.3 Примерный перечень заданий для решения прикладных задач**

Непредусмотрено учебным планом

### **7.2.4 Примерный перечень вопросов для подготовки к зачету**

1. Понятия центральности и престижа.
2. Модельные графы.
3. Degree centrality, closeness centrality, betweenness centrality, статус/rank prestige (eigenvector centrality). Центральность сети.
4. Анализ связей. Алгоритм PageRank.
5. Стохастические матрицы. Теорема Perron-Frobenius. Степенные итерации.
6. Нахождение собственного вектора. Hubs и Authorities.
7. Алгоритм HITS. Сравнение ранжировок.
8. Расстояние Kendall-Tau.
9. Метрики структурной эквивалентности узлов.
10. Эвклидово расстояние. Расстояние Хэмминга.
11. Корреляционный коэффициент. Сходство по косинусу). Ассортативное смешивание Модулярность Ассортативный коэффициент. Смешивание по степени узлов
12. Понятие сетевых сообществ (network communities). Плотность связей. Метрики.
13. Разделение графа на части (graph partitioning).
14. Разрезы (cuts) в графе. Min-cut, quotient and normalized cuts метрики.
15. Divisive and agglomerative algorithms. Repeated bisection.
16. Корреляционная матрица. Классификация алгоритмов нахождения сообществ.
17. Edge Betweenness. Newman-Girvin. Спектральные методы. Максимизация модулярности (Newman)
18. Аппроксимационные алгоритмы.
19. Randomized min-cut (Karger's algorithm).
20. Multilevel алгоритмы. Metis алгоритм.
21. Локальная кластеризация. Conductance.
22. Алгоритм Nibble.
23. Нахождение структуры в графах.
24. Graph motifs, k-cores, diad and triad census
25. Уравнение диффузии. Диффузия на сетях.
26. Дискретный оператор Лапласа, Матрица Лапласа, решение уравнения диффузии на графе. Случайные блуждания на графе.

27. Модели SI, SIR, SIS. Решения дифференциальных уравнений. Предельные случаи.
28. Модели SI, SIR, SIS на сетях. Приближенные решения дифференциальных уравнений на сетях. Предельные случаи. Иммунизация.
29. Пороговые модели принятия решений.
30. Granovetter's Threshold model коллективного поведения.
31. Определение наиболее влиятельных узлов.
32. Программные приложения для анализа социальных сетей
33. Модели формирования и роста сетей
34. Метрики структурной эквивалентности узлов.

### **7.2.5 Примерный перечень заданий для решения прикладных задач**

1. Основные направления исследования компьютерных социальных сетей
2. Основные понятия в теории сетей. Основные измеряемые свойства сетей.
3. История исследования социальных сетей
4. Модели анализа социальных сетей
5. Степенное распределение. Распределение Парето, нормализация, моменты
6. Степенные законы для дискретных переменных.
7. Масштабно-инвариантные сети (scale-free networks).
8. Закон Ципфа. Граф ранк-частота.
9. Закон Хипса
10. Закономерность Бредфорда
11. Модель Эрдеша-Реньи
12. Наблюдения Барабаши-Альберт
13. Модель LCD
14. Модель Buckley-Osthus
15. Модель копирования
16. Модель Чунг-Лу
17. Модель Янсона-Лучака
18. Модель эпидемии SI
19. Модели просачивания и заражения
20. Модель распространения эпидемии, адаптированная к социальным информационным сетям
21. Риск-факторы безмасштабной сети
22. Подходы к управлению эпистойкостью атакуемой безмасштабной сети

### **7.2.6. Методика выставления оценки при проведении промежуточной аттестации**

*(Например: Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов по задаче. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов за верно решенные 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	Модели формирования и роста сетей	ПК-5, ПК-13	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
2	Анализ структуры связей и роли узлов	ПК-5, ПК-13	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
3	Метрики структурной эквивалентности узлов.	ПК-5, ПК-13	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
4	Сетевые сообщества	ПК-5, ПК-13	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
5	Диффузия и распространение эпидемий.	ПК-5, ПК-13	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....
6	Модели распространения влияния	ПК-5, ПК-13	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту....

### **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 методике 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 методике 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 задачи экзаменатором и выставляется оценка, согласно методике выставления оценок 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 УЧЕБНОМЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)**

### **8.1 Перечень учебной литературы, необходимой для освоения дисциплины**

Основная литература

Информационное государственное и муниципальное управление [Электронный ресурс] : Учеб. пособие / Г. А. Остапенко [и др.]. - Электрон. текстовые, граф. дан. (3,13 Кб ). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.

Дополнительная литература

Теория сетевых войн [Электронный ресурс] : Учеб. пособие / А. Г. Остапенко. - Электрон. текстовые, граф. дан. (894 Мб ). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 30-00.

Методические указания к курсовому проектированию по дисциплине «Социальные сети: риски и обеспечение безопасности» для студентов специальности 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: Е. А. Шварцкопф, О. А. Остапенко. - Электрон. текстовые, граф. дан. (784 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

Методические указания к практическим занятиям по дисциплине «Социальные сети: риски и обеспечение безопасности» для студентов специальности 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: Е. А. Шварцкопф, О. А. Остапенко. - Электрон. текстовые, граф. дан. (1,01 Мб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

Методические указания к самостоятельным работам по дисциплине «Социальные сети: риски и обеспечение безопасности» для студентов специальности 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: Е. А. Шварцкопф, О. А. Остапенко. -

Электрон. текстовые, граф. дан. (267 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

**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:**

<http://eios.vorstu.ru/>

<http://www.studentlibrary.ru/>

<http://znanium.com/>

<http://ibooks.ru/>

<http://e.lanbook.com/>

<http://www.iprbookshop.ru/>

## **9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА**

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой.

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

По дисциплине «Социальные сети: риски и обеспечение безопасности» читаются лекции, проводятся практические занятия, выполняется курсовой проект.

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 расчета информационных эпидемий в социальных сетях. Занятия проводятся путем решения конкретных задач в аудитории.

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

Контроль усвоения материала дисциплины производится проверкой курсового проекта, защитой курсового проекта.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; пометать 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.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоению 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 начинаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом, зачетом, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.