МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ 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

«Математические модели информационного противоборства»

Специальность 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Специализация «Безопасность распределённых компьютерных систем»

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2017

Автор программы _____/Чопоров О.Н./

Заведующий кафедрой систем информационной безопасности _____/Остапенко А.Г./

Руководитель ОПОП _____/Остапенко А.Г./

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины

Цель изучения дисциплины – формирование у студентов профессиональных знаний о методах и моделях защиты информации в условиях информационного противоборства.

1.2. Задачи освоения дисциплины

- изучить основные аспекты и модели информационного противоборства;
- изучить основные методы и средства защиты информации для информационных систем, находящихся в состоянии информационного конфликта;
- подготовить аспирантов к применению полученных знаний для анализа подсистемы информационной безопасности информационной системы и формирования модели управления информационной безопасностью объектов, находящихся в состоянии информационного конфликта.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Математические модели информационного противоборства» относится к дисциплинам вариативной части (дисциплина по выбору) блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Математические модели информационного противоборства» направлен на формирование следующих компетенций:

ПК-4 - способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем

ПК-6 - способностью участвовать в разработке проектной и технической документации

ПК-16 - способностью разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем

ПСК-3.2 - способностью анализировать защиту информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-4	знать основные угрозы безопасности информации и модели нарушителя объекта информатизации
	уметь применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации

	владеть навыками расчета показателей эффективности защиты информации, обрабатываемой в автоматизированных системах
ПК-6	знать требования ГОСТов на оформление научно-технической документации
	уметь разрабатывать проектной и технической документации
	владеть навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации
ПК-16	знать систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации
	уметь формировать заключение о выполнении требований нормативных правовых актов и нормативных методических документов в области информационной безопасности при проверке защищенных автоматизированных систем
ПСК-3.2	знать основные требования к подсистеме аудита и политике аудита и контрольных проверок работоспособности и защищенности распределенных компьютерных систем
	уметь умеет анализировать, оценивать и исключать уязвимости информационной безопасности в распределенных компьютерных системах на основе применения автоматизированных средства мониторинга, аудита и анализа защищенности данных систем
	владеть навыками проведения анализа уязвимости программных и программно-аппаратных средств системы защиты информации

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Математические модели информационного противоборства» составляет 6 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		5	6
Аудиторные занятия (всего)	132	72	60

В том числе:			
Лекции	56	36	20
Практические занятия (ПЗ)	76	36	40
Самостоятельная работа	48	18	30
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+
Общая трудоемкость: академические часы зач.ед.	 216 6	 90 2.5	 126 3.5

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	Цели и задачи курса	Признаки информационной эпохи История информационных войн. Основные термины и определения. Концепция национальной безопасности РФ и задачи обеспечения безопасности. Нормативно-законодательное обеспечение информационной безопасности страны.	10	12	8	30
2	Понятие информационного противоборства в конфликтологии	Объекты и субъекты информационного противоборства. Особенности внешнего управления информационно-психологическими процессами. Информационно-психологическая агрессия. Понятие информационного оружия. Анализ использования технологий психологической войны.	10	12	8	30
3	Социальные сети как среда информационного противоборства	Теоретико-игровые и имитационно-оптимизационные модели влияния и противоборства в социальных сетях. Стохастические модели социальных се-	10	12	8	30

		тей. Марковская модель информационного влияния. Информационное управление и репутация членов сети. Распределённый контроль и согласование интересов.				
4	Модели политик информационной безопасности	Модели политик информационной безопасности. Классификация существующих моделей политики ИБ. Модель дискреционного доступа (DAC). Модель безопасности Белла-Ла Падулы. Ролевая модель контроля доступа (RBAC)	10	12	8	30
5	Риск-моделирование информационного противоборства в информационных системах	Информационная система как объект атак. Методика анализа и регулирования рисков при реализации угроз доступа при информационном противоборстве в информационных системах. Оценка эффективности применения комплексов мер противодействия угрозам в процессе информационного противоборства в информационных системах	16	24	16	60
		Итого	**56**	**76**	**48**	**180**

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

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

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

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».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-4	знать основные положения, концепции и математические структуры, используемые для создания и исследования моделей автоматизированных систем	знает основные положения, концепции и математические структуры, используемые для создания и исследования моделей автоматизированных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь создавать и исследовать модели автоматизированных систем	умеет создавать и исследовать модели автоматизированных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть инструментальными средствами построения и анализа моделей автоматизированных систем	владеет инструментальными средствами построения и анализа моделей автоматизированных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-6	знать виды политик управления доступом и информационными потоками в автоматизированных системах	знает виды политик управления доступом и информационными потоками в автоматизированных системах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	умеет формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть подходами к моделированию безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах в условиях информационного противоборства	владеет подходами к моделированию безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах в условиях информационного противоборства	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-16	знать методологию менеджмента рисков информационной безопасности в автоматизированных системах	знает методологию менеджмента рисков информационной безопасности в автоматизированных системах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы в усло-	умеет выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	виях информационного противоборства; умеет контролировать эффективность принятых мер по реализации политик безопасности информации распределённых информационных системах в условиях информационного противоборства	в условиях информационного противоборства; умеет контролировать эффективность принятых мер по реализации политик безопасности информации распределённых информационных системах в условиях информационного противоборства		
ПСК-3.2	знать основные требования к подсистеме аудита и политике аудита и контрольных проверок работоспособности и защищенности распределенных компьютерных систем	знает основные требования к подсистеме аудита и политике аудита и контрольных проверок работоспособности и защищенности распределенных компьютерных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь умеет анализировать, оценивать и исключать уязвимости информационной безопасности в распределенных компьютерных системах на основе применения автоматизированных средства мониторинга, аудита и анализа защищенности данных систем	умеет анализировать, оценивать и исключать уязвимости информационной безопасности в распределенных компьютерных системах на основе применения автоматизированных средства мониторинга, аудита и анализа защищенности данных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками проведения анализа уязвимости программных и программно-аппаратных средств системы защиты информации	владеет навыками проведения анализа уязвимости программных и программно-аппаратных средств системы защиты информации	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 5, 6 семестре для очной формы обучения по двух/четырехбалльной системе:

«зачтено»

«не зачтено»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
ПК-4	знать основные положения, концепции и математические структуры, используемые для создания и исследования моделей автоматизированных систем	Тест	Выполнение теста на 70-100%	Выполнение менее 70%

	уметь создавать и исследовать модели автоматизированных систем	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть инструментальными средствами построения и анализа моделей автоматизированных систем	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-6	знать виды политик управления доступом и информационными потоками в автоматизированных системах	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть подходами к моделированию безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах в условиях информационного противоборства	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-16	знать методологию менеджмента рисков информационной безопасности в автоматизированных системах	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы в условиях информационного противоборства; умеет контролировать эффективность принятых мер по реализации политик безопасности информации распределённых информационных системах в условиях информационного противоборства	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПСК-3.2	знать основные требования к подсистеме аудита и политике аудита и контрольных проверок работоспособности и	Тест	Выполнение теста на 70-100%	Выполнение менее 70%

	защищенности распределенных компьютерных систем			
	уметь умеет анализировать, оценивать и исключать уязвимости информационной безопасности в распределенных компьютерных системах на основе применения автоматизированных средства мониторинга, аудита и анализа защищенности данных систем	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть навыками проведения анализа уязвимости программных и программно-аппаратных средств системы защиты информации	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

или

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	**Результаты обучения, характеризующие сформированность компетенции**	**Критерии оценивания**	**Отлично**	**Хорошо**	**Удовл.**	**Неудовл.**
ПК-4	знать основные положения, концепции и математические структуры, используемые для создания и исследования моделей автоматизированных систем	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80- 90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь создавать и исследовать модели автоматизированных систем	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 не решены
	владеть инструментальными средствами построения и анализа моделей автоматизированных систем	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 не решены
ПК-6	знать виды политик управления доступом и информационными потоками в автоматизированных системах	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80- 90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов

	уметь формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	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 не решены
	владеть подходами к моделированию безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах в условиях информационного противоборства	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 не решены
ПК-16	знать методологию менеджмента рисков информационной безопасности в автоматизированных системах	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80- 90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы в условиях информационного противоборства; умеет контролировать эффективность принятых мер по реализации политик безопасности информации распределённых информационных системах в условиях информационного противоборства	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 не решены
ПСК-3.2	знать основные требования к подсистеме аудита и политике аудита и контрольных проверок работоспособности и защищенности распределенных компьютерных систем	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80- 90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь умеет анали-	Решение стандартных	Задачи решены в	Продемонстрирован верный	Продемонстрирован	Задачи не решены

	зировать, оценивать и исключать уязвимости информационной безопасности в распределенных компьютерных системах на основе применения автоматизированных средства мониторинга, аудита и анализа защищенности данных систем	практических задач	полном объеме и получены верные ответы	ход решения всех, но не получен верный ответ во всех задачах	ван верный ход решения в большинстве задач	
	владеть навыками проведения анализа уязвимости программных и программно-аппаратных средств системы защиты информации	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 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

7.2.2 Примерный перечень заданий для решения стандартных задач

7.2.3 Примерный перечень заданий для решения прикладных задач

7.2.4 Примерный перечень вопросов для подготовки к зачету

Укажите вопросы для зачета

7.2.5 Примерный перечень заданий для решения прикладных задач

Укажите вопросы для экзамена

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)	Код	Наименование

	дисциплины	контролируемой компетенции	оценочного средства
1	Цели и задачи курса	ПК-4, ПК-6, ПК-16, ПСК-3.2	Тест
2	Понятие информационного противоборства в конфликтологии	ПК-4, ПК-6, ПК-16, ПСК-3.2	Тест, сдача практической
3	Социальные сети как среда информационного противоборства	ПК-4, ПК-6, ПК-16, ПСК-3.2	Тест, сдача практической
4	Модели политик информационной безопасности	ПК-4, ПК-6, ПК-16, ПСК-3.2	Тест, сдача практической
5	Риск-моделирование информационного противоборства в информационных системах	ПК-4, ПК-6, ПК-16, ПСК-3.2	Тест, сдача практической

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.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература

Остапенко А.Г. Методология риск-анализа и моделирования кибернетических систем, атакуемых вредоносным программным обеспечением [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (112 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2012. - 1 файл. - 30-00.

Дополнительная литература

1.Методические указания к самостоятельным работам по дисциплинам

«Математические модели информационного противоборства», «Математическое моделирование информационных операций и атак» для студентов специальностей 090301 «Компьютерная безопасность», 090302 «Информационная безопасность телекоммуникационных систем», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: О. Н. Чопоров, Е. А. Шварцкопф. - Электрон. текстовые, граф. дан. (262 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

2.Губанов Д.А. Социальные сети. Модели информационного влияния, управления и противоборства [Электронный ресурс]: учебное пособие/ Губанов Д.А., Новиков Д.А., Чхартишвили А.Г.— Электрон. текстовые данные.— Москва: Издательство физико-математической литературы, 2010.— 228 с.— Режим доступа: http://www.iprbookshop.ru/8531.html.— ЭБС «IPRbooks».

3. Новиков Д.А. Прикладные модели информационного управления [Электронный ресурс]: монография/ Новиков Д.А., Чхартишвили А.Г.— Электрон. текстовые данные.— Москва: ИПУ РАН, 2004.— 129 с.— Режим доступа: http://www.iprbookshop.ru/8518.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:

http://att.nica.ru
http://www.edu.ru/
http://window.edu.ru/window/library
http://www.intuit.ru/catalog/
http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp
https://cchgeu.ru/education/cafedras/kafsib/?docs
http://www.eios.vorstu.ru
http://e.lanbook.com/ (ЭБС Лань)
http://IPRbookshop.ru/ (ЭБСIPRbooks)

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой. Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО

ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Математические модели информационного противоборства» читаются лекции, проводятся практические занятия.

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 индексов влияния в социальных сетях. Занятия проводятся путем решения конкретных задач в аудитории.

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.
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, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.